FINANSTILSYNET

Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme (hvidvaskloven)

November 2020

Indhold

Del 1 – Anvendelsesområde og definitioner

1. Indledning

Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme (hvidvaskloven) henvender sig til virksomheder og personer, der er omfattet af hvidvaskloven (lovbekendtgørelse nr. 380 af 2. april 2020 om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme). Vejledningen handler om, hvordan disse virksomheder og personer kan opfylde kravene i hvidvaskloven og omfatter reglerne på området for hvidvask og finansiering af terrorisme, idet der dog nogle steder er nævnt, hvordan der kan være sammenhæng til andre regelområder.

Virksomheder og personer skal således være opmærksomme på, at der kan være krav i anden lovgivning, som de samtidig skal overholde.

Denne vejledning erstatter vejledning af 11. oktober 2018 om lov om forebyggende foranstaltninger mod hvidvask af udbytte og finansiering af terrorisme (hvidvaskloven).

Hvidvaskloven gennemfører EU's 4. og 5. hvidvaskdirektiv (Europa-Parlamentets og Rådets direktiv 2015/849/EU af 20. maj 2015 og 2018/843/EU af 30. maj 2018 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme) og bygger herudover på anbefalinger fra Financial Action Task Force (FATF), som Danmark er medlem af.

Finanstilsynet har samlet information om området for hvidvask og finansiering af terrorisme på tilsynets hjemmeside: https://www.finanstilsynet.dk/Tilsyn/Information-om-udvalgte-tilsynsomraader/Hvidvask. Vejledningen anvender virksomheder som fællesbetegnelse for virksomheder og personer, der er omfattet af loven.

Hvidvaskloven bygger på en betragtning om, at virksomheder omfattet af loven skal have en risikobaseret tilgang og selv fastsætte rammerne for, hvordan de overholder hvidvasklovgivningen. Vejledningens eksempler skal ses som en måde, hvor virksomheder kan finde inspiration til overholdelse af lovens krav. Eksemplerne er dog ikke et udtryk for den eneste måde, som virksomhederne kan opfylde lovens krav på og skal heller ikke anses som en udtømmende liste for overholdelse af lovens krav.

Vejledningen kan ikke udgøre det eneste bidrag til virksomhedens risikobaserede tilgang til overholdelse af hvidvasklovgivningen. Virksomheden skal ikke kun vurdere egne forhold, men også søge inspiration i nationale og supranationale risikovurderinger samt rapporter fra f.eks. European Banking Authority (EBA) og FATF, hvor dette er relevant.

Følgende virksomheder er omfattet af hvidvaskloven:

1) Pengeinstitutter.
2) Realkreditinstitutter.
3) Fondsmæglerselskaber.
4) Livsforsikringsselskaber og tværgående pensionskasser.
5) Sparevirksomheder.
6) Udbydere af betalingstjenester og udstedere af elektroniske penge, jf. bilag 1, nr. 1-7 i lov om betalinger.

7) Forsikringsformidlere, når de formidler livsforsikringer eller andre investeringsrelaterede forsikringer.
8) Øvrige virksomheder og personer, der erhvervsmæssigt udøver en eller flere af aktiviteterne som nævnt i bilag 1, jf. dog lovens § 1, stk. 4. Se afsnit 1.1. om øvrige personer og virksomheder omfattet af hvidvaskloven.
9) Udenlandske virksomheders filialer, distributører og agenter her i landet, der udøver virksomhed efter nr. 1-7, 10 og 11.
10) Investeringsforvaltningsselskaber og forvaltere af alternative investeringsfonde, hvis disse virksomheder har direkte kundekontakt.
11) Danske UCITS og alternative investeringsfonde, hvis disse virksomheder har direkte kundekontakt.
12) Operatører af et reguleret marked, der har fået tilladelse i Danmark til at være auktionsplatform i henhold til Europa-Kommissionens forordning 2010/1031/EU af 12. november 2010 om det tidsmæssige og administrative forløb af auktioner over kvoter for drivhusgasemissioner og andre aspekter i forbindelse med sådanne auktioner i medfør af Europa-Parlamentets og Rådets direktiv 2003/87/EF om en ordning for handel med kvoter for drivhusgasemissioner i Fællesskabet.
13) Aktører, som har tilladelse til at byde direkte på auktioner, der er omfattet af Europa-Kommissionens forordning 2010/1031/EU af 12. november 2010 om det tidsmæssige og administrative forløb af auktioner over kvoter for drivhusgasemissioner og andre aspekter i forbindelse med sådanne auktioner i medfør af Europa-Parlamentets og Rådets direktiv 2003/87/EF om en ordning for handel med kvoter for drivhusgasemissioner i Fællesskabet, og som ikke allerede er omfattet efter nr. 1 og 3.
14) Advokater,
    a. når de yder bistand ved rådgivning om eller udførelse af transaktioner for deres klienter i forbindelse med
        i. køb og salg af fast ejendom eller virksomheder,
        ii. forvaltning af klienters penge, værdipapirer eller andre aktiver,
        iii. åbning eller forvaltning af bankkonti eller værdipapirdepoter,
        iv. tilvejebringelse af nødvendig kapital til oprettelse, drift eller ledelse af virksomheder eller
        v. oprettelse, drift eller ledelse af virksomheder, fonde mv., eller
    b. når de på en klients vegne og for dennes regning foretager en finansiel transaktion eller en transaktion vedrørende fast ejendom.
15) Revisorer og revisionsvirksomheder godkendt i henhold til revisorloven.
16) Ejendomsmæglere og ejendomsmæglervirksomheder, herunder når de optræder som mellemmænd i forbindelse med udlejning af fast ejendom.
17) Virksomheder og personer, der i øvrigt erhvervsmæssigt leverer samme ydelser som de i nr. 14-16 nævnte persongrupper, herunder revisorer, som ikke er godkendt i henhold til revisorloven, skatterådgivere, eksterne bogholdere og enhver anden person, der forpligter sig til at yde hjælp, bistand eller rådgivning om skatteanliggender som sin vigtigste erhvervsmæssige virksomhed.
18) Udbydere af tjenesteydelser til virksomheder, jf. lovens § 2, nr. 12, se afsnit 1.3 om registrering hos Erhvervsstyrelsen.
19) Valutavekslingsvirksomhed, jf. dog lovens § 1, stk. 4.
20) Udbydere af spil, jf. dog lovens § 1, stk. 5.
21) Danmarks Nationalbank, i det omfang den udøver tilsvarende virksomhed som institutter nævnt i nr. 1.

22) Virksomheder og personer, der erhvervsmæssigt opbevarer, handler med eller formidler handel med kunstværker, herunder gallerier og auktionshuse, hvor værdien af transaktionen eller af en række indbyrdes forbundne transaktioner udgør 50.000 kr. eller derover.
23) Udbydere af veksling mellem virtuelle valutaer og fiatvalutaer.
24) Udbydere af virtuelle tegnebøger.

Ovenstående punkt 6) omfatter virksomheder, der udsteder elektroniske penge eller udbyder betalingstjenester, og som er underlagt krav om tilladelse som betalingsinstitut eller e-pengeinstitut eller begrænset tilladelse til at udbyde betalingstjenester eller udstede e-penge efter reglerne i lov om betalinger. Virksomheder, der kun udbyder kontooplysningstjenester, jf. § 60 i lov om betalinger, er dog ikke omfattet. Virksomheder, der udbyder betalingstjenester, men ikke er omfattet af et tilladelseskrav efter lov om betalinger, eksempelvis virksomheder omfattet af § 5, nr. 14-17, i lov om betalinger, er ikke omfattet.

I forhold til punkt 22) er det ikke alle kunsttyper, der er omfattet af hvidvaskloven. Der henvises til Erhvervsstyrelsens quick-guide (https://erhvervsstyrelsen.dk/quick-guide-kunstbranchen) for yderligere information om hvilke kunsttyper, der er omfattet samt hvilke forhold man skal være særligt opmærksom på, når man opbevarer, handler med eller formidler handel med kunstværker.

I forhold til punkt 23) er virtuel valuta et digitalt udtryk for værdi, som ikke er udstedt eller garanteret af en centralbank eller en offentlig myndighed og ikke nødvendigvis er bundet til en lovligt oprettet valuta. Virtuel valuta har ikke samme retlige status som valuta eller penge, men accepteres af fysiske eller juridiske personer som vekslingsmiddel og kan overføres, lagres og handles elektronisk. Ved fiatvaluta forstås et lovligt betalingsmiddel, som er udstedt af en centralbank.

Ovenstående punkt 24) omfatter en enhed, som leverer tjenester til at beskytte private kryptografiske nøgler på vegne af deres kunder med henblik på at opbevare, lagre og overføre virtuelle valutaer. En privat kryptografisk nøgle skal forstås som en adgang til at disponere over en virtuel valuta på en given placering. Hvis en privat kryptografisk nøgle mistes, mistes adgangen til at flytte den virtuelle valuta til en anden placering.

1.1. Øvrige virksomheder og personer omfattet af hvidvaskloven - bilag 1

Henvisning til hvidvaskloven: § 48, stk. 1 og bilag 1. Henvisning til 4. hvidvaskdirektiv: Artikel. 3, stk. 2, litra a. Henvisning til anden lovgivning: Lov om finansiel virksomhed bilag 1 og 2.

Hvidvasklovens § 1, stk. 1, nr. 8, er en opsamlingsbestemmelse, der omfatter virksomheder, som erhvervsmæssigt udøver en eller flere af de finansielle aktiviteter, der er nævnt i bilag 1, uden at den pågældende virksomhed er omfattet af § 1, stk. 1, nr. 1-7.

Bilag 1 til hvidvaskloven er en sammenskrivning af bilag 1 og bilag 2 til lov om finansiel virksomhed, der oplister pengeinstitut- og kreditinstitutvirksomhed. Dog er kreditoplysningsvirksomheder samt øvrig virksomhed i forbindelse med omsætning af penge og kreditmidler ikke omfattet af hvidvasklovens bilag 1.

Bilag 1 i hvidvaskloven skal fortolkes i overensstemmelse med lov om finansiel virksomhed for så vidt angår de finansielle aktiviteter, hvor der er sammenfald mellem bilagene.

Hvis en virksomhed udøver en eller flere aktiviteter i bilag 1 til hvidvaskloven, skal virksomheden registreres hos Finanstilsynet. Se afsnit 1.2. om hvidvaskregistrering hos Finanstilsynet.

Se herudover afsnit 1.1. om øvrige virksomheder og personer omfattet af hvidvaskloven.

1.1.1. Modtagelse af indlån og andre tilbagebetalingspligtige midler

Dette omfatter virksomheder, der henvender sig til offentligheden, og som erhvervsmæssigt udbyder indlån og andre tilbagebetalingspligtige midler uden at skulle have en tilladelse som pengeinstitut eller sparevirksomhed.

Indlån og andre tilbagebetalingspligtige midler er indskud, hvor indskyderen har krav på at få sin fordring tilbagebetalt i sin helhed.

1.1.2. Udlånsvirksomhed

Udlånsvirksomhed omfatter blandt andet forbrugerkreditter, realkreditlån, factoring og diskontering samt handelskreditter (inkl. forfaitering). Alle former for udlånsvirksomhed er omfattet. De underpunkter, der nævnes, er alene eksempler, der ikke indebærer nogen begrænsninger i de låneformer, der er omfattet. Udlånsvirksomhed omfatter både udlån til erhverv og til private. Formidling af lån er ikke omfattet.

1.1.3. Finansiel leasing

Ved finansiel leasing forstås de typer af leasingaftaler, hvor leasingtager bærer den finansielle risiko for leasingudstyrets anslåede restværdi ved leasingaftalens udløb.
Leasingstager forpligter sig til i leasingperioden at betale en leasingafgift, der er en afvikling på det "bagvedliggende lån" i leasingselskabet.
Leasingudstyret har ofte en restværdi ved leasingaftalens udløb. Det indskrives derfor ofte i leasingaftalen, at leasingtager på dette tidspunkt er forpligtet til på anfordring at anvise en køber af udstyret til den anslåede restværdi.

Operationel leasing er en anden leasingform, der ikke er omfattet af hvidvaskloven. Ved operationel leasing bærer leasingtager ikke risikoen for restværdien af leasingudstyret ved leasingaftalens udløb. Ved leasingaftalens udløb afleverer leasingtager udstyret tilbage til leasingselskabet, og det er leasingselskabet, der bærer risikoen for, at leasingudstyret kan indbringe den anslåede restværdi. Leasingudstyret har på tidspunktet for udgangen af en operationel leasingaftale en ikke ubetydelig anslået restværdi.

1.1.4. Udstedelse og administration af andre betalingsmidler (for eksempel rejsechecks og bankveksler), i det omfang aktiviteten ikke er omfattet af lov om betalinger

Dette omfatter udstedelse og administration af andre betalingsmidler, i det omfang aktiviteten ikke er omfattet af lov om betalinger. Dette betyder, at f.eks. udstedelse af rejsechecks og bankveksler er omfattet. Oplistningen er alene eksempler og er derfor ikke udtømmende.

1.1.5. Sikkerhedsstillelse og garantier

Lån mod sikkerhedsstillelse, f.eks. fakturabelåning eller lån mod pant i fast ejendom, løsøre eller værdipapirer, er omfattet. Garantiudstedelse (kaution) af enhver art er omfattet. Det er dog en forudsætning, at virksomheden udøves erhvervsmæssigt, f.eks. et kautionsforsikringsselskab.

1.1.6. Transaktioner for kunders regning

De transaktioner for kunders regninger, der er omfattet, er:

a) pengemarkedsinstrumenter (checks, veksler, indskudsbeviser mv.),
b) valutamarkedet,
c) finansielle futures og optioner,
d) valuta- og renteinstrumenter,
e) værdipapirer.

Ved pengemarkedsinstrumenter forstås de instrumenter, der normalt omsættes på pengemarkedet, f.eks. skatkammerbeviser, der er kortfristede gældsbreve udstedt af staten.

1.1.7. Medvirken ved emission af værdipapirer og tjenesteydelser i forbindelse hermed

Dette omfatter f.eks. medvirken til notering på et reguleret marked.

1.1.8. Rådgivning til virksomheder vedrørende kapitalstruktur, industristrategi og dermed beslægtede spørgsmål samt rådgivning og tjenesteydelser vedrørende sammenslutning og opkøb af virksomheder

Dette omfatter blandt andet rådgivning om notering og placering af aktier og aktierelaterede værdipapirer via regulerede markedspladser, private placeringer af unoterede aktier, større sekundære aktieplaceringer via regulerede markedspladser samt rådgivning i forbindelse med gennemførelse af fusioner og virksomhedsoverdragelse. Denne form for virksomhed betegnes også "merchant banking".

1.1.9. Pengeformidling (money broking)

Ved pengeformidling forstås, virksomhed, der består i at formidle kontakt mellem virksomheder, der ønsker at låne penge, og virksomheder, der ønsker at udlåne penge. Pengemarkedet er en samlebetegnelse for de finansielle markeder for aktiver involveret i kortfristede lån/udlån med en løbetid på et år eller mindre.

1.1.10. Porteføljeadministration og -rådgivning

Udøver en virksomhed erhvervsmæssigt porteføljeadministration og –rådgivning om køb og salg af værdipapirer, og er virksomheden ikke omfattet af de virksomhedstyper, der specifikt er nævnt i hvidvasklovens § 1, stk. 1, er virksomheden omfattet af loven for den del af virksomhedens aktivitet, der vedrører porteføljeadministration og –rådgivning.

Aktiviteten "porteføljeadministration og –rådgivning" omfatter portefølje- og investeringsrådgivning, hvor en virksomhed udbyder personlige anbefalinger til en kunde, enten på anmodning eller på investeringsselskabets eget initiativ, af en eller flere transaktioner i tilknytning til finansielle instrumenter. Det er således denne type aktivitet, der er omfattet af hvidvasklovens regler.

1.1.11. Opbevaring og forvaltning af værdipapirer

Forvaltning adskiller sig i denne sammenhæng fra "porteføljeadministration og rådgivning" ved, at forvaltning forudsætter et diskretionært mandat til at købe og sælge værdipapirer fra kunden uden dennes samtykke til den konkrete disposition.

1.1.12. Boksudlejning

Boksudlejning er omfattet af bilag 1 til hvidvaskloven.

Udbud af boksudlejning kræver en registrering efter hvidvaskloven, fordi en boks kan anvendes til opbevaring af bl.a. kontante midler, ædelmetaller og andre fysiske genstande, der har en høj værdi. Se afsnit 1.2 om hvidvaskregistrering hos Finanstilsynet.

Hvis virksomheden kun udbyder opbevaring af f.eks. møbler, bagage, køretøjer og lignende, er det ikke omfattet af bilag 1 til hvidvaskloven. Tilsvarende er kortvarig, lejlighedsvis opbevaring, som et hotel f.eks. stiller til rådighed for sine kunder, ikke omfattet.

1.2. Hvidvaskregistrering hos Finanstilsynet

Henvisning til hvidvaskloven: § 1, stk. 1, nr. 8, 23 og 24, og § 48, stk. 1 og 2. Henvisning til 4. hvidvaskdirektiv: Artikel 47, stk. 1. Henvisning til 5. hvidvaskdirektiv: Artikel 1, stk.1, nr. 29.

Virksomheder, der erhvervsmæssigt påtænker at udøve en eller flere aktiviteter, der er oplistet i hvidvasklovens bilag 1, skal anmelde sig til registrering hos Finanstilsynet.

Registrering hos Finanstilsynet er en forudsætning for, at virksomheden kan udøve den omhandlede aktivitet. Det betyder, at virksomheder, der driver virksomhed efter bilag 1 eller efter § 1, stk. 1, nr. 23 og 24, uden at have anmeldt sig til registrering, eller som er nægtet registrering, udøver ulovlig virksomhed.

Registreringspligten gennemføres, for at Finanstilsynet kan føre tilsyn med virksomheder, der erhvervsmæssigt udøver en eller flere af de aktiviteter, som er nævnt i bilag 1, eller de aktiviteter der er omfattet af § 1, stk. 1, nr. 23 og 24. Virksomheder, der allerede i henhold til anden lovgivning er under Finanstilsynets tilsyn, skal ikke registreres i medfør af § 48, stk. 1.

Anmeldelse skal ske, selvom aktiviteten ikke er virksomhedens hovedaktivitet. Virksomheden skal dog ikke registreres, hvis der blot er tale om enkeltstående erhvervsmæssige dispositioner, der har naturlig tilknytning til virksomhedens hovedaktivitet. Eksempelvis omfatter begrebet erhvervsmæssigt ikke virksomheders placering af overskudslikviditet, hvor formålet er passiv formuepleje, f.eks. løbende placering af overskudslikviditet i børsnoterede aktier eller obligationer.

Med erhvervsmæssigt forstås:

1) at aktiviteten bliver udbudt til tredjemand (”kunder”) eller
2) at aktiviteten har et sådan omfang, at den udgør en ikke ubetydelig del af virksomhedens omsætning.

Hæderlighedsvurdering

En virksomhed, der søger om at blive registreret hos Finanstilsynet, må ikke være dømt for et strafbart forhold, der begrunder nærliggende fare for misbrug af registreringen. Finanstilsynet kan inddrage registreringen, hvis en virksomhed efterfølgende bliver dømt for et sådant forhold.

Finanstilsynet skal vurdere, om personer eller medlemmer af ledelsen og kredsen af reelle ejere i virksomheder, der skal registreres hos Finanstilsynet, opfylder krav om hæderlighed. De virksomheder og personer, der er omfattet af bestemmelsen, skal give Finanstilsynet de oplysninger, der er nødvendige for, at Finanstilsynet kan vurdere, om kravene er opfyldt.

Finanstilsynets vurdering sker særligt med henblik på at sikre, at de nævnte virksomheder, herunder medlemmer af ledelsen og kredsen af reelle ejere, der udøver en eller flere aktiviteter i bilag 1, eksempelvis ikke tidligere er dømt for en økonomisk forbrydelse.

Finanstilsynets har pligt til at undlade at registrere en virksomhed, hvis virksomheden eller virksomhedens ledelse eller reelle ejere er dømt for et strafbart forhold, der begrunder en nærliggende fare for misbrug af registreringen.

Formålet med bestemmelsen er at minimere risikoen for hvidvask af penge i virksomheden og kanalisering af penge til terrorformål ved at hindre, at personer med bestemmende indflydelse på virksomheden kan anvende virksomheden til kriminelle formål.

Det er som udgangspunkt kun strafbare handlinger, der relaterer sig til ovenstående typer kriminalitet, der indgår i Finanstilsynets vurdering. Domme for skatteunddragelse vil kunne medføre et afslag på registrering under hensyn til, at skatteunddragelse er omfattet af definitionen af hvidvask. Se afsnit 2.1 om definitioner, hvidvask.

1.3. Registrering hos Erhvervsstyrelsen

Henvisning til hvidvaskloven: § 1, stk. 1, nr. 18, § 2, stk. 1, nr. 12, § 57, stk. 2 og § 58.

Henvisning til 4. hvidvaskdirektiv: Artikel 47 (Artikel 2, stk. 1, nr. 3, litra c.).

Henvisning til anden lovgivning: Bekendtgørelse om anmeldelse og registrering af udbydere af tjenesteydelser til virksomheder i Erhvervsstyrelsens register til bekæmpelse af hvidvask.

Virksomheder, som udbyder tjenesteydelser til virksomheder, jf. § 2, nr. 12, skal registreres hos Erhvervsstyrelsen i register til bekæmpelse af hvidvask for lovligt at kunne udøve denne virksomhed.

Baggrunden for registreringspligten er, at udbydere af tjenesteydelser til virksomheder anses for at være særligt udsatte for en risiko for at blive misbrugt af deres kunder i forbindelse med hvidvask og terrorfinansiering.

Det bemærkes at advokater og advokatvirksomheder, revisorer og revisionsvirksomheder samt ejendomsmæglere og ejendomsmæglervirksomheder, som er omfattet af hvidvasklovens § 1, stk. 1, nr. 14-16, ikke skal registreres i Erhvervsstyrelsens register til bekæmpelse af hvidvask, selvom de udbyder samme ydelser som omfattet af registreringspligten.

Det bemærkes i øvrigt at bogholdere, skatterådgivere mv., som er omfattet af hvidvasklovens § 1, stk. 1, nr. 17, ikke skal registreres, medmindre de erhvervsmæssigt også udbyder mindst én af ydelserne som nævnt i § 2, nr. 12.

For at være omfattet af registreringspligten skal virksomheden udbyde mindst én af følgende ydelser:

1) *Oprettelse af selskaber, virksomheder eller andre juridiske personer*
    a) Bestemmelsen omfatter både oprettelse af selskaber, virksomheder og andre juridiske personer. Bistand til oprettelse af frivillige foreninger mv. vil derfor også være omfattet.

    b) Registreringspligten gælder for al form for erhvervsmæssig bistand til udarbejdelse af dokumenter, kontakt til myndigheder og registrering af selskaber eller lignende. Det er således ikke afgørende, om den pågældende foretager selve anmeldelsen eller registreringen hos Erhvervsstyrelsen, men om den pågældende foretager det konkrete arbejde ved oprettelsen.

    c) Bestemmelsen omfatter alene erhvervsmæssigt udbud til tredjemand.

2) *Virtuelle kontorhoteller*
    a) Bestemmelsen omfatter den, der stiller hjemstedsadresse eller anden adresse, der på lignende vis er beregnet som kontaktadresse, og dertil knyttede tjenester til rådighed for en virksomhed.

    b) Med ”*dertil knyttede tjenester*” menes tjenester, der relaterer sig til drift af virksomheden. Det kan f.eks. bestå i en reception, telefontjeneste, videresendelse af post, virksomhedsadministration, bogholderi eller lignende.

    c) Bestemmelsen omfatter alene såkaldte ”virtuelle kunder”, som ikke befinder sig fysisk på adressen.

    d) Har en virksomhed både virtuelle og fysiske kunder, er det alene de virtuelle kunder, som omfattes af hvidvasklovens anvendelsesområde.

    e) Det er vurderingen, at risikoen for hvidvask og terrorfinansiering er høj i forbindelse med virtuelle kunder, da kunden har mulighed for at skjule eller sløre sin identitet.

3) *Professionelle ledelsesmedlemmer*
    a) Bestemmelsen omfatter personer, der fungerer som eller sørger for, at en anden person fungerer som ledelsesmedlem i en virksomhed, eller som deltager i et interessentskab eller en tilsvarende post i andre virksomheder.

    b) Professionelle ledelsesmedlemmer omfatter f.eks. de personer, som i erhvervsøjemed fungerer som eksempelvis bestyrelsesmedlem eller direktør i en virksomhed. Det afgørende er, at ledelsesmedlemmet agerer på vegne af tredjemand, og at der ikke er tale om en ansættelse eller udpegning i traditionel forstand.

    c) Omfattet af bestemmelsen er eksempelvis personer, som i en opstartsfase, fungerer som direktør for en udenlandsk virksomhed, som skal etableres i Danmark.

4) *Forvaltere eller administratorer af en trust, fond eller lignende juridisk arrangement*

a) Bestemmelsen omfatter personer, der fungerer som eller sørger for, at en anden person fungerer som forvalter eller administrator i en trust, fond eller lignende juridisk arrangement.

b) Definitionen omfatter blandt andet de såkaldte trustees, dvs. de personer, der af stifteren af en trust er udpeget til at forvalte midlerne i trusten.

5) Nominees

a) Bestemmelsen omfatter personer der fungerer som eller sørger for, at en anden fungerer som nominee for tredjemand, medmindre det drejer sig om en virksomhed, hvis ejerandele mv. handles på et reguleret marked eller et tilsvarende marked, som er undergivet oplysningspligt i overensstemmelse med EU-retten eller tilsvarende internationale standarder.

b) Definitionen omfatter f.eks. personer der fungerer som repræsentanter for aktionæren, eller sørger for at andre gør det, dvs. såkaldte nominees, som indskriver aktier i eget navn i aktionærfortegnelsen, men hvor aktierne ejes af andre.

Erhvervsmæssigt udbud

For at ydelsen omfattes af registreringspligten, skal den udbydes erhvervsmæssigt.

Med erhvervsmæssigt forstås, at ydelserne udbydes på markedslignende vilkår, samt at virksomheden normalt modtager vederlag for ydelserne.

Det er ikke afgørende, om den pågældende tjenesteydelse er overskudsgivende, eller om der i den konkrete situation ikke betales vederlag. Enkeltstående udbud af de omhandlede tjenesteydelser, som ikke kan karakteriseres som erhvervsmæssig, vil ikke være omfattet.

Hæderlighedsvurdering

En virksomhed eller person, der søger om at blive registreret hos Erhvervsstyrelsen, må ikke være dømt for et strafbart forhold, der begrunder nærliggende fare for misbrug af stillingen. Virksomheden må endvidere ikke have indgivet begæring om rekonstruktionsbehandling eller konkurs, eller være under rekonstruktionsbehandling eller konkursbehandling.

Erhvervsstyrelsen skal vurdere, om personer, herunder medlemmer af ledelsen og kredsen af reelle ejere i virksomheder, der skal registreres hos Erhvervsstyrelsen, opfylder kravet om hæderlighed/egnethed. De virksomheder og personer, der er omfattet af bestemmelsen, skal give Erhvervsstyrelsen de oplysninger, der er nødvendige for, at Erhvervsstyrelsen kan vurdere, om kravene er opfyldt, hvilket også gælder oplysninger om efterfølgende ændringer.

Erhvervsstyrelsens vurdering sker særligt med henblik på at sikre, at de nævnte virksomheder, herunder medlemmer af ledelsen og kredsen af reelle ejere, der udbyder ydelser omfattet af § 2, nr. 12, eksempelvis ikke tidligere er dømt for en økonomisk forbrydelse der begrunder en nærliggende fare for misbrug af de ydelser, som udbydes, og Erhvervsstyrelsen har i disse tilfælde pligt til at undlade at registrere virksomheden.

Det bemærkes, at kravet om hæderlighed vedrørende strafbare forhold, tilsvarende finder anvendelse på ledelsesmedlemmer og reelle ejere i virksomheder, samt for personer omfattet af § 1, stk. 1, nr. 17, herunder bl.a. skatterådgivere og bogholdere, jf. hvidvasklovens § 57, stk. 2.

Erhvervsstyrelsen har endvidere pligt til at undlade at registrere en virksomhed, hvis et medlem af virksomhedens ledelse har indgivet begæring om rekonstruktionsbehandling, konkurs eller gældssanering, eller er under rekonstruktionsbehandling, konkursbehandling eller gældssanering.

Formålet med bestemmelsen er at minimere risikoen for hvidvask af penge i virksomheden og kanalisering af penge til terrorformål ved at hindre, at personer med bestemmende indflydelse på virksomheden kan anvende virksomheden til kriminelle formål.

Det er som udgangspunkt kun strafbare handlinger, der relaterer sig til ovenstående typer kriminalitet, der indgår i Erhvervsstyrelsens vurdering. Domme for skatteunddragelse vil kunne medføre et afslag på registrering under hensyn til, at skatteunddragelse er omfattet af definitionen af hvidvask. Se afsnit 2.1 om definitioner, hvidvask.

Erhvervsstyrelsen kan inddrage en registrering, hvis virksomheden, et medlem af dens ledelse eller en reel ejer, efterfølgende omfattes af forhold, som ville medføre nægtelse af registrering. Herudover kan Erhvervsstyrelsen inddrage registreringen, hvis nye medlemmer af en virksomheds øverste eller daglige ledelse eller nye reelle ejere ikke giver Erhvervsstyrelsen de oplysninger, der er nødvendige for, at Erhvervsstyrelsen kan vurdere, om disse er omfattet af § 58, stk. 2 eller 3. Erhvervsstyrelsen kan endvidere inddrage registreringen, hvis virksomheden eller personen gør sig skyldig i en grov eller gentagne overtrædelser af hvidvaskloven.

1.4. Undtagelsesbekendtgørelser

1.4.1. Virksomheder, der udøver aktiviteter i bilag 1 i begrænset omfang og valutaveksling

Henvisning til hvidvaskloven: § 1, stk. 4.

Henvisning til 4. hvidvaskdirektiv: Artikel 2, stk. 3.

Henvisning bekendtgørelse: nr. 1358 af 30. november 2017 om hvilke virksomheder og personer, der kan undtages fra lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme (hvidvaskloven).

I bekendtgørelse[1] om hvilke virksomheder og personer, der kan undtages hvidvaskloven, er virksomheder, der udøver finansiel aktivitet i et begrænset omfang, undtaget eller delvist undtaget.

Undtagelsesbekendtgørelsen omfatter kun virksomheder, der er omfattet af hvidvasklovens bilag 1, nr. 1 og 4-12, og valutavekslingsvirksomheder.

Bekendtgørelsen undtager virksomhederne fra visse krav til kundekendskabsprocedurerne, nemlig § 10, nr. 1, og §§ 14 og 18.

[1] Nr. 1358 af 30. november 2017

Undtagelsen er betinget af, at risikoen for hvidvask og finansiering af terrorisme er begrænset, og at aktiviteten udøves lejlighedsvis eller i et meget begrænset omfang.

Af bekendtgørelsen følger seks kumulative betingelser. Det betyder, at alle betingelser skal være opfyldt, for at virksomheden er omfattet af undtagelsen:

1) Den samlede aktivitet skal være begrænset og må ikke overstige følgende beløb på årsbasis:
   a) 70.000 euro for virksomheder, der udøver aktivitet som nævnt i lovens bilag 1, nr. 1 og 4-12.
   b) 15.000 euro for valutavekslingsvirksomheder.
2) Den finansielle aktivitet skal være begrænset på transaktionsbasis og må ikke overstige følgende beløb:
   a) 1.000 euro for aktiviteter nævnt i lovens bilag 1, nr. 1 og 4-12.
   b) 500 euro for valutavekslingsvirksomheder.
3) Den finansielle aktivitet må ikke være virksomhedens eller personens hovedaktivitet, og den må ikke overstige 5 pct. af den pågældende virksomheds eller persons samlede omsætning pr. år.
4) Den finansielle aktivitet skal være accessorisk virksomhed, som har direkte tilknytning til virksomhedens eller personens hovedaktivitet.
5) Virksomhedens eller personens hovedaktivitet må ikke være en aktivitet omfattet af § 1, stk. 1, nr. 14-18 og 20, i hvidvaskloven.
6) Den finansielle aktivitet må kun udbydes til kunder, der er omfattet af virksomhedens hovedaktivitet.

Ad 1) Den første betingelse omfatter virksomhedens samlede omsætning. Denne må ikke overstige tærskelværdien i punkt a eller b.

Ad 2) Den anden betingelse omfatter den enkelte transaktions størrelse. Transaktioner omfatter både transaktioner, der gennemføres på én gang, og transaktioner, der gennemføres som flere transaktioner, der ser ud til at være indbyrdes forbundne.

Udøver virksomheden flere end én af de under nr. 1 eller nr. 2 nævnte aktiviteter, finder det laveste beløb anvendelse. Det betyder, at hvis virksomheden udbyder valutaveksling og en anden aktivitet omfattet af bilaget 1, nr. 1 eller 4-12, f.eks. indlånsvirksomhed, er det tærsklen på 500 euro, der er afgørende for, om den enkelte transaktion overstiger denne. Hvis den overstiger 500 euro, kan virksomheden ikke undtages fra hvidvaskloven.

Ad 3) Denne betingelse omfatter, at aktiviteten ikke må være virksomhedens hovedaktivitet, og at aktiviteten ikke må overstige 5 pct. af virksomhedens samlede omsætning pr. år.

Ad 4) Denne betingelse omfatter, at aktiviteten skal være accessorisk virksomhed, det betyder, at aktiviteten skal have tilknytning til virksomhedens hovedaktivitet.

Ad 5) Denne betingelse omfatter aktiviteter, som er udbudt af advokater eller advokatvirksomheder, når de er omfattet af stk. 1, nr. 14, revisorer og revisionsvirksomheder, ejendomsmæglere og ejendomsmæglervirksomheder, udbydere af tjenesteydelser, udbud af spil og virksomheder, der erhvervsmæssigt leverer samme ydelser som de nævnte personer og virksomheder. Disse kan ikke blive undtaget i henhold til § 2, stk. 2, i bekendtgørelsen.

Ad 6) Denne betingelse omfatter aktiviteter, der ikke udbydes til offentligheden, men alene til virksomhedens kunder, der er kunder i forhold til virksomhedens hovedaktivitet. Betingelsen hænger derfor sammen med, at aktiviteten skal være accessorisk til virksomhedens hovedaktivitet. Aktiviteten må derfor ikke tilbydes andre kunder, end de kunder, som er kunder i forhold til virksomhedens hovedaktivitet.

Virksomheder, der er omfattet af bekendtgørelsen, skal give Finanstilsynet meddelelse om, at de benytter undtagelsen. Meddelelsen skal gives skriftligt hvert år

1.4.2. Lempede krav til kundekendskabsproceduren for udstedere af elektroniske penge

Henvisning til hvidvaskloven: § 21, stk. 2.

Henvisning til 4. hvidvaskdirektiv: Artikel 12, stk. 1.
Henvisning til 5. hvidvaskdirektiv: Artikel 1, stk.1, nr. 7.

Henvisning: bekendtgørelse nr. 311 af 26. marts 2020 om lempede krav til kundekendskabsproceduren efter lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme (hvidvaskloven) for udstedere af elektroniske penge.

Bekendtgørelsen om lempede krav til kundekendskabsproceduren efter hvidvaskloven undtager pengeinstitutter, når disse udsteder elektroniske penge, samt visse andre udstedere af elektroniske penge fra kundekendskabsprocedurerne i § 11, stk. 1, nr. 1-4, og § 14.

Af bekendtgørelsen følger fem kumulative betingelser. Det betyder, at alle betingelser skal være opfyldt, for at virksomheden er omfattet af undtagelsen:

1) betalingsinstrumentet er ikke genopfyldeligt eller har en maksimal månedlig betalingstransaktionsgrænse på 150 euro, som udelukkende kan anvendes i Danmark,
2) det maksimale elektronisk lagrede beløb må ikke overstige 150 euro,
3) betalingsinstrumentet kan udelukkende anvendes til køb af varer eller tjenesteydelser,
4) betalingsinstrumentet kan ikke finansieres med anonyme elektroniske penge, og
5) udstederen skal foretage tilstrækkelig overvågning af transaktioner eller forretningsforbindelser til at kunne opdage usædvanlige eller mistænkelige transaktioner.

Et betalingsinstrument, der ikke er genopfyldeligt, jf. nr. 1, kan f.eks. være et gavekort, hvor det ikke er muligt at indsætte yderligere midler på efter udstedelsen af gavekortet.

Undtagelsen vedrørende gennemførelse af visse dele af kundekendskabsproceduren for udbydere af elektroniske penge gælder ikke ved kontantindløsning eller kontanthævning af pengeværdien af elektroniske penge, hvis det indløste beløb overstiger 50euro, eller hvis der er tale om betalingstransaktioner, der iværksættes via internettet eller lignende, hvor det beløb, der betales, overstiger 50 euro pr. transaktion.

2. Definitioner

2.1. Hvidvask

Henvisning til hvidvaskloven: § 3. Henvisning til 4. hvidvaskdirektiv: Artikel 1, stk. 3. Henvisning til anden lovgivning: Straffelovens § 290 og § 290 a.

"Hvidvask" defineres som:

1) Uberettiget at modtage eller skaffe sig eller andre del i økonomisk udbytte eller midler, der er opnået ved en strafbar lovovertrædelse.
2) Uberettiget at skjule, opbevare, transportere, hjælpe til afhændelse eller på anden måde efterfølgende virke til at sikre det økonomiske udbytte eller midlerne fra en strafbar lovovertrædelse.
3) Forsøg på eller medvirken til sådanne dispositioner.

Der er ikke nogen bagatelgrænse for, hvornår et forhold er omfattet af definitionen af hvidvask.

Definitionen omfatter også dispositioner foretaget af den, der har begået den strafbare lovovertrædelse, som udbyttet eller midlerne hidrører fra. Dette kaldes for selvhvidvask, der i dansk ret ikke straffes efter den almindelige hæleribestemmelse i straffelovens § 290, fordi straf for den bagvedliggende kriminalitet udtømmende gør op med strafansvar for også de senere tilknyttede dispositioner. Selvhvidvask er imidlertid omfattet af bestemmelsen om hvidvask i straffelovens § 290 a, som kun vedrører hvidvask af penge.

Det er ikke afgørende for, om der foreligger hvidvask, om de handlinger, som har frembragt det økonomiske udbytte eller de midler, der skal hvidvaskes blev foretaget i Danmark. Der foreligger således hvidvask, også selv om de handlinger, som har frembragt det økonomiske udbytte eller de midler, der skal hvidvaskes, blev gennemført på en anden medlemsstats eller et tredjelands område.

Hvidvasklovens definition af hvidvask skal forstås i overensstemmelse med straffelovens § 290 om hæleri og § 290 a om hvidvask.

> **§ 290.** For hæleri straffes med bøde eller fængsel indtil 1 år og 6 måneder den, som uberettiget modtager eller skaffer sig eller andre del i udbytte, der er opnået ved en strafbar lovovertrædelse, og den, der uberettiget ved at skjule, opbevare, transportere, hjælpe til afhændelse eller på lignende måde efterfølgende virker til at sikre en anden udbyttet af en strafbar lovovertrædelse, medmindre forholdet er omfattet af § 290 a.
> Stk. 2. Straffen kan stige til fængsel i 6 år, når hæleriet er af særligt grov beskaffenhed navnlig på grund af forbrydelsens erhvervsmæssige eller professionelle karakter eller som følge af den opnåede eller tilsigtede vinding, eller når et større antal forbrydelser er begået.
> Stk. 3. Straf efter denne bestemmelse kan ikke pålægges den, som modtager udbytte til sædvanligt underhold fra familiemedlemmer eller samlever, eller den, der modtager udbytte som normalt vederlag for sædvanlige forbrugsvarer, brugsting eller tjenester.

> **§ 290 a.** For hvidvask straffes med bøde eller fængsel indtil 1 år og 6 måneder den, der konverterer eller overfører penge, som direkte eller indirekte er udbytte af en strafbar lovovertrædelse, for at skjule eller tilsløre den ulovlige oprindelse.
> Stk. 2. Straffen kan stige til fængsel i 8 år, når hvidvasken er af særligt grov beskaffenhed navnlig på grund af forbrydelsens erhvervsmæssige eller professionelle karakter eller som følge af den opnåede eller tilsigtede vinding, eller når et større antal forbrydelser er begået.

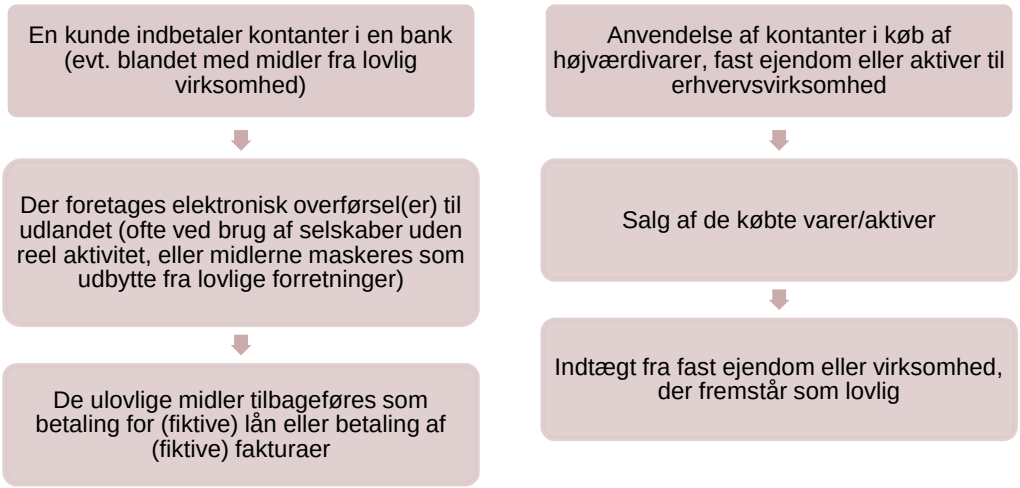
Ad 1) Karakteristisk for hvidvasktransaktioner og aktiviteter er, at de har til formål at skjule midlernes oprindelse gennem en sløringsproces. Det er ikke et krav, at processen skal være kompliceret, og i mange tilfælde kan kunden have deltaget i en mindre del af processen.

Ad 2) Strafbar lovovertrædelse omfatter både overtrædelser af straffeloven og af speciallovgivningen samt tilsvarende forhold begået i udlandet, for hvilke der er hjemlet strafansvar. Skatteunddragelse er overtrædelse af skatte-, told- eller afgiftslovgivningen, hvorved der opnås eller kan opnås uberettiget vinding.

Strafferetligt er hvidvask dækket af straffelovens §§ 290 og 290 a, der vedrører udbytte fra alle strafbare forhold.

Ad 3) Hvidvask defineres også som forsøg på eller medvirken til sådanne dispositioner som nævnt i nr. 1 og 2. Forsøg og medvirken skal forstås i overensstemmelse med straffelovens 4. kapitel.

Nedenfor fremgår eksempler på, hvornår hvidvask kan forekomme:



2.2. Finansiering af terrorisme

Henvisning til hvidvaskloven: § 4.

Henvisning til 4. hvidvaskdirektiv: Artikel 1, stk. 5.

Henvisning til anden lovgivning: Straffelovens §§ 114 og 114 b.

"Finansiering af terrorisme" defineres i hvidvasklovens § 4. Definitionen er overensstemmende med definitionen i straffelovens § 114 b, for så vidt angår handlinger omfattet af straffelovens § 114, der definerer terrorisme.

Straffelovens § 114 b definerer finansiering af terrorisme som de situationer, hvor der

1) direkte eller indirekte yder økonomisk støtte til,
2) direkte eller indirekte tilvejebringer eller indsamler midler til eller
3) direkte eller indirekte stiller penge, andre formuegoder eller finansielle eller andre lignende ydelser til rådighed for en person, en gruppe eller en sammenslutning, der begår eller har til hensigt at begå handlinger omfattet af § 114 eller § 114 a.

2.3. Kontantforbud

Henvisning til hvidvaskloven: § 5.

Henvisning til 4. hvidvaskdirektiv: Artikel 2, stk. 1, nr. 3, litra e, og artikel 11, litra d, i 4.

Virksomheder, der ikke er omfattet af hvidvasklovens § 1, stk. 1, er omfattet af et kontantforbud, som er fastsat i hvidvasklovens § 5.

Det betyder, at erhvervsdrivende, som ikke er omfattet af hvidvasklovens regler, ikke må modtage kontantbetalinger på 50.000 kr. eller derover, hvad enten betalingen sker på én gang eller som flere betalinger, der er eller ser ud til at være indbyrdes forbundet.

Med "kontantbetalinger" skal forstås betaling med kontanter, dvs. fysiske penge. Kontantforbuddet omfatter derfor ikke f.eks. betaling med et betalingskort, eller at en kunde indbetaler penge til sin egen konto og herefter overfører pengene til forhandlerens konto.

Forbuddet omfatter salg, der sker erhvervsmæssigt. Forbuddet omfatter ikke kun en erhvervsdrivendes salg af genstande, men også f.eks. erhvervsdrivendes levering af tjenesteydelser og salg af fast ejendom.

Forbuddet gælder, selvom den erhvervsdrivende modtager kontantbetalinger på 50.000 kr. eller derover uden for landets grænser.

Erhvervsdrivende, der ikke er omfattet af § 1, stk. 1, er derfor kun underlagt kontantforbuddet i § 5 og forbuddet mod 500-euro sedler, se afsnit 2.5.

Forbuddet har baggrund i, at store betalinger med kontanter øger risikoen for hvidvask og finansiering af terrorisme.

2.3.1. Indbyrdes forbundne betalinger

Forbuddet omfatter ikke kun betalinger, der sker på én gang, men også betalinger, der ser ud til at være indbyrdes forbundet, hvis det samlede beløb udgør 50.000 kr. eller derover. Dette er for at forhindre, at forbuddet kan omgås.

Det betyder ikke, at løbende ydelser i sig selv er om omfattet af forbuddet, men hvis betalingen af f.eks. leje af et hus eller en bil eller betaling ved f.eks. levering af vand og varme for en enkelt periode udgør 50.000 kr. eller derover, så vil betalingen blive omfattet af kontantforbuddet.

Hvis der f.eks. er tale om ratevis betaling, eksempelvis i forbindelse med køb af en løsøregenstand eller en fast ejendom eller i forbindelse med betaling for en entrepriseydelse eller en rejse, vil de enkelte rater være indbyrdes forbundne, og kontantforbuddet vil dermed ramme tilfælde, hvor den samlede betaling udgør 50.000 kr. eller derover. Såfremt en række kontantbetalinger eksempelvis vedrører samme faktura, og betalingerne tilsammen udgør 50.000 kr. eller derover, vil kontantforbuddet være overtrådt.

Højesteret har i dom af 24. april 2019 i sag 174/2018 (U 2019.2445 H) taget stilling til, hvornår betalinger kan anses for at være indbyrdes forbundne. Ifølge dommen vil det være i strid med forbuddet, når en erhvervsdrivende på én gang modtager kontant betaling på 50.000 kr. eller derudover, uanset om betalingen dækker køb af en eller flere genstande, og uden hensyn til, om der måtte være indbyrdes forbindelse mellem de enkelte køb. Endvidere er det også uden betydning, om der er sket særskilt fakturering af de enkelte køb.

Det vil efter Finanstilsynets opfattelse være i strid med forbuddet, hvis flere betalinger, der samlet set er på 50.000 kr. eller derover, er eller ser ud til at være indbyrdes forbundet. Disse betalinger behøver ikke ske på én gang, når betalingerne dækker flere forskellige varer eller tjenesteydelser, som er købt ved samme aftale. Betingelsen om indbyrdes forbindelse kan herudover være opfyldt, hvis betalingen dækker flere købsaftaler, som er sammenhængende, f.eks. i kraft af et samhandelsmønster eller aftale om rabat.

Det følger endvidere efter Finanstilsynets opfattelse af dommen, at såfremt der gennemføres en handel på under 50.000 kr., og samme kunde vender tilbage senere samme dag uden forbindelse eller sammenhæng til dagens første køb og foretager endnu et køb, hvorved summen af kontantbetalinger samme dag fra samme kunde overstiger 50.000 kr., vil der ikke være tale om en overtrædelse af kontantforbuddet.

2.4. Falske penge

Henvisning til hvidvaskloven: § 6.

Henvisning til anden lovgivning: Artikel 6, stk. 1, i Rådets forordning 2009/44/EF af 18. december 2008 om ændring af forordning 2001/1338/EF om fastlæggelse af de foranstaltninger, der er nødvendige for at beskytte euroen mod falskmøntneri, der indeholder en lignende forpligtelse i forhold til eurosedler og euromønter.

Virksomheder, der deltager i håndtering og udlevering af pengesedler og mønter til offentligheden, har pligt til at tage alle sedler og mønter, som de ved eller har grund til at tro er falske, ud af omløb og overgive disse til politiet. Det samme gør sig gældende for virksomheder, hvis aktivitet består i at veksle pengesedler og mønter i forskellig valuta.

Kravet i hvidvaskloven omfatter ikke sedler og mønter i euro, fordi et tilsvarende krav for eurosedler og euromønter er fastsat i en forordning om fastlæggelse af de foranstaltninger, der er nødvendige for at beskytte euroen mod falskmøntneri. I forordningen er der bl.a. et krav til de omfattede virksomheder om, at de skal sikre, at eurosedler og euromønter, som virksomheden har modtaget, og som virksomheden vil bringe i omløb igen, kontrolleres med henblik på ægthed, og at virksomheder påser, at falske eurosedler og euromønter afsløres og overgives til de kompetente nationale myndigheder. Se henvisning i boksen ovenfor.

Kravet i hvidvaskloven er derfor fastsat med henblik på at også andre typer valuta end euro, herunder danske kroner omfattes af pligten til straks at overgive formodede falske sedler og mønter til politiet.

2.5. Forbud mod anvendelse af 500-eurosedler

Henvisning til hvidvaskloven: § 6 a.

Virksomheder og personer er omfattet af et forbud mod anvendelse af 500-eurosedler, som er fastsat i hvidvasklovens § 6 a. Forbuddet mod anvendelse af 500-eurosedler omfatter alle virksomheder og personer og er dermed ikke kun rettet mod virksomheder, der er omfattet af hvidvaskloven. Forbuddet gælder, uanset om anvendelsen sker som led i udførelse af erhvervsvirksomhed eller i privat øjemed.

Forbuddet har den betydning, at 500-eurosedler ikke må anvendes, herunder udleveres, indleveres, veksles, bruges som betalingsmiddel eller overdrages, i Danmark. Det er udelukkende anvendelse af 500-eurosedler i Danmark, der er omfattet af forbuddet. Bestemmelsen har ingen betydning for anvendelse af 500-eurosedler i andre lande end Danmark. Selve besiddelsen af 500-eurosedler er ikke omfattet af forbuddet, og det er således ikke ulovligt at være i besiddelse af 500-eurosedler, f.eks. til brug for ophold i udlandet med legitime formål som ferie, forretningsrejse eller lignende.

Anvendelse
Ved anvendelse forstås enhver handling, hvori en eller flere 500-eurosedler overgår fra én juridisk eller fysisk person til en anden juridisk eller fysisk person, uanset omstændighederne omkring overdragelsen.

Det vil være en anvendelse i strid med forbuddet, i tilfælde hvor et pengeinstitut hæver et beløb i kroner på en konto svarende til værdien af en 500-euroseddel og derefter udleverer en 500-euroseddel til kunden.

Ligeledes vil det være i strid med forbuddet, hvis en kunde indleverer en 500-euroseddel til et pengeinstitut med henblik på, at værdien af 500-eurosedlen f.eks. skal indsættes på kundens konto. Modtagelse og efterfølgende veksling af en 500-euroseddel til andre seddelværdier eller til anden valuta i blandt andre pengeinstitutter og valutavekslingsvirksomheder vil også være en anvendelse i strid med forbuddet.

Enhver betaling med en 500-euroseddel vil være anvendelse i strid med forbuddet, herunder f.eks. betaling med 500-eurosedler i supermarkeder og andre virksomheder. Køb mellem ikke-erhvervsdrivende, hvor betalingen sker med en 500-euroseddel, er ligeledes omfattet af forbuddet. Det er således både overdragelse og modtagelse af 500-eurosedler i forbindelse med salg af et aktiv mellem to private parter der er omfattet, ligesom en overdragelse af en 500-euroseddel i form af f.eks. gave vil være en overdragelse i strid med forbuddet, både i relation til at give og modtage 500-eurosedlen.

Forbuddet gælder dog ikke i de tilfælde, hvor der sker en overdragelse af 500-eurosedler i forbindelse med boskifte, f.eks. dødsbo eller konkursbo, og udlodning af midler heraf.

Del 2 – Risikovurdering og risikostyring

3. Risikovurdering

Henvisning til hvidvaskloven: § 7, stk. 1. Henvisning til 4. hvidvaskdirektiv: Artikel 8, stk. 2, 1. pkt.

Virksomheden skal foretage en risikovurdering af sin iboende risiko for hvidvask og finansiering af terrorisme. Med "iboende risiko" menes i denne forbindelse den risiko, der er for, at virksomheden kan blive misbrugt til hvidvask eller terrorfinansiering. Der tages i første omgang ikke højde for de foranstaltninger, som virksomheden har iværksat for at begrænse risikoen.

Risikovurderingen skal foretages med udgangspunkt i virksomhedens forretningsmodel og skal klarlægge, hvilke forretningsområder i virksomheden, der er eksponeret for hvidvask- og/eller terrorfinansieringsrisici, hvor store disse risici er, og hvordan de kan manifestere sig. Med en virksomheds forretningsmodel menes i denne forbindelse en kombination af:

1) de kundetyper, som virksomheden har,
2) de produkter, tjenesteydelser og transaktioner, som virksomheden tilbyder kunderne,
3) virksomhedens leveringskanaler til at tilbyde produkterne og/eller udføre tjenesteydelserne,
4) lande eller geografiske områder, hvor forretningsaktiviteterne udøves,
5) virksomhedens organisation og
6) virksomhedens koncernstruktur.

Risikovurderingen danner grundlag for, at virksomheden kan vurdere, hvilke forretningsområder der skal prioriteres for at undgå, at virksomheden kan misbruges til hvidvask og finansiering af terrorisme, samt hvilke operationelle forretningsgange der skal iværksættes for de enkelte forretningsområder. Risikovurderingen skal dermed danne grundlaget for, hvordan virksomheden tilrettelægger sine politikker, forretningsgange og kontroller, jf. afsnit 2 nedenfor.

Konkret betyder den risikobaserede tilgang, at virksomheden skal identificere og vurdere og forstå den iboende risiko for, at virksomheden kan blive misbrugt til hvidvask eller finansiering af terrorisme. Virksomheden kan dermed bruge sine ressourcer på områder, hvor risikoen er størst.

Risikovurderingen skal bygge på relevante dokumenter, herunder f.eks. den supranationale og den nationale risikovurdering, erfaringer opnået via medier og samarbejde med myndigheder mv. og ikke mindst virksomhedens egne erfaringer fra kundeovervågning etc. På Finanstilsynets hjemmeside findes links til nationale og supranationale risikovurderinger og en række andre links til dokumenter, der i øvrigt med fordel kan indgå i risikovurderingen.[2]

Risikovurderingens indhold og omfang skal være proportional med virksomhedens risikofaktorer, virksomhedens størrelse og forretningsomfang. Risikovurderingen skal løbende opdateres, så den afspejler

[2] https://www.finanstilsynet.dk/Tilsyn/Information-om-udvalgte-tilsynsomraader/Hvidvask/Links-vedr-hvidvask

virksomhedens aktuelle risikoprofil. Virksomheden skal vurdere, hvornår risikovurderingen skal opdateres. Som udgangspunkt skal risikovurderingen opdateres en gang årligt. Derudover skal den opdateres, når virksomhedens forretningsmodel ændres væsentligt, eller ændringer i nye nationale eller supranationale vurderinger vurderes at kunne påvirke risikovurderingerne, jf. også afsnit 1.4. om undtagelsesbekendtgørelser.

Nedenstående figur illustrerer processen fra konstateringen af den iboende risiko til konstateringen af den risiko, der er tilbage, når virksomheden har truffet beslutning om politikker og forretningsgange mv. Den risiko, der er tilbage, efter at de risikobegrænsende foranstaltninger er taget med i vurderingen, kan betegnes den residuale risiko. Der henvises til beskrivelsen nedenfor.

Som figuren nedenfor illustrerer, er der i en virksomheds forretningsmodel en iboende risiko for at blive misbrugt til hvidvask eller terrorfinansiering. Denne kan ændres, hvis virksomheden beslutter at ændre forretningsmodellen, f.eks. hvis virksomheden beslutter at ændre sammensætningen af kundetyper, produkttyper eller leveringskanaler mv. Hvis virksomheden på denne vis vælger overordnet at fjerne nogle risikofaktorer fra sin forretningsmodel, kan det påvirke den iboende risiko i nedadgående retning. Det omvendte gælder, hvis virksomheden som følge af nye produkter eller nye kundetyper får nye eller højere risikofaktorer. Hvis og når forretningsmodellen er ændret og ligger fast, er det den nye aktuelle iboende risiko, som virksomheden skal lægge til grund for udarbejdelsen af sine forretningsgange, politikker og kontroller.

Virksomhedens politikker, forretningsgange og kontroller er virksomhedens risikobegrænsende tiltag, dvs. det virksomheden gør for at få en effektiv forebyggelse, begrænsning og styring af risici for hvidvask og finansiering af terrorisme. Den residuale risiko, som virksomheden løber for at blive misbrugt til hvidvask og finansiering af terrorisme, er den risiko, der kan være tilbage, selv med en effektiv forebyggelse, begrænsning og styring.

Risikovurderingen behøver ikke at være kompleks eller omfattende, særligt ikke for virksomheder med en enkel forretningsmodel, f.eks. virksomheder, som kun udbyder få og simple produkter. Det væsentlige er, at virksomheden kommer omkring alle risiciene. Målet er, at vurderingen kan fungere som et operationelt og anvendeligt værktøj, der skaber et overblik og en forståelse for virksomhedens iboende risici og for, hvilke tiltag der er nødvendige for at begrænse risiciene.

En risikovurdering kan udarbejdes af en central enhed i en koncern/virksomhed med filialetablering i et eller flere lande, for eksempel moderselskabet, men det er et krav, at risikovurderingen tilpasses den enkelte juridiske enheds eller filials forhold, herunder den juridiske enheds eller filials forretningsmodel og etableringslandets risikoforhold og regler. Risikovurderingen skal endvidere underbygges af oplysninger, som er relevante for den pågældende juridiske enhed eller filial i koncernen. Se afsnit 5 vedrørende koncerner.

3.1. Metode og dokumentation

Virksomheden skal identificere sine risikofaktorer og vurdere hver enkelt af disse og den sammenhæng, der er mellem risikofaktorerne. Ved vurderingen skal virksomheden fastlægge, i hvilken grad de identificerede risikofaktorer påvirker den overordnede iboende risiko. Virksomheden skal hermed ud fra en holistisk betragtning konkret vurdere hvor og i hvilken grad, disse faktorer kan bevirke, at virksomheden kan blive misbrugt til hvidvask eller finansiering af terrorisme.

En måde, hvorpå virksomheden kan vurdere sine samlede risici, kan være at vægte de enkelte risikofaktorer. Vurderingen af risikofaktorerne skal tage udgangspunkt i risikoen separat for hvidvask og for finansiering af terrorisme, da disse kan være forskellige. Virksomheden skal dermed i sin risikovurdering have forholdt sig til begge forhold. Eksempelvis kan et produkt have begrænset risiko i forhold til hvidvask men øget risiko i forhold til finansiering af terrorisme. Et eksempel er små pengeoverførsler til udlandet. Små enkeltvise pengeoverførsler vil som udgangspunkt ikke udgøre en stor risiko for hvidvask af penge, da der er tale om små beløb. Finansiering af terrorisme er derimod kendetegnet ved, at det kan være små overførsler, der foretages til lande eller geografiske områder, hvor der foregår terroraktivitet. Det illegitime formål med overførslerne er lettere at skjule, når det er små beløb. Det er derfor vigtigt, når virksomheden vurderer sine risici, at virksomheden holder sig for øje, at risikofaktorerne for henholdsvis hvidvask og finansiering af terrorisme ikke altid har samme karakter.

Virksomheden skal indsamle tilstrækkelige oplysninger til at kunne identificere alle virksomhedens risikofaktorer. Hvidvasklovens § 7, stk. 1, opregner risikofaktorer, som virksomheden skal tage i betragtning i sin samlede vurdering. Hvidvasklovens oplistning af risikofaktorer er ikke udtømmende, hvorfor virksomheden selv i fornødent omfang kan identificere andre relevante risikofaktorer. Virksomheden kan også i sin vurdering af de enkelte risikofaktorer konstatere, at nogle risikofaktorer ikke er relevante for virksomheden, og at virksomheden derfor har en meget begrænset eller slet ingen iboende risiko i forhold til disse konkrete risikofaktorer. Det er derfor relevant, at virksomheden sammenholder disse begrænsede risici med andre risikofaktorer i virksomheden for at vurdere, hvorvidt risikofaktorerne kan påvirke hinanden.

Virksomheden skal dokumentere sin vurdering af risikofaktorerne. Dokumentationen skal knyttes til virksomhedens forretningsmodel, som også danner grundlaget for vurderingen. Risikovurderingen kræver derfor en tilstrækkelig grundig analyse af forretningsmodellen. Virksomheden kan lægge sin egen viden og erfaring fra indsamlede data, kundekendskab, efterspurgte produkter mv. til grund som en del af dokumentationen for den overordnede vurdering. Endvidere skal dokumentationen for risikovurderingen

tage udgangspunkt i virksomhedens overvejelser og beslutninger på baggrund af den supranationale og nationale risikovurdering og/eller i andre relevante former for dokumentation på området, f.eks. information udsendt af FATF, EBA og brancheorganisationer samt landerapporter om f.eks. korruption, informationer fra troværdige offentlige eller kommercielle kilder og vejledningens del 2 vedrørende reglerne om risikovurdering og risikostyring på hvidvaskområdet, jf. det indledende afsnit. Virksomheden kan få inspiration til relevant materiale på Finanstilsynets hjemmeside.[3]

Dokumentationen kan ske ved, at virksomheden gemmer alle oplysninger og dokumenter, som virksomheden lægger til grund for de vurderinger, den foretager, samt noterer de konklusioner, der er foretaget. Virksomheden kan også dokumentere i interne oplysninger, observationer, dokumentationer mv. såvel som i nationale eller internationale vurderinger, rapporter, statistiker mv. Virksomheden kan f.eks. i sin vurdering af, hvorledes et produkt indebærer en risiko for hvidvask eller finansiering af terrorisme, benytte den supranationale risikovurdering af den specifikke produkttype og hermed vurdere og dokumentere produktets indflydelse på virksomhedens risikoprofil.

3.2. Risikofaktorer

Henvisning til hvidvaskloven: § 7, stk. 1, 1. og 2. pkt. Henvisning til 4. hvidvaskdirektiv: Artikel 8, stk. 1.

Når virksomheden vurderer sine risikofaktorer, kan virksomheden bl.a. søge hjælp til at foretage vurderingerne i hvidvasklovens bilag 2 og 3, som opremser situationer, der kan være indikation for henholdsvis begrænset og høj risiko. Bilagene er ikke udtømmende. Virksomheden kan herudover vurdere sine risikofaktorer som anført nedenfor. Uanset om en risikofaktor som udgangspunkt er høj eller lav, skal virksomheden foretage sine egne vurderinger og overvåge kunderne i overensstemmelse med hvidvasklovens regler.

3.2.1. Kundetyper

Virksomheden skal vurdere sine kundetyper som en af virksomhedens risikofaktorer. Risikovurderingen efter § 7 baseres på virksomheden og dennes overordnede risikoprofil, hvorimod risikovurderingen efter § 11 foretages på virksomhedens enkelte kunder. Se afsnit 13 om risikovurdering – kundekendskabsprocedurer. Virksomheden kan inddrage faktorer og overordnede erfaringer fra virksomhedens § 11-vurderinger i sin overordnede risikovurdering, men det er vigtigt, at virksomheden sondrer mellem bestemmelsernes forskellige udgangspunkter og derfor foretager selvstændige vurderinger ud fra begge bestemmelser. Risikovurderingen i § 7 skal derfor ikke baseres på konkrete vurderinger af enkeltkunder.

Vurderingen kan overordnet tage udgangspunkt i, i hvilket omfang kundetyperne er fysiske eller juridiske personer og herefter i kundetypernes professionelle og erhvervsmæssige aktiviteter, omdømme og adfærd og for juridiske personer også deres reelle ejere. Vurderingen skal ske på et overordnet plan. Virksomheden skal derfor til brug for § 7-vurderingen f.eks. ikke vurdere den enkelte kunde eller reelle ejer. Virksomheden skal f.eks. vurdere, i hvilken grad en kundeportefølje af juridiske personer med reelle ejere placeret i udlandet påvirker den overordnede risikoprofil.

[3] https://www.finanstilsynet.dk/Tilsyn/Information-om-udvalgte-tilsynsomraader/Hvidvask/Links-vedr-hvidvask

Hvis kunderne er juridiske personer, er det relevant at se på virksomhedstyperne, og på hvilke regler disse er underlagt. Eksempelvis kan børsnoterede selskaber generelt betragtes som begrænset risiko bl.a. med baggrund i, at børsnoterede selskaber er undergivet en særlig oplysningspligt i overensstemmelse med EU-retten, hvorimod pengeoverførselsvirksomheder eller valutavekslingsvirksomheder generelt betragtes som højere risiko.

Flere faktorer er relevante, når virksomheden foretager analysen af sit kundesegment som en risikofaktor. Det kan bl.a. vurderes, hvorvidt en kundetype:

1) har forbindelse til en sektor, der er forbundet med høj risiko for hvidvask eller terrorfinansiering,
2) har forbindelse til en sektor, hvor der er store kontantbeløb i omløb, eller
3) omfatter politisk eksponerede personer.

Ved en analyse af kundetyper kan virksomheden i øvrigt lægge vægt på:

1) Formålet med etableringen af virksomheden.
2) Om kundetypen i anden lov er underlagt oplysningskrav, som sikrer større gennemsigtighed omkring virksomhedstypen.
3) Om virksomheden har kundetyper med transaktioner i/til/fra et land, som vurderes til ikke at have effektive regler til bekæmpelse af hvidvask og finansiering af terrorisme eller om virksomheden har kundetyper, der er virksomheder etableret i et sådant land.
4) Om virksomheden har kundetyper, der er virksomheder etableret i et land med højere korruptionsniveau.

Ovenstående undersøgelsespunkter er en inspiration til risikovurderingen og er ikke udtryk for hverken en obligatorisk eller udtømmende liste. Virksomheden er ansvarlig for at fastlægge de nødvendige undersøgelsespunkter.

3.2.2. Produkter, tjenesteydelser og transaktioner

Når virksomheden skal risikovurdere sine produkter, tjenesteydelser og/eller transaktioner, kan virksomheden bl.a. afdække, om de kan tænkes at blive brugt til hvidvask eller finansiering af terrorisme, herunder:

1) i hvilken grad produkterne, tjenesteydelserne og transaktionerne er egnede til at fremme anonymitet,
2) i hvilken grad produkterne, tjenesteydelserne og transaktionerne er komplekse og
3) produkterne, tjenesteydelserne og transaktionernes værdi og størrelse.

Ved fastlæggelse af om produktet, tjenesteydelsen eller transaktionens er egnet til at fremme anonymitet, kan virksomheden vurdere, i hvilket omfang modtageren, har mulighed for at skjule sin identitet. Dette kan f.eks. være tilfældet, hvis produktet eller tjenesteydelsen angår køb og/eller salg af ihændehaveraktier eller transaktioner uden direkte kontakt eller kendskab til den endelige modtager af værdipapirer eller kontante midler mv.
Ved produkternes, tjenesteydelsernes og transaktionernes kompleksitet kan virksomheden vurdere:

1) om transaktionerne med produktet/tjenesteydelsen involverer flere parter eller flere jurisdiktioner
2) om produkterne, tjenesteydelserne eller transaktionerne giver kunderne mulighed for at modtage betalinger fra tredjemand, og at dette kan ske fra en ukendt eller ikke-associeret tredjemand, og
3) om der kan foretages ekstraordinære betalinger, som ikke er regelmæssige, og som ikke beror på et fast mønster, f.eks. en førtidig indfrielse af et lån.

Ved fastlæggelse af produkternes, tjenesteydelsernes og transaktionernes værdi og størrelse kan virksomheden vurdere, i hvilket omfang produkterne eller tjenesteydelserne angår kontanthåndteringer/kontante betalinger og i hvor stor grad, der er høje transaktionsværdier/mange transaktioner eller mulighed herfor, f.eks. om der er bestemt et præmieniveau eller et loft, som kan begrænse risikoen.

Produkter, tjenesteydelser eller transaktioner, der som udgangspunkt er af begrænset risiko, kan eksempelvis være:

1) Livsforsikringer med en årlig lav præmie.
2) Pensionsordninger til ansatte, hvor bidragene betales direkte via fradrag i lønnen.
3) Porteføljepleje, hvor der alene er fuldmagt til at handle på vegne af kunden, og hvor kunden har konto eller depot i en anden finansiel virksomhed.
4) Produkter, hvor risikoen kontrolleres af andre faktorer, f.eks. gennemsigtighed i forhold til ejerskab. Eksempler på dette er realkreditlån samt porteføljeadministration og –rådgivning.

For yderligere eksempler se bilag 2 til hvidvaskloven.

Produkter, tjenesteydelser eller transaktioner, der potentielt er af høj risiko, kan eksempelvis være:

1) Private banking, wealth management eller lignende, fordi det er en produkttype, der normalt tilbydes kunder med høj formue. Det kan også være en betegnelse for et kundesegment, der spænder fra standardprodukter til kunder med skræddersyede produkter med komplekse selskabsprodukter.
   Faktorer inden for private banking, wealth management eller lignende, der kan være forbundet med øget risiko, kan være hyppige indskud og udtræk af midler. Det kan således være lettere at skjule et illegitimt beløb i en stor formue, og erfaringsmæssigt søges sorte penge ofte vasket hvide ved at omdanne dem til afkast af værdipapirer. Endvidere er det en produkttype, der ofte kan skabe meget tæt kontakt og loyalitet mellem rådgiveren og kunden, som kan besværliggøre den øgede overvågning, som et risikoprodukt kræver. Det vil eksempelvis også være komplekst i de tilfælde, hvor det skræddersys til den konkrete kunde og angår store transaktionssummer. For denne produkttype vil det derfor bl.a. vil være relevant at sikre et kendskab til midlernes oprindelse og til kundens formål med de ønskede transaktioner og investeringer mv.
2) Enkeltstående pengeoverførsler eller pengeoverførsler, hvor der ikke etableres et reelt kundeforhold og dermed ikke opnås et godt kundekendskab eller kundeovervågning.
   Misbrug af produktet kan bl.a. sløres ved at foretage flere små overførsler, som enkeltvis ikke ser mistænkelige ud. Erfaringsmæssigt er denne produkttype benyttet til finansiering af terrorisme.
3) Valutaveksling, fordi det er et produkt, hvor der oftest ikke indgås en fast forretningsforbindelse, og der er derfor ikke sikret et godt kendskab til kundens formål og til midlernes oprindelse. Derudover er der tale om transaktioner, hvor der ofte indgår kontanter.
   Valutaveksling anvendes erfaringsmæssigt til terrorfinansiering ved at veksle danske kroner til euro eller amerikanske dollars, som sendes fysisk til brug for terrorfinansiering.
4) Produkter og tjenesteydelser, der anvender nye teknologier, og hvor der endnu ikke er erfaring med disse og derfor heller ikke et tilstrækkeligt kendskab til de potentielle risici.

For yderligere eksempler henvises til bilag 3 til hvidvaskloven, ligesom de nationale og supranationale risikovurderinger indeholder angivelser af, hvordan hvidvask og finansiering af terrorisme kan ske, og hvor risiciene er store.

3.2.3. Leveringskanaler

Virksomhedens transaktions- og leveringskanaler har også afgørende betydning for virksomhedens risikovurdering. I identifikationen af virksomhedens leveringskanaler kan virksomheden overordnet klarlægge:

1) hvordan forretningsforbindelsen med kunderne bliver indgået og
2) hvordan virksomheden leverer produktet, tjenesteydelsen eller transaktionen til kunderne.

Virksomheden kan endvidere vurdere:

1) i hvilket omfang forretningsforbindelsen består uden fysisk kontakt med kunden eller modparter og uden f.eks. digitale sikkerhedsforanstaltninger. En fysisk kontakt med en juridisk person kan eksempelvis være, når den juridiske person repræsenteres af en anden person med prokura/fuldmagt,
2) hvilke eksterne parter/modparter der er behov for, for at kunne levere produktet eller udføre tjenesteydelsen og
3) eventuelle introducerende parter eller formidlere, virksomhedens brugere og karakteren af deres forbindelse til virksomheden.

Virksomheden kan f.eks. vurdere, om kunden er introduceret af en tredjemand, og hvad virksomhedens kendskab er til denne, herunder om tredjemand har effektive procedurer til bekæmpelse af hvidvask og finansiering af terrorisme, er baseret inden for EU og er underlagt et effektivt tilsyn i det land, er underlagt regler om forebyggelse af hvidvask eller finansiering af terrorisme.

Leveringskanaler, der isoleret set kan indikere en begrænset risiko, kan eksempelvis være:

1) En forretningsforbindelse, der er indgået med fysisk kontakt med kunden eller med elektroniske løsninger, der er stor tillid til.
2) Almindeligt indlån, hvor der ikke er en ekstern leveringskanal, dvs. hvor indskud sker som indbetaling af løn og træk sker via normale betalingstransaktioner.
3) Realkreditlån, hvor formidlingen af kundeforholdet til realkreditinstituttet sker via kundens pengeinstitut.

For yderligere eksempler se bilag 2 til hvidvaskloven.

3.2.4. Lande og geografiske områder

Virksomheden skal vurdere de risici, som kan være forbundet med lande eller geografiske områder, hvortil virksomheden har en tilknytning. Hvor virksomheden har positiv viden om et kundesegment eller kunders reelle ejere i relation til lande og geografiske forhold, kan virksomheden eksempelvis inddrage:

1) i hvilket land kundetyperne og/eller de reelle ejere er baseret
2) i hvilket land kundetyperne og/eller de reelle ejere har deres forretninger og
3) i hvilke lande kundetyperne har relevante personlige eller forretningsmæssige forbindelser.

Virksomheden skal ikke i den overordnede risikovurdering vurdere konkrete kunder, men virksomheden skal inddrage sin viden om sine kundetyper og kunders reelle ejere. Har virksomheden f.eks. et kundesegment, hvor de reelle ejere er placeret i højrisikolande, bør dette indgå i risikovurderingen af virksomhedens risikofaktorer i relation til lande og geografiske områder.

Det er således ikke nødvendigt, at virksomheden undersøger enkelte kunder eller reelle ejere for at kunne udarbejde virksomhedens risikovurdering.

I forbindelse med kendskab til virksomhedens kundetyper og analysen af, hvilke lande kundetyperne er baseret i eller har deres personlige eller forretningsmæssige forbindelser i, kan virksomheden vurdere de geografiske forhold, eksempelvis:

1) om landet har tilstrækkelige regler, der forebygger og bekæmper hvidvask og finansiering af terrorisme
2) om landet har en effektiv tilsynsmyndighed på området
3) om kunder har relationer til et land eller geografisk område, hvor der genereres penge med store hvidvaskrisici eller med mange forbrydelser på området
4) om der i relation til kunder sendes penge til lande, hvor der vides at være terroraktiviteter
5) om virksomheden har udenlandsk politisk eksponerede personer som kunder, og hvorledes disses geografiske tilknytning kan vurderes at være tegn på en øget risiko for hvidvask og finansiering af terrorisme
6) om virksomheden har kunder, der fremgår af EU's sanktionslister.

Når virksomheden skal vurdere landets regler og tilsynsmyndigheders effektivitet, kan virksomheden bl.a. anvende FATF's rapporter, sorte og grå lister, rapporter udarbejdet af bl.a. FSRB og OECD, Transparency Internationals korruptionsliste m.fl.[4]

3.2.5. Sektorspecifikke eksempler

Dette afsnit indeholder nogle konkrete eksempler på risikovurderinger. Eksemplerne skal støtte virksomhederne i deres risikovurdering, men det er virksomhederne, der selv skal foretage en konkret vurdering. Eksemplerne er udtryk for situationer, der indebærer en risiko, herunder både høj og begrænset risiko. De er relevante, fordi også en begrænset risiko er grundlag for, at virksomheden skal foretage en konkret risikovurdering.

Fondsmæglervirksomheder:
For fondsmæglervirksomheder kan nedenstående eksempel illustrere en konkret vurdering.

Fondsmæglere skal vurdere de produkter eller tjenesteydelser, som de udbyder. For fondsmæglere er lov om finansiel virksomheds bilag 4 og 5 derfor relevant i identifikationen af disse. Flere produkter og tjenesteydelser vil isoleret set indebære en begrænset risiko, og derfor skal de vurderes i forhold til de andre risikofaktorer, herunder fondsmæglerens kundetyper og eventuelle geografiske tilknytninger. F.eks. kan en fondsmægler udbyde skønsmæssig porteføljepleje, hvor transaktionerne alene sker via et pengeinstitut, hvor fondsmægleren har tilstrækkelig tillid til, at der er effektive procedurer til bekæmpelse af hvidvask og finansiering af terrorisme. Fondsmægleren kan også udbyde skønsmæssig porteføljepleje, hvor transaktionerne sker via en kreds af værdipapirhandlere, men hvor samtlige transaktioner afvikles direkte på kundens konto og depot i kundens pengeinstitut efter instruks fra fondsmægleren. Disse produkter vil som udgangspunkt vurderes til at indebære en begrænset risiko, men hvis produktet udbydes til PEP'er eller andre højt profilerede kunder eller udenlandske kunder, vil selve kundetypen kunne medføre en højere risiko, hvorfor der vil være behov for kundekendskabsprocedurer, der sikrer et godt og ajourført kendskab til kunderne og til midlernes oprindelse.

Finansiel leasing:
For virksomheder, der udbyder finansiel leasing, kan nedenstående eksempel illustrere en konkret vurdering.

[4] https://www.finanstilsynet.dk/Tilsyn/Information-om-udvalgte-tilsynsomraader/Hvidvask/Risikovurdering-af-lande

Ved finansiel leasing af biler skal virksomheden være opmærksom på, at denne type produkt/tjenesteydelse kan misbruges til finansiering af terrorisme. En person kan lease en bil uden intention om at levere den tilbage og herefter melde bilen stjålet med det formål f.eks. at benytte et salg af bilen til finansiering af terrorisme.

Der kan også være tale om, at personen beholder bilen, for at en terrororganisation kan benytte den i kampe i konfliktzoner eller til terrorangreb i vestlige lande. Hvis hensigten med at lease en bil er at transportere den til en konfliktzone, vil der oftest være tale om en større bil, der er velegnet til brug i konfliktområder, f.eks. en stor SUV, 4x4 eller lignende. En indikator for denne kundetype kan f.eks. være personer, der går efter en bestemt type bil til brug i konfliktområder, som beskrevet ovenfor, og/eller ikke tidligere har ejet en bil.

En faktor, der kan indikere en begrænset risiko ved leasing af produkter/tjenesteydelser, er, at der er tale om et produkt med lav værdi.

Liv- og pensionsvirksomheder:
For virksomheder, der udbyder pensionsordninger, kan nedenstående eksempel illustrere en konkret vurdering:

Pensionsordninger oprettet som led i ansættelsen oprettes altid via arbejdsgiveren. Det er arbejdsgiveren, som indbetaler både sit eget og arbejdstagerens bidrag til pensionsordningen.

Der er generelt set derfor en meget begrænset risiko for, at obligatoriske pensionsordninger oprettet som led i et ansættelsesforhold kan anvendes til hvidvask. Dette billede ændres ikke, selvom ordningen giver muligheder for supplerende frivillige indbetalinger og evt. genkøb, hvilket primært kan begrundes med beskatningsmæssige forhold. Det er pensionsforsikringsselskabet, der sørger for at afregne arbejdsmarkedsbidrag ved indbetaling af skat eller afgifter ved udbetaling.

For pensionsordninger, der ikke er skattebegunstigede, er der en højere risiko for, at disse kan blive udnyttet til hvidvask end skattebegunstige ordninger.

Et eksempel på en ikke-skattebegunstiget ordning er en pensionsordning efter pensionsbeskatningslovens § 53 A, en såkaldt § 53 A ordning.

§ 53 A ordninger anvendes ofte i forbindelse med udstationering og lignende, hvor en medarbejder fortsætter sine indbetalinger på en tidligere arbejdsgiverindbetalt ordning, men ikke længere har en indkomst i Danmark at anvende fradraget i. Ordningen kan dog også tegnes privat, men ordningen er mindre attraktiv for personer, der er skattepligtige i Danmark.

Da der er tale om beskattede midler, som derfor ikke skal beskattes på udbetalingstidspunktet, står det forsikringstageren og pensionsselskabet friere eventuelt at aftale en kortere løbetid for udbetalingen. Heri ligger der således en risiko for, at pensionstageren søger at udnytte indbetalinger på ordningen til hvidvask af midler, som hidrører fra kriminel aktivitet, herunder skatteunddragelse. Dette sammenholdt med en mulig kortere løbetid gør, at ordningen kan være mere attraktiv til forsøg på hvidvask end øvrige pensionsprodukter.

Livsforsikring:
For virksomheder, der udbyder livsforsikringer, kan nedenstående eksempel illustrere en konkret vurdering:

Lav præmie på en livsforsikring, som anført i hvidvasklovens bilag 2, kan anskues ud fra virksomhedens profil, produktet og den konkrete kunde. Det vil derfor være forskelligt, hvad der anses for en lav præmie i det enkelte selskab.

Gruppelivsordninger for private er kendetegnet ved større ordninger med lav præmie, til gengæld stilles der ofte krav til helbredsoplysninger ved indtegning. Risikoen forbundet med gruppelivsforsikringer er begrænset som følge af, at der skal indtræde en forsikringsbegivenhed, før der kan ske udbetaling.

Det samme gør sig gældende for arbejdsmarkedspensionsordninger/firmapensionsordninger.

Udbydere af veksling mellem virtuelle valutaer og fiatvalutaer:
For virksomheder, der udbyder veksling mellem virtuelle valutaer og fiatvalutaer, kan nedenstående eksempler illustrere en konkret vurdering:

Ved veksling af virtuelle valutaer med øget anonymitet – såkaldte Privacy Coins – skal virksomheden være opmærksom på, at denne type af produkter kan bruges til hvidvask og finansiering af terrorisme i samme omfang som kontanter. Virksomheden har begrænset mulighed for at vurdere midlernes oprindelse og forretningsforbindelsens formål, idet forretningsforbindelsen kan sende og modtage disse virtuelle valutaer uden at efterlade sig digitale spor.

Tilsvarende gør en risiko sig gældende for veksling af virtuelle valutaer, der forudgående har gennemgået adskillige vekslinger, med det formål at sløre en før-forbrydelse. Før-forbrydelsen er typisk bedrageri (scams), løsesum (ransomeware) og hacks. De foregående vekslinger, der skal sløre før-forbrydelsen, kan eksempelvis ske ved brug af tjenesteydelser, såsom ”tumblers”, ”mixers” og ”scramblers”. Sløringen af en før-forbrydelse kan dog også ske uden brug af en tjenesteydelse, men ved, at de virtuelle valutaer sendes mellem en række forskellige adresser og muligvis også splittes op i mindre summer, før de veksles til fiatvaluta.

Betalingsinitieringstjenester:
For virksomheder, der udbyder betalingsinitieringstjenester, kan nedenstående eksempel illustrere en konkret vurdering:

En udbyder af betalingsinitieringstjenester (PISP) iværksætter en betalingsordre efter instruktion fra brugeren med henblik på at foretage en betalingstransaktion fra en betalingskonto, der udbydes af en anden udbyder af betalingstjenester end PISP’en. I modsætning til andre udbydere af betalingstjenester gennemfører en PISP ikke selv betalingstransaktioner og må ikke holde eller komme i besiddelse af brugerens midler. Det kan medføre, at hvidvaskrisikoen for en PISP kan være begrænset, men det medfører også, at en PISP bør overveje andre risikofaktorer end andre udbydere af betalingstjenester.

Med udgangspunkt i sin forretningsmodel skal en PISP vurdere, hvilke kunder der indgås forretningsforbindelser med. Det kan eksempelvis være en internetforretning, som løbende modtager betalinger for varer og tjenester fra kunder via betalingsinitieringstjenesten. Det kan også være fysiske personer, der

anvender en PISP (ofte i sammenhæng med en kontooplysningstjeneste) til at administrere en række forskellige konti, der eventuelt føres af flere forskellige kontoførende udbydere.

Betalingsinitieringstjenester er et ny type tilladelse. Der sker derfor fortsat en stor udvikling i de forretningsmodeller, der kan omfattes af tilladelsen. Det vil således afhænge af den konkrete forretningsmodel, hvordan en PISP skal iagttage sine forpligtelser i henhold til hvidvaskloven. Uanset at hvidvaskrisikoen kan være begrænset, og at transaktionerne typisk gennemføres via kundernes bankkonti, kan en PISP ikke alene forlade sig på, at det kontoførende institut er omfattet af hvidvasklovens krav.

En PISP iværksætter betalinger via et såkaldt API eller dedikeret interface, som den kontoførende udbyder, typisk et pengeinstitut, stiller til rådighed. Et API kan som følge af dets tekniske indretning begrænse, hvilke oplysninger, der er tilgængelig for en PISP. Det kan eksempelvis være oplysninger om identiteten på ejeren af den konto, hvorfra der foretages en betaling. Uanset at en PISP ikke forpligtes udover, hvad et API gør muligt, skal en PISP løbende overvåge og vurdere, hvilke transaktioner dens kunder iværksætter, og om disse giver anledning til nærmere undersøgelse, jf. undersøgelsespligten i hvidvaskloven.

En PISP bør som udgangspunkt altid skulle foretage en risikovurdering af kundeforholdet. I den sammenhæng bør en PISP inddrage geografiske forhold, eksempelvis hvis der betales til eller fra en betalingskonto, der føres i et højrisikoland. En PISP bør ligeledes inddrage forhold vedrørende kunden, f.eks. at kunden foretager en række betalinger til samme modtager, uanset om dette er fra samme eller forskellige konti, at kunden foretager store transaktioner, eller kundens transaktioner i øvrigt er usædvanlige.

3.3. Opdatering af risikovurderingen

Virksomhedens risikovurdering skal løbende holdes opdateret. Det betyder, at den skal afspejle virksomhedens aktuelle risikoprofil. Virksomheden vurderer, hvor ofte den skal revideres. Det beror på en konkret risikovurdering i forhold til forretningsmodellen. Som udgangspunkt skal risikovurderingen dog opdateres mindst en gang om året.

En opdatering af virksomhedens risikovurdering kan bestå i, at virksomheden har gennemgået risikovurdering og vurderet, at der ikke er grundlag for opdatering af denne. På samme måde kan virksomheden også vurdere, at det kun er nødvendigt at opdatere dele af virksomhedens risikovurdering.

Undtagelsesvist kan virksomheden opdatere sin risikovurdering med længere mellemrum, hvis forholdene og risikofaktorerne er statiske og umiddelbart ikke ændrer sig.

Virksomheden kan beslutte, at risikovurderingen skal opdateres ved faste intervaller. Den bør dog som minimum opdateres i forbindelse med væsentlige ændringer i forretningsmodellen og/eller risikoforholdene, og når der foreligger nye nationale eller supranationale risikovurderinger med nye vurderinger, også selvom virksomheden har fastsat et fast interval for opdatering.

Virksomheden kan afvige fra det fastsatte interval, f.eks. hvis virksomheden udskyder opdateringer få måneder, når virksomheden har en viden om, at der inden for kort tid kommer en ny national risikovurdering eller lignende.

Hvis en virksomhed har en forretningsmodel, hvor risikofaktorerne ofte ændrer sig, som er kompleks eller hvor den foregående risikovurdering har vist, at virksomheden har en høj iboende risiko for hvidvask eller

finansiering af terrorisme, bør risikovurderingen opdateres oftere med henblik på at sikre, at den er overensstemmende med den aktuelle risikoprofil.

Udgangspunktet om opdatering en gang årligt betyder, at virksomheden som minimum skal vurdere, om der er behov for en opdatering af risikovurderingen.

Når risikovurderingen opdateres, skal virksomheden vurdere, hvorvidt og hvorledes virksomhedens politikker, forretningsgange og kontroller også skal opdateres, så de er overensstemmende med virksomhedens overordnede og aktuelle risikoprofil.

Hvis virksomheden ikke har ændret forretningsmodel, og der ikke er ændrede ydre risikofaktorer, som begrunder det, vil virksomheden formentlig ikke have behov for at ændre sine politikker og måske heller ikke sine forretningsgange og kontroller.

Virksomheden bør løbende gennemgå sine risikofaktorer, herunder f.eks. om virksomheden har indgået forretningsforbindelser med nye kundetyper, har udviklet nye produkter, har udviklet nye systemer, eller udbyder tjenesteydelser i et nyt geografisk område. Virksomheden skal hermed vurdere risikofaktorerne for at afklare, om der er ændringer i risiciene, som påvirker den aktuelle risikoprofil. Dette bør ligeledes ske løbende i takt med, at virksomheden f.eks. foretager risikovurderinger som led af deres kundekendskabsprocedurer i henhold til hvidvasklovens kapitel 3.

Virksomheden skal være opmærksom på, at hvis der sker ændringer i virksomhedens forretningsmodel, f.eks. hvis virksomheden beslutter at udbyde nye produkter, tjenesteydelser eller leveringskanaler, bør der ske en opdatering af risikovurderingen, før virksomheden begynder at udbyde disse nye teknologier.

Virksomhedens forretningsgange og kontroller skal bl.a. sikre, at nye overordnede tendenser eller ændring i virksomhedens risikofaktorer opdages, samt at relevante informationskilder gennemgås.

4. Politikker, forretningsgange og kontroller

Henvisning til hvidvaskloven: § 8, stk. 1.

Henvisning til 4. hvidvaskdirektiv: Artikel 8, stk. 3 og 4.

Bekendtgørelse nr. 1026 af 30. juni 2016 om ledelse og styring af pengeinstitutter m.fl.
Bekendtgørelse nr. 1723 af 16. december 2015 om ledelse og styring i forsikringsselskaber m.v.

4.1. Baggrund

Hvidvasklovens § 8 stiller krav om, at virksomheden skal udarbejde skriftlige politikker, forretningsgange og kontroller.

Politikker er i denne sammenhæng virksomhedens overordnede beslutninger om, hvordan virksomheden skal indrettes, og hvordan opgaver i relation til forebyggelse af hvidvask og finansiering af terrorisme skal løses på baggrund af den forståelse for virksomhedens risikoprofil, som er opnået i risikovurderingen.

Forretningsgange er virksomhedens konkrete og operationelle udmøntning af politikkerne, således bliver vurderingerne f.eks. til forretningsgange og arbejdsbeskrivelser.

Kontroller er virksomhedens kontrol af, at virksomhedens beslutninger og forretningsgange overholdes på hvidvaskområdet. Endvidere skal der være en uafhængig intern kontrol med, at kontrollerne foretages, og at de er egnede og effektive. Kontrollerne skal være beskrevet i virksomhedens politikker og forretningsgange.

Se figuren nedenfor, der illustrerer processen i forhold til hvidvasklovens krav om risikovurdering og risikostyring. Processen er forsimplet ved en overordnet opdeling i tre led.

Politikkerne på hvidvaskområdet skal udarbejdes på baggrund af risikovurderingen, som virksomheden har foretaget i henhold til § 7, stk. 1. Der gælder ingen formkrav for virksomhedens politikker og forretningsgange, dog skal de være skriftlige, og de skal være tilgængelige og effektive for virksomheden. De skal som minimum omfatte politikker og forretningsgange for:

1) Risikostyring.
2) Kundekendskabsprocedurer.
3) Undersøgelses-, noterings-, og underretningspligt.
4) Opbevaring af oplysninger.
5) Screening af medarbejdere.
6) Intern kontrol.

At politikker og forretningsgange skal være skriftlige indebærer ikke, at de skal foreligge i papirform. De kan lagres digitalt. Idet der ikke gælder formkrav, er der ikke krav om, at politikker og forretningsgange for de enkelte led skal udformes i særskilte dokumenter. Det overordnede mål er, at virksomheden har

vurderet og dokumenteret sin iboende risiko, har fastsat sine overordnede strategiske mål og sine operationelle metoder til opnåelse af disse mål samt kontroller af, at målene efterleves.

Virksomhedens politikker, forretningsgange og kontroller på hvidvaskområdet skal godkendes af den hvidvaskansvarlige med henblik på, om de er tilstrækkelige til at opfylde kravene i hvidvaskloven. Virksomheden skal være opmærksom på, at der i anden lovgivning kan være krav om, at politikkerne også godkendes af bestyrelsen. Virksomheder, der i henhold til anden lovgivning er forpligtet til at have en compliancefunktion, skal udpege en complianceansvarlig, som skal være forpligtet til uafhængigt at vurdere, om virksomhedens politikker, forretningsgange og kontroller er effektive til forebyggelse og bekæmpelse af hvidvask og finansiering af terrorisme og om disse efterleves. For virksomheder, der har en uafhængig intern revisionsfunktion, skal denne sikre overholdelsen af virksomhedens § 8, stk. 1-forpligtelse. I relevant omfang skal virksomheder desuden udpege et medlem af direktionen, som skal sikre, at virksomheden overholder hvidvasklovgivningen.

Opsummerende betyder dette, at virksomheden kan have op til fire led i sin sikring af, at politikkerne, forretningsgangene og kontrollerne er effektive, og at virksomheden overholder hvidvaskloven. For nogle små virksomheder er det kun relevant med en hvidvaskansvarlig, og for små virksomheder med krav om en compliancefunktion kan den hvidvaskansvarlige også være den complianceansvarlige, hvis virksomheden har en berettiget begrundelse i virksomhedens størrelse eller sammensætning af aktiviteter. I sådanne tilfælde skal virksomheden dog have fokus på, at de opgaver, som ligger hos den hvidvaskansvarlige, som udgangspunkt ikke er opgaver, der skal varetages af virksomhedens compliancefunktion. Det skal derfor som minimum altid sikres, at medarbejdere ikke er involveret i udførelsen af opgaver, som de kontrollerer som led i deres compliance-opgaver.

4.2. Politikker

Virksomhedens politikker på hvidvaskområdet skal indeholde identifikation, vurdering og afgrænsning af virksomhedens risikofaktorer som konklusion på virksomhedens risikovurdering samt de overordnede strategiske mål til forebyggelse af hvidvask og finansiering af terrorisme for virksomhedens identificerede risici.

Virksomhedens iboende risiko og efterfølgende residuale risiko afspejler virksomhedens risikoprofil på hvidvaskområdet. Virksomhedens risikovillighed ligger derfor i den forretningsmodel, som virksomheden har opbygget. Med risikovillighed forstås, at virksomheden i sit valg og indretning af sin forretningsmodel vælger at acceptere nogle iboende risici. Det betyder, at virksomheden med risikobegrænsende foranstaltninger skal nedbringe risiciene for at kunne blive misbrugt til hvidvask og finansiering af terrorisme, så de residuale risici kommer på et acceptabelt niveau. Den residuale risiko, som virksomheden løber for at blive misbrugt til hvidvask og terrorisme, er den risiko, der kan være tilbage, selv med en effektiv forebyggelse, begrænsning og styring.

Et eksempel på ovenstående er, hvis virksomheden vælger at udbyde tjenesteydelser til lande med forhøjet risiko uden for EU, skal virksomheden sikre effektive forretningsgange, som tager højde for den øgede eksponering for risici, som virksomheden får ved at udbyde tjenesteydelser til sådanne lande. Virksomheden kan have en forretningsmodel med en høj iboende risiko, men det betyder, at virksomheden skal have passende ressourcer og tilrettelagt effektive politikker, forretningsgange og kontroller, der

reducerer de risici, som forretningsmodellen medfører, til et acceptabelt niveau. Endvidere skal virksomheden sikre, at der iværksættes kundeovervågning, som er proportional i forhold til de risici, virksomheden har.

Virksomhedens politikker skal derfor indeholde beskrivelser af de risikofaktorer, som virksomheden ønsker at påtage sig og anvisninger om, hvorledes virksomhedens strategiske mål opnås.

Risikovilligheden kan som ovenfor beskrevet konkret være virksomhedens stillingtagen til, om der f.eks. er produkttyper, som virksomheden ikke vil udbyde, eller om der er særlige geografiske områder, som virksomheden ikke ønsker at basere sig i.

Virksomhedens politikker skal bl.a. omfatte en stillingtagen til:

1) identifikation og afgrænsning af de risici, som virksomheden i sin forretningsmodel påtager sig,
2) principperne for risikostyringen,
3) risikostyringens formål,
4) virksomhedens risikoområder,
5) risikovillighed,
6) ansvarsfordeling og
7) risikoledelse og -styring organisatorisk i virksomheden.

Virksomhedens politikker kan skrives i et eller flere dokumenter.

4.3. Forretningsgange

Forretningsgange på hvidvaskområdet består af en beskrivelse af de aktiviteter, som virksomheden udfører med henblik på at sikre, at lovgivningen bliver overholdt, samt at virksomhedens politikker og forretningsgange efterleves.

Forretningsgangene skal tage udgangspunkt i virksomhedens forretningsmodel, politikker og de særlige forhold, der gælder for den enkelte virksomhed. De skal være et let anvendeligt værktøj for ansatte i virksomheden, og skal derfor på en klar og tydelig måde beskrive forretningsområdet, ansvarsplacering, herunder hvem der er ansvarlig for de enkelte opgaver, samt hvordan opgaverne skal udføres.

Forretningsgangene skal beskrive, hvordan følgende områder bliver håndteret i praksis:

1) Risikostyring.
2) Kundekendskabsprocedurer.
3) Undersøgelses-, noterings-, og underretningspligt.
4) Opbevaring af oplysninger.
5) Screening af medarbejdere.
6) Intern kontrol.

Forretningsgangene skal beskrive de enkelte aktiviteter i opgaveudførelsen af hvert område. Et eksempel på dette i forhold til noteringspligten kan være en beskrivelse af, hvor de ansatte i virksomheden skal foretage deres noteringer, f.eks. på kundens profil i virksomhedens sagsstyringssystem, og hvilke typer observationer og informationer der skal noteres.

Det er et krav, at dokumentationen af forretningsgange er lettilgængelige og overskuelig for de ansatte.

4.3.1. Risikostyring

Virksomhedens risikostyring på hvidvaskområdet skal tage udgangspunkt i virksomhedens forretningsmodel og de risici, som virksomheden har identificeret i sin risikovurdering.

Risikostyring er virksomhedens opmærksomhed på risici, og hvordan virksomheden reagerer på og indarbejder nye konstaterede risici.

Virksomheden skal sikre sig, at dens organisering er opbygget, så den sikrer klare definerede ansvarsområder, og at der samtidig er effektive forretningsgange til at identificere, overvåge og rapportere om risici for, at virksomheden er eller kan blive misbrugt til hvidvask eller terrorfinansiering. Derudover skal virksomheden have forretningsgange for, hvordan den håndterer konstaterede overtrædelser af virksomhedens politikker og forretningsgange.

I risikostyring ligger der også, at virksomheden skal følge risikoudviklingen inden for hvidvask og terrorfinansiering og tage højde for, hvordan denne påvirker virksomhedens risikovurdering, og dermed også politikker, forretningsgange og kontroller.

4.3.2. Screening af medarbejdere

Virksomheden skal forebygge, at ansatte kan misbruge deres stilling til hvidvask og finansiering af terrorisme eller medvirken hertil.

Screening af ansatte består af følgende to dele:

1) Sikring af, at den ansatte ikke er dømt for et strafbart forhold, der øger risiciene for, at personen kan misbruge sin stilling.
2) Sikring af, at den ansatte har tilstrækkelige kvalifikationer på hvidvaskområdet til at varetage stillingen.

Ad. 1) Sikre, at den ansatte ikke er dømt for et strafbart forhold, der øger risiciene for, at personen kan misbruge sin stilling.
Screening af ansatte, hvor der er en risiko for misbrug af stillingen til hvidvask eller finansiering af terrorisme, herunder medvirken hertil, skal ske forud for ansættelsen. Virksomheden kan f.eks. kontrollere dette ved at bede den ansatte om at fremvise sin straffeattest. Der er ikke tale om, at alle strafbare forhold øger risiciene for, at personen kan misbruge sin stilling. For eksempel vil domme for økonomisk kriminalitet og groft skattesvig som udgangspunkt medføre en øget risiko. Der kan således foretages en væsentlighedsbetragtning i forhold til hvilke domme, der medfører en øget risiko.

Det er dog vigtigt, at screeningen altid foretages på baggrund af en risikobaseret tilgang og er proportional med ansættelsesforholdet og den konkrete funktion, som den ansatte skal varetage eller varetager. Virksomheden skal forholde sig til hvilke funktioner, der konkret er relevante at underlægge screeningsprocedurer.

Det er ikke et krav, at alle ansatte skal screenes, men der skal ses på, hvilken funktion den ansatte skal varetage. Det vil for eksempel ikke være relevant for ansatte, der ikke varetager funktioner, der sikrer opfyldelse af hvidvaskloven. Screening af ansatte vil dog altid være relevant i tilfælde, hvor den ansatte varetager en funktion, hvor denne direkte eller indirekte kan misbruge sin stilling til at medvirke til hvidvask eller terrorfinansiering. Det er eksempelvis relevant ved:

1) Ansatte, der udfører kundekendskabsprocedurer.
2) Ansatte, der har adgang til at foretage transaktioner.
3) Ansatte, der har fået uddelegeret opgaver fra den hvidvaskansvarlige.
4) Ansatte, der arbejder i virksomhedens compliancefunktion.
5) Ansatte, der arbejder i virksomhedens interne revision eller interne auditfunktion.

Medarbejdere i ledende og/eller betroede stillinger vil desuden være særligt relevante at screene.

Virksomheden skal også på et risikobaseret grundlag sikre, at den bliver orienteret, hvis en ansat i løbet af ansættelsen bliver dømt for et strafbart forhold, der øger risiciene for, at personen kan misbruge sin stilling. Dette kan for eksempel gøres ved:

1) at virksomheden indsætter en oplysningspligt i sine ansættelseskontrakter, så den ansatte skal oplyse, hvis personen bliver dømt for et strafbart forhold under ansættelsen, eller
2) at virksomheden med et vist interval eller ved stikprøver beder den ansatte om at fremvise sin straffeattest og gemmer dokumentation på, at straffeattesten er blevet fremvist.

De foreslåede procedurer er eksempler, og de er derfor ikke udtryk for en praksis, som virksomheden er forpligtet til at følge. Virksomheden skal selv vurdere, hvilken procedure, der er mest hensigtsmæssig for virksomheden i forhold til at opnå formålet med reglerne om screening, og som er overensstemmende med databeskyttelseslovgivningen. Hvis virksomheden screener med et vist interval, kan virksomheden fastsætte intervallet ud fra en risikovurdering.

En ansats interne skift i virksomheden vil kunne begrunde screening af den ansatte, hvis dette ikke tidligere er sket.

Ansatte kan bestille en straffeattest digitalt via politiets hjemmeside, hvis de har NemID.

Ad. 2) Sikre, at den ansatte har tilstrækkelige kvalifikationer på hvidvaskområdet til at varetage stillingen. Kravet om screening indebærer også, at virksomheden skal sikre, at ansatte besidder de nødvendige kvalifikationer på hvidvaskområdet til at varetage stillingen på betryggende vis. Dette kan dog ske gennem uddannelse efter ansættelsen. Virksomheden skal dybest set sikre sig, at de ansatte har de nødvendige evner, viden og ekspertise til at udføre deres funktion i virksomheden effektivt.

Virksomhedernes forretningsgange og interne kontroller skal tage højde for, at en ansat kan misbruge sin stilling, jf. afsnit 7 om uddannelse.

4.3.3. Intern kontrol

Virksomheden skal etablere en intern kontrol, hvilket betyder, at virksomheden skal sikre, at der foretages kontrol af, om virksomheden overholder lovens krav på hvidvaskområdet.

Virksomheden skal i sine forretningsgange beskrive sine kontrolforanstaltninger, og samtidig skal virksomheden dokumentere de foretagne kontroller. Der skal således være en angivelse af, hvad kontrollen skal sikre, hvor hyppigt den skal foretages, hvordan den skal foretages, og hvordan der skal rapporteres om kontrollen til ledelsen og andre organisatoriske enheder. Der henvises til bestemmelser om intern kontrol i ledelsesbekendtgørelserne.

For virksomheder, der har en complianceansvarlig, skal kontrol både udføres i virksomhedens drift og også af den complianceansvarlige. Det vil sige, at der skal udføres første linjekontrol i virksomhedens forretning, og samtidig skal der ske anden linjekontrol af disse af den complianceansvarlige. For andre virksomheder eller personer skal det fastlægges, hvordan kontrollen udføres. Se afsnit 6.3 om complianceansvarlig.

For at der kan være tale om en effektiv kontrol, skal der være en tilstrækkelig uafhængighed mellem den, der foretager kontrollen, og den, der kontrolleres. I små virksomheder kan det være tilstrækkeligt, at den direkte leder kontrollerer den ansatte, mens det i større virksomheder kan være nødvendigt, at kontrollen foretages af en anden afdeling end den udførende.

Intern kontrol består af følgende to dele:

1) kontrol af, at virksomhedens politikker og forretningsgange overholdes
2) kontrol af, at kontrollerne bliver udført og er egnede

Der skal foretages kontroller med et passende interval af, at politikker, forretningsgange og kontroller overholdes. Kontroller skal foretages på følgende områder:

1) Risikostyring.
2) Kundekendskabsprocedurer.
3) Undersøgelses-, noterings- og underretningspligt.
4) Opbevaring af oplysninger.
5) Screening af medarbejdere.

Kontrollerne kan for eksempel udføres ved, at virksomheden udtager stikprøver på de forskellige områder og kontrollerer, at forretningsgangene på det enkelte område bliver overholdt.

Virksomheder skal indrette deres intern kontrol efter virksomhedens størrelse og de risici, der er forbundet med virksomhedens forretningsmodel. Virksomheder, der bliver drevet af kun en person, f.eks. en enkeltmandsvirksomhed uden ansatte, der bliver drevet af indehaveren, kan derfor tilrette deres interne kontrol efter virksomhedens størrelse og det forhold, at der ikke kan være samme uafhængighed i den interne kontrol, som hvis der var flere ansatte i virksomheden. Den interne kontrol i denne type virksomheder kan f.eks. være, at indehaveren med et fast interval, f.eks. 2-3 gange i kvartalet udtager en række stikprøver og kontrollerer, at virksomhedens forretningsgange er blevet overholdt. Det kan f.eks. være en kontrol af, om der er foretaget tilstrækkelige kundekendskabsprocedurer og indhentet korrekt materiale i den forbindelse samt en kontrol af, at der er foretaget opslag op mod sanktionslister.

5. Koncerner

Henvisning til hvidvaskloven: § 9, stk. 1 og 2 og § 31.

Henvisning til 4. hvidvaskdirektiv: Artikel 45, stk. 1.

Hvidvasklovens § 9 omhandler koncernforbundne virksomheder. Denne bestemmelse dækker forholdet mellem flere virksomheder i en koncern, mens § 8 regulerer den enkelte virksomhed i koncernen.

Kravene i § 9 gælder kun de dele af koncernen, som hvidvaskloven finder anvendelse på, se hvidvasklovens § 1, stk. 1.

Det betyder, at hvis et datterselskab ikke er omfattet af hvidvaskloven, er der ikke krav om, at de koncernfælles politikker og forretningsgange gælder for det pågældende datterselskab.

Kravene i § 9 gælder ikke for koncerner, hvor kun datterselskaber er omfattet af hvidvaskloven.

5.1. Udveksling af oplysninger i koncerner

Virksomheder i koncerner skal have tilstrækkelige:

1) skriftlige politikker for databeskyttelse og
2) skriftlige politikker og forretningsgange for udveksling af oplysninger inden for koncernen, der udveksles med det formål at bekæmpe hvidvask og terrorfinansiering.

Med reglerne om udveksling af oplysninger er der adgang til, at virksomheder i en koncern kan udveksle oplysninger, hvis de overholder koncernens forretningsgange herom, som skal overholde kravene i hvidvaskloven. Forretningsgange for udveksling af oplysninger i en koncern skal udarbejdes i overensstemmelse med databeskyttelseslovgivningen.

5.2. Koncernfælles risikovurdering, politikker og forretningsgange

Risikovurdering, politikker og forretningsgange i et moderselskab/hovedselskab skal dække hele koncernen, dog kun de dele af koncernen, der er omfattet af hvidvaskloven. Det betyder, at risikovurdering, politikker og forretningsgange kan udarbejdes af en central enhed i koncernen, for eksempel moderselskabet/hovedselskabet. Det er dog et krav, at disse er tilpasset den enkelte juridiske enheds eller filials forhold, herunder den juridiske enheds eller filials forretningsmodel og etableringslandets risikoforhold og regler.

Det er moderselskabets/hovedselskabets ansvar, at risikovurdering, politikker og forretningsgange på koncernniveau bliver udarbejdet.

Virksomheder, der er en del af en koncern, skal gennemføre koncernens politikker og forretningsgange. Helt overordnet skal den enkelte juridiske enheds eller filials politikker og forretningsgange være i overensstemmelse med moderselskabets/hovedselskabets.

Politikker og forretningsgange i udenlandske virksomheder, der har datterselskaber eller filialer etableret i Danmark, skal leve op til kravene i hvidvaskloven for så vidt angår forhold, der specifikt angår danske forhold. Det betyder for eksempel, at der skal inddrages risikobetragtninger, der vedrører Danmark.

Omvendt skal danske koncerner, der har datterselskaber eller filialer i andre lande, sikre, at koncernens politikker og forretningsgange overholder værtslandets (etableringslandets) regler om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme.

Med reglerne om grænseoverskridende virksomhed følger et krav om, at moderselskabet/hovedselskabet sikrer, at den etablerede koncernvirksomheds politikker, forretningsgange og kontroller om risikostyring, kundekendskabsprocedurer, undersøgelses-, noterings- og underretningspligt, opbevaring af oplysninger, screening af medarbejdere og intern kontrol overholder de nationale bestemmelser i etableringslandet.

Endvidere skal moderselskabet/hovedselskabet sikre, at der med faste intervaller føres kontrol med, at politikker, forretningsgange og kontroller overholdes i den etablerede virksomhed. Dette kan ske ved stikprøve eller ved besøg i den etablerede virksomhed.

Begrebet koncern skal forstås i overensstemmelse med selskabslovens definition af koncern.

6. Ansvarlige personer og funktioner

Hvidvaskloven stiller krav om, at en række ansvarlige personer og funktioner varetager forskellige områder i forhold til krav i hvidvaskloven. Nogle af disse gælder alle virksomheder, der er underlagt lovens krav, mens andre kun gælder finansielle virksomheder.

I det følgende kapitel er de forskellige ansvarlige personer og funktioner beskrevet.

Bestemmelse	**§ 7, stk. 2 (§ 8, stk. 2)**	**§ 8, stk. 3**	**§ 8, stk. 4**	**§ 8, stk. 5**
Funktion	**Den hvidvaskansvarlige**	**Den complianceansvarlige**	**Intern revision**	**Ansvarligt medlem af direktionen**
Hvornår skal en ansvarlig udpeges:	Udpeges i virksomheder, som omfattes af hvidvasklovens 1, stk. 1, nr. 1-8, 10-11, 19, 23 og 24.	Udpeges, når virksomheden, jf. anden lovgivning, er forpligtet til at have en compliancefunktion.	Gælder for virksomheder, som er omfattet af § 1, stk. 1-7, og som har intern revision.	Virksomheder skal, hvor det er vurderes relevant, udpege et medlem af direktionen, der er ansvarlig for gennemførelse af kravene i hvidvaskloven.
Hvilke opgaver skal den ansvarlige varetage:	Godkende virksomhedens politikker, forretningsgange og kontroller på hvidvaskområdet. Godkende forretningsforbindelser med kunder der har hjemsted i et højrisikotredjeland (§ 17, stk. 2), med PEP'er (§ 18, stk. 3) og med korre-	Uafhængigt kontrollere og vurdere, om virksomhedens forretningsgange og foranstaltninger er effektive.	Vurdere hvorvidt virksomhedens politikker, forretningsgange og kontroller er tilrettelagt og fungerer på betryggende vis i overensstemmelse med hvidvasklovens krav.	Sikre, at virksomheden gennemfører og overholder kravene i hvidvaskloven ved effektive politikker, forretningsgange og kontroller.

	spondentforbindelser (§ 19, stk. 1, nr. 3).			
Hvem er den ansvarlige:	Ansat eller medlem af den daglige ledelse med fuldmagt til at træffe beslutninger på virksomhedens vegne.	Person på ledelsesniveau.	Intern revision, der er ansat af bestyrelsen.	Person, som er medlem af direktionen. I virksomheder med kun én direktør, er det automatisk direktøren.

6.1. Hvidvaskansvarlig – den § 7, stk. 2-udpegede person

Henvisning til hvidvaskloven: § 7, stk. 2, § 8, stk. 2, § 18, stk. 3 og § 19, stk. 1, nr. 3.

Henvisning til 4. hvidvaskdirektiv: Artikel 3, nr. 12, artikel 8, stk. 5, artikel 19, stk. 1, litra c, og artikel 20, stk. 1, litra b, (i).

Den daglige ledelse, som oftest er virksomhedens direktion, skal udpege en ansat, der har fuldmagt til at træffe beslutninger på virksomhedens vegne om godkendelse af virksomheden politikker, forretningsgange og kontroller og om godkendelse af særlige kundeforhold. Kravet gælder følgende typer virksomheder:

1) Pengeinstitutter.
2) Realkreditinstitutter.
3) Fondsmæglerselskaber.
4) Livsforsikringsselskaber og tværgående pensionskasser.
5) Sparevirksomheder.
6) Udbydere af betalingstjenester og udstedere af elektroniske penge, jf. bilag 1, nr. 1-7 i lov om betalinger.
7) Forsikringsformidlere, når de formidler livsforsikringer eller andre investeringsrelaterede forsikringer.
8) Virksomheder, der erhvervsmæssigt udøver aktiviteter som fremgår af hvidvasklovens bilag 1.
9) Investeringsforvaltningsselskaber og forvaltere af alternative investeringsfonde, hvis disse virksomheder har direkte kundekontakt.
10) Danske UCITS og alternative investeringsfonde, hvis disse virksomheder har direkte kundekontakt.
11) Valutavekslingsvirksomheder.

Filialer af udenlandske virksomheder er ikke omfattet af kravet.

For at opfylde kravet skal den udpegede person reelt være involveret i virksomhedens arbejde med forebyggelse af hvidvask og finansiering af terrorisme.

Den hvidvaskansvarlige kan være et medlem af virksomhedens daglige ledelse eller en anden ansat. Den hvidvaskansvarlige skal kunne træffe beslutninger, som vedrører virksomhedens risikoeksponering på hvidvaskområdet. Den hvidvaskansvarliges ansvarsopgaver og fuldmagt til godkendelse fratager ikke virksomhedens ledelse det overordnede ansvar. Fuldmagten sikrer, at den hvidvaskansvarlige, hvor denne ikke indgår i ledelsen, får en beslutningskompetence på ledelsesniveau. Der kan være tilfælde, hvor den hvidvaskansvarlige i sin beslutning om godkendelse af f.eks. en forretningsforbindelse med en politisk eksponeret person vælger at indhente yderligere godkendelse fra den daglige ledelse, fordi den politisk eksponerede persons risikoprofil udgør en væsentlig risiko for hvidvask eller finansiering af terrorisme.

Hvidvasklovens krav er, at den hvidvaskansvarlige skal have tilstrækkeligt kendskab til virksomhedens risikoprofil og specifikke risikofaktorer. I større virksomheder vil den administrerende direktør ikke kunne udpeges, da denne vil forestå en for omfattende opgaveportefølje og fungere på et for højt niveau til samtidig effektivt at kunne opfylde forpligtelsen i § 7, stk. 2.

De konkrete rammer for personens involvering skal fastlægges af virksomheden. Det er vigtigt, at personen for at kunne varetage ansvaret, har adgang til virksomhedens kundedatabaser og øvrige relevante oplysninger, herunder bestyrelses- og revisionsprotokoller.

6.2. Den hvidvaskansvarliges ansvarsområder

Den hvidvaskansvarlige skal:

1) Have fuldmagt til at træffe beslutninger på virksomhedens vegne til godkendelse af følgende:
    a) politikker, forretningsgange og kontroller (§ 8, stk. 2)
    b) etablering og videreførelse af forretningsforbindelser som har hjemsted i et land, der er opført på Europa-Kommissionens liste over højrisikolande (§ 17, stk. 2)
    c) etablering og videreførelse af forretningsforbindelser med PEP'er (politisk eksponerede personer) og deres nærtstående og nære samarbejdspartnere (§ 18, stk. 3)
    d) etablering af grænseoverskridende korrespondentforbindelser (§ 19, stk. 1, nr. 3)
2) Have viden og indsigt i virksomhedens risici på hvidvaskområdet og derfor kunne træffe beslutninger, som er gavnlige for virksomhedens bekæmpelse af hvidvask og finansiering af terrorisme.

Virksomheden bør tilrettelægge den hvidvaskansvarliges arbejde sådan, at medarbejdere såvel som den øverste ledelse kan konsultere den hvidvaskansvarlige på alle relevante områder og orientere, så snart der er ny viden, som den hvidvaskansvarlige bør være bekendt med.

Endvidere skal den hvidvaskansvarlige have en tilstrækkelig grad af uafhængighed samt mulighed for at kunne rapportere direkte til direktionen og bestyrelsen om forhold på området for hvidvask og finansiering af terrorisme. Det er vigtigt at understrege, at rapportering til bestyrelsen er en mulighed, som den hvidvaskansvarlige skal benytte, hvis den hvidvaskansvarlige skønner, at det er nødvendigt. Der er derfor ikke en generel pligt til, at den hvidvaskansvarlige rapporterer til bestyrelsen.

Den hvidvaskansvarlige skal følge de forretningsgange, som virksomheden har tilrettelagt på området for hvidvask og finansiering af terrorisme. I virksomheder, der er pålagt at have en compliancefunktion, er det virksomhedens complianceansvarlige, der skal undersøge og føre uafhængig kontrol med, at den hvidvaskansvarliges forretningsgange er effektive.

6.2.1. Uddelegering

Den hvidvaskansvarlige har mulighed for at uddelegere de opgaver, der følger af bestemmelsen, til en eller flere medarbejdere med tilstrækkeligt kendskab til virksomhedens risikoprofil i forhold til hvidvask og finansiering af terrorisme. En eventuel uddelegering skal omfatte en eller flere navngivne personer eller navngivne stillinger. Der må aldrig kunne opstå tvivl om, hvilken person eller stilling opgaven er uddelegeret til. Der kan ikke ske uddelegering af de opgaver, der skal varetages efter § 7, stk. 2, til en enhed i virksomheden, f.eks. virksomhedens compliancefunktion.

En uddelegering til en eller flere personer vil særligt være relevant i større virksomheder med flere afdelinger, hvis arbejde omfattes af hvidvaskloven. Det er vigtigt at bemærke, at ansvaret i § 7, stk. 2 ikke kan uddelegeres, men påhviler den person, der er udpeget i henhold til bestemmelsen.

Fordi ansvaret altid ligger hos den hvidvaskansvarlige, vil der ved uddelegering af opgaver til en eller flere andre navngivne personer eller stillinger f.eks. kunne fastlægges et krav om rapportering eller lignende til den hvidvaskansvarlige, således at han eller hun fortsat kan bære det endelige ansvar.

6.3. Complianceansvarlig

Henvisning til hvidvaskloven: § 8, stk. 3.

Henvisning til 4. hvidvaskdirektiv: Artikel 8, stk. 4 litra a.

Om kravene til en complianceansvarlig henvises til:
Bekendtgørelse nr. 1026 af 30. juni 2016 om ledelse og styring af pengeinstitutter m.fl. og bekendtgørelse nr. 1723 af 16. december 2015 om ledelse og styring af forsikringsselskaber m.v.

Hvis en virksomhed i forbindelse med anden lovgivning er forpligtet til at have en compliancefunktion, skal virksomheden udpege en complianceansvarlig på ledelsesniveau.

Formålet med kravet om en complianceansvarlig er alene at fastlægge, at for finansielle virksomheder, der allerede har en forpligtelse til at have en complianceansvarlig i anden lovgivning, gælder, at den complianceansvarliges funktion også skal omfatte forpligtelser efter hvidvasklovgivningen.

Kravet gælder for følgende virksomheder, der i henhold til anden lovgivning skal have en compliancefunktion:

a) Pengeinstitutter.
b) Realkreditinstitutter.
c) Fondsmæglerselskaber.
d) Livsforsikringsselskaber og tværgående pensionskasser.
e) Sparevirksomheder.
f) Udbydere af betalingstjenester og udstedere af elektroniske penge, jf. bilag 1, nr. 1-7 i lov om betalinger.

g) Forsikringsformidlere, når de formidler livsforsikringer eller andre investeringsrelaterede forsikringer.

Filialer af udenlandske virksomheder er ikke omfattet af kravet.

Den complianceansvarlige skal fungere uafhængigt. Den complianceansvarlige skal kontrollere og vurdere, at virksomheden overholder hvidvaskloven og regler udstedt i medfør heraf. Det betyder, at personen skal kontrollere og vurdere, om virksomhedens forretningsgange og metoder for bekæmpelse af hvidvask og terrorfinansiering er egnet og effektive samt kontrollere, at virksomheden underretter Hvidvasksekretariatet, jf. lovens § 26, stk. 1. Derudover skal den complianceansvarlige kontrollere og vurdere, om de foranstaltninger, der iværksættes for at afhjælpe eventuelle mangler, er effektive.

Den complianceansvarlige skal som en del af virksomhedens interne kontrol sikre, at kontrollen foretaget af virksomheden er tilstrækkelig. Se afsnit 4.3.3 om intern kontrol.

Det kan også være den complianceansvarlige, der som uafhængig af den daglige ledelse, håndterer ansattes indberetning af overtrædelser eller potentielle overtrædelser (whistleblowerordning) efter lovens § 35, stk. 1, og § 36 a, stk. 1 og 2. Se afsnit 29 om whistleblowerordning.

6.4. Ansvarligt direktionsmedlem

Henvisning til hvidvaskloven: § 8, stk. 5. Henvisning til 4. hvidvaskdirektiv: Artikel 46, stk. 4.

Virksomheder skal, hvor det er vurderet relevant, udpege et medlem af direktionen, der er ansvarlig for gennemførelse af kravene i hvidvaskloven og regler udstedt i medfør heraf.

Dette betyder, at virksomheder, der ikke har en direktion, ikke er forpligtet til at udpege en person i henhold til bestemmelsen. Bestemmelsen tilsigter derfor ikke at indføre krav om, at virksomheder skal foretage organisatoriske ændringer.

Virksomheders indretning og drift foretages af direktionen i virksomheder, der har en direktion. Kravet om at udpege et ansvarligt direktionsmedlem skal dermed sikre, at hensynet og formålet med bestemmelsen forankres ledelsesmæssigt.

Der er ikke krav om, at virksomheder, der ikke har en direktion (f.eks. personligt ejede virksomheder), udpeger et direktionsmedlem.

Det ansvarlige direktionsmedlem har en særlig forpligtelse til at sikre, at virksomheden efterlever reglerne i hvidvaskloven. Personens opgave er at sikre ledelsesmæssig forankring af og ledelsesmæssig fokus på forebyggende foranstaltninger mod hvidvask og terrorfinansiering. Dette fratager dog ikke den øvrige daglige ledelse for ansvar.

Det ansvarlige direktionsmedlem kan f.eks. varetage opgaven ved løbende at have møder med den hvidvask- og complianceansvarlige og få status på virksomhedens overholdelse af reglerne i hvidvasklovgivningen, implementering af nye regler på hvidvaskområdet. Hvis virksomheden har mangler i forhold til

overholdelse af hvidvasklovgivningen, skal det ansvarlige direktionsmedlem sørge for opfølgning på, at disse mangler bliver udbedret.

Der kan i mindre virksomheder være personsammenfald mellem personen udpeget i henhold til denne bestemmelse og den hvidvaskansvarlige, jf. § 7, stk. 2, eller den complianceansvarlige i § 8, stk. 3.

Filialer i Danmark af udenlandske virksomheder
Der skal ikke i en filial i Danmark af en udenlandsk virksomhed udpeges en person efter hvidvasklovens § 8, stk. 5.

Filialer i udlandet af danske virksomheder
Hvis en dansk virksomhed har filialer i udlandet, skal de være opmærksomme på, at det ansvarlige direktionsmedlem også er ansvarlig i forhold til eventuelle filialer beliggende i udlandet.

6.5. Intern revision/intern audit

Henvisning til hvidvaskloven: § 8, stk. 4.

Henvisning til 4. hvidvaskdirektiv: Artikel 8, stk. 4, litra b.

Om kravene til intern revision henvises til:
Bekendtgørelse nr. 1912 af 22. december 2015 om revisionens gennemførelse i finansielle virksomheder m.v. samt finansielle koncerner.

Hvis en virksomhed har en intern revision eller intern audit, skal bestyrelsen i virksomheden sikre, at den interne revision eller interne audit vurderer, om virksomhedens politikker, forretningsgange og kontroller på hvidvaskområdet er tilrettelagt og fungerer på betryggende vis.

Formålet med kravet til intern revision eller intern audit er alene at fastlægge, at der for finansielle virksomheder, der allerede har en forpligtelse til at have en uafhængig revision eller audit, gælder, at denne funktion også varetager revision eller audit med overholdelse af kravene i hvidvaskloven og regler udstedt i medfør heraf. Det betyder, at funktionsbeskrivelsen for den interne revision eller interne audit skal indeholde bestemmelser om, at den interne revision eller interne audit skal sikre virksomhedens overholdelse af skriftlige politikker, forretningsgange og kontroller på området for hvidvask og finansiering af terrorisme.

Kravet gælder følgende virksomheder, hvis de har en intern revision eller intern audit:
1) Pengeinstitutter.
2) Realkreditinstitutter.
3) Fondsmæglerselskaber.
4) Livsforsikringsselskaber og tværgående pensionskasser.
5) Sparevirksomheder.
6) Udbydere af betalingstjenester og udstedere af elektroniske penge, jf. bilag 1, nr. 1-7, i lov om betalinger.
7) Forsikringsformidlere, når de formidler livsforsikringer eller andre investeringsrelaterede forsikringer.

7. Uddannelse

Henvisning til hvidvaskloven: § 8, stk. 6.

Henvisning til 4. hvidvaskdirektiv: Artikel 46, stk. 1.

Om kravene til grundkursus for bestyrelsesmedlemmer henvises til:
Bekendtgørelse nr. 1424 af 29. november 2016 om grundkursus for medlemmer af bestyrelsen i pengeinstitutter, realkreditinstitutter og forsikringsselskaber.

Virksomheden skal efter bestemmelsen i § 8, stk. 6, sikre, at ansatte, herunder ledelsen har modtaget tilstrækkelig undervisning i kravene i hvidvaskloven. Kravet gælder også undervisning af den del af virksomhedens ledelse, der beskæftiger sig med forebyggelse af hvidvask og terrorfinansiering. Kravet gælder for virksomhedens direktion og øverste ledelse.

Det følger herudover af anden lovgivning, at bestyrelsesmedlemmer i et pengeinstitut, et realkreditinstitut eller i et forsikringsselskab skal gennemføre et grundkursus bl.a. inden for hvidvaskforebyggelse, se bekendtgørelse om grundkursus for medlemmer af bestyrelsen i pengeinstitutter, realkreditinstitutter og forsikringsselskaber.

Virksomheden er ikke forpligtet til at undervise ansatte, der varetager funktioner, der ikke relaterer sig til hvidvask eller terrorfinansiering.

Der er krav om, at virksomheden har et egentligt undervisningsprogram. Virksomhedens forretningsgange og kontroller skal samtidig sikre, at undervisningen gennemføres for ansatte, der har med behandling af kundehold at gøre.

Det er ikke tilstrækkeligt at udlevere og gennemgå virksomhedens skriftlige politikker og forretningsgange med de ansatte. Det vil ligeledes heller ikke være tale om tilstrækkelig undervisning, hvis undervisningen alene gennemgår lovgivningens krav, men denne ikke er relateret til for eksempel virksomhedens forretningsmodel, herunder dens produktudbud, kundetyper mv.

Virksomheden kan vælge, at de enkelte ansatte kun modtager undervisning inden for deres relevante arbejdsområde. Undervisningen skal sikre, at de ansatte har et betryggende kendskab til de krav, der er på området for hvidvask og terrorfinansiering, samt hvilken betydning kravene har for den enkelte ansattes varetagelse af hendes eller hans arbejdsopgaver. Den ansatte skal kunne varetage sin jobfunktion på fuld forsvarlig måde og sikre, at virksomheden overholder lovens krav.

Virksomheden skal sikre, at de ansatte deltager i undervisningen.

For særlige forretningsområder skal undervisningen være tilpasset de ansattes særlige funktioner, herunder fremhævelse af de indikatorer på hvidvask og terrorfinansiering, der kan tænkes at forekomme på disse områder. Sådanne særlige områder er for eksempel værdipapirhandel, import/eksportfinansiering og grænseoverskridende korrespondentforbindelser.

Virksomhedens ansatte skal også modtage uddannelse i relevante bestemmelser om databeskyttelse for at sikre, at personoplysninger bliver behandlet i overensstemmelse med databeskyttelseslovgivningen. Dette skal være med til at sikre, at personoplysninger indhentet efter reglerne i hvidvaskloven alene sker med henblik på at efterleve kravene i hvidvaskloven.

Kravet om tilstrækkelig undervisning indebærer, at virksomheden med passende intervaller skal efteruddanne sine ansatte og ledelsen. Ved opdatering af virksomhedens forretningsgange skal der ske efteruddannelse af ansatte, hvor dette har betydning for de pågældende ansattes arbejdsfunktion.

Del 3 – Kundekendskabsprocedurer

Det er et grundlæggende princip i hvidvasklovgivningen, at virksomheden skal kende sine kunder. Reglerne om kundekendskabsprocedurer findes i hvidvasklovens kapitel 3, §§ 10-21.

Formålet med kundekendskabsprocedurer er, at forebygge hvidvask og finansiering af terrorisme, ved at virksomheder ved, hvem deres kunder er, og hvad der er kundens formål med forretningsforbindelsen eller den enkeltstående transaktion.

Kundekendeskabsprocedurer er en forpligtigelse, der gælder kontinuerligt i hele kundeforholdet. Det betyder, at oplysninger om kunden skal opdateres med passende intervaller ud fra en risikovurdering, se afsnit 8.3 om kundekendskabsprocedurer på passende tidspunkter. Virksomheden skal kunne dokumentere de oplysninger, som virksomheden indhenter i henhold til hvidvasklovens kapitel 3.

Ved overdragelse af en kundeportefølje har køberen pligt til at sikre, at risikovurderingen, risikostyringen og kundekendskabsprocedurer mv. lever op til hvidvasklovens krav. Det er ikke et krav, at køberen gennemfører fornyede kundekendskabsprocedurer på hele kundeporteføljen på tidspunktet for overdragelsen, men køberen er fra overdragelsestidspunktet ansvarlig for at leve op til hvidvasklovens krav, herunder at der sker en opdatering af oplysninger om den overdragne kundeportefølje. Ved en fusion af en eller flere virksomheder, vil det ligeledes være det nye eller det fortsættende selskab, som har ansvaret for at leve op til hvidvasklovens krav. I det omfang der sker en virksomhedsoverdragelse, i form af en overdragelse af kapitalandelene i en virksomhed underlagt hvidvaskloven, vil virksomheden, der overdrages, fortsat være pligtsubjekt efter hvidvaskloven, mens erhververen af kapitalandelene som udgangspunkt ikke vil have et direkte ansvar for, at virksomheden opfylder hvidvasklovens krav om kundekendskabsprocedurer.

Hvad er en kunde?
Begrebet kunde dækker over både fysiske personer og juridiske personer (f.eks. selskaber, foreninger og offentlige myndigheder).

Et kundeforhold opstår, når virksomheden enten etablerer en forretningsforbindelse med en kunde eller foretager en enkeltstående transaktion for en kunde. Dette kan f.eks. omfatte, at virksomheden indgår aftale med en fysisk eller juridisk person om, f.eks. åbning af en konto (udlån, indlån, leasing mv.) eller et depot, en pengeoverførsel, valutaveksling, køb eller salg af værdipapirer, en rådgivningsopgave, en formidlingsopgave, f.eks. salg af fast ejendom eller en aftale om at udarbejde et regnskab eller udføre revision.

Kunden er den fysiske eller juridiske person, som virksomheden indgår et aftaleforhold med eller på hvis vegne virksomheden gennemfører en transaktion eller aktivitet.

Hvidvasklovens kundebegreb omfatter alene egne kunder og således ikke kunders kunder. Tilsvarende omfatter lovens forretningsforbindelsesbegreb alene egne forretningsforbindelser og således ikke forretningsforbindelsers forretningsforbindelser. Der skal dermed ikke gennemføres kundekendskabsprocedurer i forhold til kunders kunder eller forretningsforbindelsers forretningsforbindelser, og transaktionsovervågning skal alene omfatte de midler, som overføres/modtages via kundes konto.

Eksempler på kundeforhold

1) Ved værgemål og samværgemål er værgen den person, der handler på vegne af kunden. Kunden er den umyndige eller personen under værgemål eller samværgemål.

2) Ved en børneopsparing er det barnet, der er kunden. Opretteren af børneopsparingen handler på vegne af kunden.

3) En leasingtager er leasingselskabets kunde. Den forhandler, som leasingselskabet køber udstyret af og/eller sælger udstyret til ved leasingaftalens udløb, er ikke omfattet af kundebegrebet i hvidvaskloven.

4) En kautionist for en fordring, f.eks. et lån i et pengeinstitut eller realkreditinstitut, skal betragtes som kunde ved optagelse af lånet, da kautionisten har indgået en aftale med pengeinstituttet/realkreditinstituttet, hvorved der er etableret en forretningsforbindelse. Det betyder, at det i en sådan situation er både låntager og kautionist, der skal betragtes som kunder.

5) Ved tredjemandspant er det en konkret vurdering af det enkelte forhold, om der bliver etableret en forretningsforbindelse. Hvis der i forbindelse med tredjemandspant bliver oprettet en konto, vil der altid være tale om etablering af en forretningsforbindelse.

6) Ved livsforsikringer og pensioner er kunden den fysiske eller juridiske person, som selskabet indgår aftale med (forsikringstager), og som er indehaver af forsikringspolicen. Ved arbejdsmarkedspensioner og firmaordninger, hvor der udstedes selvstændige policer, er det lønmodtageren, der skal identificeres og kontrolleres som kunde. Ved gruppeforsikringsordninger, hvor der ikke udstedes selvstændige policer, er det arbejdsgiveren/foreningen, der skal identificeres og kontrolleres som kunde. Når livsforsikringsselskaber foretager eller sælger en investering, etableres der ikke et kundeforhold. Dette skyldes, at livsforsikringsselskaber alene etablerer kundeforhold i hvidvasklovens forstand til de fysiske og juridiske personer, som selskabet indgår aftale med og som er indehavere af en forsikringspolice.

7) En revisor kan indhente hjælp hos tredjemand (f.eks. en anden revisor eller en skatterådgiver) til udførelsen af opgaver for en kunde. Tredjemand vil her som udgangspunkt skulle anses som underleverandør til revisor. De konkrete omstændigheder kan dog medføre, at tredjemand er indgået i et kundeforhold med revisors kunde. Dette vil f.eks. være tilfældet ved revisors afgivelse af erklæringer. Hvem der er tredjemands kunde, beror derfor bl.a. på en konkret vurdering af, hvem kundeforholdet er indgået med, opgavens omfang og varighed, med hvem kontakten sker, samt til hvem ydelsen faktureres.

8) En ejendomsmægler (sælgermægler), som bistår ved salg af en fast ejendom, skal anse både sælger og køber som kunder. Hvis køber er repræsenteret af en anden ejendomsmægler, revisor, advokat eller andre, som udbyder samme ydelser, jf. hvidvasklovens § 1, stk. 1, nr. 17, skal køber ikke anses som kunde for sælgermægler.

9) En købermægler, uanset om denne er registreret som ejendomsmægler, som bistår ved et køb af en fast ejendom, skal anse både sælger og køber som kunder. Hvis sælger er repræsenteret af en ejendomsmægler, revisor, advokat eller andre som udbyder samme ydelser, jf. § 1, stk. 1, nr. 17, anses sælger alene for at have indgået en forretningsforbindelse med denne.

10) Advokaters kunder/forretningsforbindelser er deres klienter, og et klientforhold skal betragtes som etableret ved advokatens accept af at ville repræsentere klienten. I mange tilfælde etableres et klientforhold i løbet af det første møde med klienten.

11) Ved værdipapirhandel[5] er kunden den fysiske eller juridiske person, som virksomheden indgår aftale med om køb eller salg af værdipapirer.

12) Særligt på området værdipapirhandel kan følgende eksempler på afgrænsning af kundebegrebet anføres:
    a) En modpart, som en værdipapirhandler[6] henvender sig til med henblik på at udføre en kundes ordre, er ikke kunde hos værdipapirhandleren.
    b) En værdipapirhandler, der henvender sig til en virksomhed, er kunde hos virksomheden. Værdipapirhandlerens kunder er ikke kunder hos virksomheden.
    c) Hvis en kunde har depot og/eller konto hos en virksomhed, er kunden dog stadig kunde hos virksomheden i kraft af depotet og/eller kontoen, selvom kunden henvender sig gennem en værdipapirhandler, f.eks. gennem en porteføljeplejeaftale hos værdipapirhandleren.
    d) Modparter, som en virksomhed indgår handler med via en markedsplads, som defineret i direktiv 2014/65/EU (MiFID II) eller en markedsplads beliggende i et tredjeland, som er omfattet af en beslutning om ækvivalens truffet af Europa Kommissionen eller en anden relevant myndighed, er ikke kunder.
    e) Modparter, som en virksomhed indgår bilaterale værdipapirhandler med, er ikke kunder, hvis det er en aftalt betingelse, at der sker clearing via en af følgende enheder:
        i. En central modpart (CCP) som har opnået tilladelse som central modpart (CCP) fra en kompetent myndighed i en medlemsstat i henhold til Kapitel 1, Afsnit III i Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 om OTC-derivater, centrale modparter og transaktionsregistre (som ændret).
        ii. En central modpart (CCP) beliggende i et tredjeland, som er anerkendt af ESMA i henhold til Artikel 25 i Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 om OTC-derivater, centrale modparter og transaktionsregistre (som ændret).
    f) En person, der ejer værdipapirer udstedt af en virksomhed, er ikke kunde hos virksomheden.

13) Ved betalingsinitieringstjenester består den aftalemæssige relation mellem udbyderen af betalingsinitieringstjenesten og den enkelte internetforretning/webshop om udbyderens levering af og internetforretnings/webshops integrering af betalingsløsningen til brug for internetforretningens/webshoppens kundes onlinehandel. Betalingsinitieringstjenestens forretningsforbindelse er således internetforretningen/webshoppen, mens internetforretningen/webshoppens kunde ikke er forretningsforbindelse i forhold til betalingsinitieringstjenesten.

[5] I denne vejledning dækker begrebet værdipapirhandel handel med finansielle instrumenter som defineret i lov om kapitalmarkeder og i bilag 5 til lov om finansiel virksomhed.
[6] I denne vejledning omfatter begrebet værdipapirhandler både definitionen i medfør af lov om finansiel virksomhed og virksomheder med tilsvarende tilladelse fra et EU-land eller under tilsvarende tilsyn i et tredjeland.

8. Hvornår skal en virksomhed gennemføre kundekendskabsprocedurer

Hvidvasklovens § 10 beskriver, hvornår en virksomhed skal gennemføre kundekendskabsprocedurer:

1) Ved etablering af en forretningsforbindelse.
2) Når en kundes relevante omstændigheder ændrer sig.
3) På passende tidspunkter, herunder når virksomheden eller personen i løbet af det relevante kalenderår er juridisk forpligtet til at kontakte kunden med henblik på at undersøge enhver relevant oplysning vedrørende den eller de reelle ejere.
4) Ved enkeltstående transaktioner over et vist beløb.
5) Ved udbud af spil, hvor indsatsen eller udbetalingen er over et vist beløb.
6) Ved mistanke om hvidvask eller finansiering af terrorisme.
7) Ved tvivl om tidligere indhentede oplysninger om kunden.

De følgende afsnit beskriver ovenstående situationer nærmere.

8.1. Etablering af en forretningsforbindelse

Henvisning til hvidvaskloven: § 10, stk. 1, nr. 1. Henvisning til 4. hvidvaskdirektiv: Artikel 11, litra a.

Det er udgangspunktet, at en virksomhed etablerer en forretningsforbindelse, når virksomheden udfører en ydelse eller sælger et produkt til en kunde. For kundeforhold hvor der ikke bliver etableret en forretningsforbindelse, se afsnit 8.4 om enkeltstående transaktioner.

Når virksomheden etablerer et kundeforhold, hvor det på tidspunktet for etableringen forventes, at kundeforholdet bliver af en vis varighed, etableres der en forretningsforbindelse. Der vil derfor være tale om etablering af en forretningsforbindelse, hvis virksomheden vurderer, at kunden vil benytte sig af virksomhedens ydelser gentagne gange og dermed vil være en jævnlig tilbagevendende kunde.

Der er altid tale om etablering af en forretningsforbindelse, hvis en kunde får oprettet en konto eller lignende hos virksomheden f.eks. i forhold til indlån, udlån, leasing eller aftale om ejendomssalg.

Der må ikke oprettes anonyme konti eller konti under falske navne, og derfor er det et krav, at der altid gennemføres kundekendskabsprocedurer ved etablering af en forretningsforbindelse.

8.2. En kundes relevante omstændigheder ændrer sig

Hvis der er tale om en etableret forretningsforbindelse, og kundens relevante omstændigheder ændrer sig, skal kundeskabsprocedurerne gennemføres igen.

Virksomheden skal reagere, hvis den bliver opmærksom på ændringer i kundeforholdet f.eks. en større udvidelse af kundeengagementet og/eller på ændringer i kundens virksomhed.

Virksomheden skal i disse situationer ud fra en risikovurdering tage stilling til, om der skal indhentes nye oplysninger om kunden, herunder eksempelvis indhentelse af identitetsoplysninger på ny og kontrol af disse.

Hvis kunden er en juridisk person, skal virksomheden på baggrund af en risikovurdering tage stilling til, om der skal indhentes nye oplysninger om de reelle ejere. Hvis virksomheden har fået nye reelle ejere, skal virksomheden identificere og gennemføre rimelige foranstaltninger for at kontrollere de nye reelle ejere. Derudover vil der ofte være behov for, at virksomheden klarlægger den nye ejer- og kontrolstruktur for den pågældende kunde.

Eksempler på, at kundens relevante omstændigheder ændrer sig:

1) Hvis kundens formål eller tilsigtede beskaffenhed med forretningsforbindelsen ændrer sig væsentligt, f.eks. fordi kunden begynder at foretage langt større transaktioner end tidligere, se afsnit 9.7 om forretningsforbindelsens formål og tilsigtede beskaffenhed.
2) Hvis en kunde får status som PEP.
3) Hvis en kunde til/fraflytter Danmark eller flytter sit forretningssted til/fra Danmark, herunder særligt til/fra højrisikolande.
4) Hvis en kundes ejer- og kontrolstruktur ændrer sig, f.eks. på grund af en virksomhedsomdannelse eller fordi virksomheden får inddraget en tilladelse til at udføre visse aktiviteter.

Virksomheden skal gennemføre kundekendskabsprocedurer, når virksomheden får viden om, at kundens relevante omstændigheder ændrer sig. Dette kan f.eks. være som led af virksomhedens overvågning, løbende gennemførelse af kundekendskabsprocedurer eller hvis virksomheden på anden måde får positiv viden om kunden, se afsnit 9.8 om løbende overvågning af forretningsforbindelsen.

8.3. Kundekendskabsprocedurer på passende tidspunkter

Når der er tale om en etableret forretningsforbindelse, skal virksomheden gennemføre kundekendskabsprocedurerne med passende intervaller i kundeforholdet. Kravet om at gennemføre kundekendskabsprocedurer gælder ligeledes, når virksomheden i løbet af det relevante kalenderår er juridisk forpligtet til at kontakte kunden med henblik på at undersøge enhver relevant oplysning vedrørende den eller de reelle ejere. Formålet er at sikre, at de oplysninger, virksomheden har om en eksisterende kunde, er korrekte og tilstrækkelige. Virksomheden skal derfor, ud over gennemførelse af kundekendskabsprocedurer, hvis kundens relevante omstændigheder ændres, også sikre, at de gennemføres ved faste intervaller, og når virksomheden er juridisk forpligtet til at kontakte kunden.

Med "juridisk forpligtet" menes, at en virksomhed er forpligtet til at kontakte en kunde med henblik på at undersøge enhver relevant oplysning vedrørende den eller de reelle ejere. En sådan forpligtelse kan f.eks. bestå i henhold til direktivet om administrativt samarbejde på beskatningsområdet[7], særligt CRS-reglerne og herunder også FATCA-reglerne.

Er en virksomhed forpligtet til at kontakte kunden, skal virksomheden samtidig hermed undersøge, om enhver relevant oplysning vedrørende den eller de reelle ejere forsat er korrekte.

[7] Rådets direktiv 2011/16/EU af 15. februar 2011 om administrativt samarbejde på beskatningsområdet, som bl.a. ændret ved Rådets direktiv 2014/107/EU.

Et eksempel herpå kan være, når en virksomhed er forpligtet til at gennemføre kravene om passende omhu (due diligence) efter CRS-reglerne og i den forbindelse bliver opmærksom på nye relevante oplysninger vedrørende en persons status. Her vil virksomheden være forpligtet til at kontakte kunden med henblik på at indhente en ny egenerklæring eller bevisdokument og vil i den forbindelse ligeledes være forpligtet til at undersøge enhver relevant oplysning vedrørende den eller de reelle ejere.

Et andet eksempel herpå kan være, når en forvalter af en trust i medfør af hvidvasklovens § 46 a, stk. 5, gennemfører sin årlige undersøgelse af, om der er sket ændringer af de registrerede oplysninger om kundens (trustens) reelle ejere, og vurderer, at det er nødvendigt at kontakte en eller flere, som indgår i trusten, herunder f.eks. trustens stifter eller andre trustees.

Kravet om gennemførelse af kundekendskabsprocedurer ved passende intervaller skal foretages på et risikobaseret grundlag. Det vil sige, at virksomheden skal fastsætte intervallet ud fra en risikovurdering af kundeforholdet. Virksomheden kan samle kunderne i forskellige kundekategorier, f.eks. kunder med begrænset risiko og kunder med øget risiko, og kan eksempelvis fastsatte ét interval for kunder med begrænset risiko og et andet interval for kunder med øget risiko. Virksomheden kan dog ikke beslutte, at kundekendskabsprocedurerne ikke gennemføres.

Det er således hensigten, at virksomheden fokuserer på kundeforhold med øgede risici, mens der ved kundeforhold med begrænsede risici ikke er behov for samme omfattende og hyppige procedurer.

Der er ikke fastsat en lovbestemt metode til, hvordan virksomheden gennemfører kundekendskabsprocedurer ved passende intervaller. Kundekendskabsprocedurerne kan derfor gennemføres ved f.eks. en automatiseret og/eller en manuel proces. Dette skal dog ske ud fra en risikobaseret tilgang.

Hvis der er tale om et kundeforhold med en juridisk person, kan det for eksempel være relevant i tilfælde med begrænsede risici med passende intervaller at kontrollere, om kunden har fået nye reelle ejere.

8.4. Enkeltstående transaktioner

Henvisning til hvidvaskloven: § 10, stk. 1, nr. 2.

Henvisning til 4. hvidvaskdirektiv: Artikel 11, stk. 1, litra b.

Anden lovgivning: Europa-Parlamentets og Rådets forordning (EU) 2015/847 af 20. maj 2015 om oplysninger, der skal medsendes ved pengeoverførsler, og om ophævelse af forordning (EF) nr. 1781/2006.

Udgangspunktet er, at en virksomhed etablerer en forretningsforbindelse, når den udfører transaktioner for en kunde, og der dermed skal gennemføres kundekendskabsprocedurer. Virksomheden kan dog udføre enkeltstående transaktioner for kunder, der ikke med jævne mellemrum benytter sig af virksomheden.

Virksomheden skal i sine procedurer for kundekendskab sikre sig, at virksomheden er i stand til at afgrænse, hvornår en kunde går fra at være en kunde, som virksomheden gennemfører enkeltstående transaktioner for, til at være en forretningsforbindelse. Virksomheden kan derfor fastlægge en række

kriterier for at vurdere, om der er tale om en forretningsforbindelse eller ej. Sådanne kriterier kan f.eks. være:

1) Antallet af gange kunden benytter sig af virksomheden.
2) Tidsintervallet mellem to transaktioner.
3) Antallet af transaktioner.

Når der er tale om enkeltstående transaktioner, skal virksomheden gennemføre kundekendskabsprocedurer, når virksomheden udfører transaktioner for en kunde på mindst 15.000 euro.

For pengeoverførsel og valutaveksling gælder der andre grænser. Der skal ved pengeoverførsel gennemføres kundekendskabsprocedurer, når virksomheden udfører en enkeltstående transaktion på mere end 1.000 euro og ved valutaveksling skal procedurerne gennemføres, når transaktionen er 500 euro eller derover.

Kendes transaktionens størrelse ikke på forhånd, skal der gennemføres kundekendskabsprocedurer, så snart der er en formodning om, at transaktionen eller transaktionerne samlet vil komme til at modsvare et beløb på henholdsvis de 15.000 euro, 1.000 euro eller 500 euro.

De nævnte grænser gælder, uanset om transaktionen sker på én gang eller som flere transaktioner, der er eller ser ud til at være indbyrdes forbundne.

Eksempler på indbyrdes forbundne transaktioner:

1) En kunde beder om at få overført henholdsvis 800 euro og 900 euro og overstiger dermed grænsen på 1.000 euro.
2) En kunde kommer igen flere gange samme dag eller dagen efter og foretager samme type transaktion.
3) En kunde kommer flere dage i træk og får vekslet beløb, der tilsammen modsvarer et beløb på 500 euro eller mere.

Der er tale om en enkeltstående transaktion, når der ikke bliver etableret en forretningsforbindelse. Det vil sige, at der ikke er tale om en enkeltstående transaktion, hvis der er etableret eller bliver etableret en forretningsforbindelse på grund af andre ydelser, f.eks. kontooprettelse, rådgivning eller lignende.

Jævnligt tilbagevendende kunder hos f.eks. valutavekslingsvirksomheder og pengeoverførselsvirksomheder vil skulle betragtes som forretningsforbindelser. Det er en konkret vurdering, hvornår en kunde, der foretager gentagne enkeltstående transaktioner skal betragtes som en etableret forretningsforbindelse, og der dermed skal gennemføres kundekendskabsprocedurer. Det afhænger blandt andet af, hvor ofte kunden foretager en transaktion samt hvor lang en tidsperiode, der er imellem de enkelte transaktioner. Se afsnit 8.1 om etablering af en forretningsforbindelse.

Hvis der er mistanke om hvidvask eller finansiering af terrorisme, skal der altid gennemføres kundekendskabsprocedurer, se afsnit 8.6 om mistanke om hvidvask og finansiering af terrorisme.

Virksomheden skal være opmærksom på, at virksomheden ved pengeoverførsler skal overholde kravene i pengeoverførselsforordningen om oplysninger om betaler og betalingsmodtager. Dette krav gælder, selvom virksomheden ikke er forpligtet til at gennemføre kundekendskabsprocedurer efter kravene i hvidvaskloven.

Se afsnit 8.8. om enkeltstående aktiviteter, der ikke er transaktioner.

8.5. Udbud af spil, hvor indsatsen eller udbetalingen er over et vist beløb

Henvisning til hvidvaskloven: § 10, stk. 1, nr. 3. Henvisning til 4. hvidvaskdirektiv: Artikel 11, litra d.

En udbyder af spil defineres som en juridisk eller fysisk person etableret her i landet, der erhvervsmæssigt udbyder spil. Alle udbydere af spil, som er omfattet af lov om spil, anses for at drive erhvervsmæssig virksomhed.

Kun udbydere af spil, der er etableret i Danmark, er omfattet af hvidvaskloven. Spiludbydere med en dansk tilladelse til at udbyde spil anses for etableret her i landet og er dermed også omfattet af loven.[8]

De enkelte forhandlere af spil i butikker, kiosker mv., som forhandler spillet i spiludbyderens navn, er ikke omfattet af hvidvaskloven. Dette indebærer, at det er spiludbyderens ansvar at sikre, at en forhandler gennemfører kundekendskabsprocedurer, hvis dette ikke allerede er sket ved etablering af forretningsforbindelsen. Forhandleren skal i sådanne tilfælde gennemføre kundekendskabsprocedurer, hvis spilleren lægger en indsats eller får udbetalt en gevinst eller begge dele på mindst 2.000 euro, hvad enten transaktionen sker på én gang eller som flere transaktioner, der ser ud til at være indbyrdes forbundne.

Det er valgfrit for virksomheden at afgøre, hvilken del af processen der udløser udførslen af kundekendskabsproceduren.

Om flere transaktioner er indbyrdes forbundet, kan vurderes ud fra den enkelte forhandler og inden for en periode på 24 timer. Som hovedregel anses flere transaktioner i forbindelse med en virksomheds salg af væddemål inden for et døgn hos samme forhandler for at være indbyrdes forbundne. Som eksempel kan nævnes, at hvis en kunde går ind og ud af den samme butik flere gange på et døgn og foretager flere transaktioner i forbindelse hermed, vil det være at betragte som forbundne transaktioner. Det samme er tilfældet, hvis kunden deler transaktionen op ved samme besøg.

Det bemærkes, at definitionen af indbyrdes forbudne transaktioner i det landbaserede udbud af væddemål ikke kan anvendes ved onlinespil, da den tilgængelige datamængde og generelle muligheder for at følge spilleren her er langt større.

Virksomheden skal altid være opmærksom på, om der etableres en forretningsforbindelse, f.eks. ved oprettelse af loyalitetskort eller ordninger, hvorved en gevinst overføres til en bankkonto. Ved onlinespil indgås en forretningsforbindelse fra begyndelsen af kundeforholdet, da der etableres en spilkonto, inden spil påbegyndes. Se afsnit 8.1 om etablering af en forretningsforbindelse.

For yderligere information om spil henvises til Spillemyndighedens fagspecifikke hvidvaskvejledning[9].

[8] Dette fremgår af FT 2016-17 L41 Betænkning over Forslag til lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme (hvidvaskloven) afgivet af Erhvervs-, Vækst- og Eksportudvalget den 30. maj 2017, side 9-10.

[9] www.spillemyndigheden.dk/uploads/2020-01/Version%201.1%20Spillemyndighedens%20vejledning%20om%20forebyggende%20foranstaltninger%20mod%20hvidvask%20af%20udbytte%20og%20finansiering%20af%20terrorisme.pdf

8.6. Mistanke om hvidvask eller finansiering af terrorisme

Henvisning til hvidvaskloven: § 10, stk. 1, nr. 4.

Henvisning til 4. hvidvaskdirektiv: Artikel 11, stk. 1, litra e.

Virksomheden skal altid gennemføre kundekendskabsprocedurer, når virksomheden har viden eller mistanke om hvidvask eller finansiering af terrorisme. Kravet gælder selvom der kun er tale om en enkeltstående transaktion under et vist beløb, se afsnit 8.4 om enkeltstående transaktioner, eller udbud af spil, hvor indsatsen eller udbetalingen er under 2.000 euro, se afsnit 8.5 om udbud af spil, hvor indsatsen eller udbetaling er over et vist beløb.

Der kan være situationer med mistanke, hvor det ikke er muligt at gennemføre kundekendskabsprocedurer, f.eks. hvis kunden nægter at give disse oplysninger eller forlader virksomheden, når disse oplysninger bliver efterspurgt. Virksomheden skal i disse tilfælde foretage en underretning til Hvidvasksekretariatet med de oplysninger, som virksomheden er i besiddelse af.

8.7. Tidligere indhentede oplysninger om kunden

Henvisning til hvidvaskloven: § 10, stk. 1, nr. 5.

Henvisning til 4. hvidvaskdirektiv: Artikel 11, stk. 1, litra f.

Bekendtgørelse nr. 1376 af 12. december 2019 om indberetning af uoverensstemmelser i oplysninger om reelle ejere.

Erhvervsstyrelsens vejledning om reelle ejere.

Virksomheden skal gennemføre kundekendskabsprocedurer, hvis der er tvivl om, hvorvidt de indhentede oplysninger om kundens identitet mv. er korrekte og/eller tilstrækkelige.

Det betyder, at hvis virksomheden får grund til at tro, at de indhentede oplysninger ikke er tilstrækkelige og/eller korrekte, skal der gennemføres kundekendskabsprocedurer på ny. Der ligger i kravet, at der skal ske gennemførelse af hele kundekendskabsproceduren eller dele af kundekendskabsproceduren ud fra en risikobetragtning. Det er derfor ikke nødvendigvis kun en opdatering af kundens identitetsoplysninger. Virksomheden skal foretage en konkret vurdering af hvilke oplysninger, der skal indhentes.

Virksomheden bør sondre mellem, hvorvidt oplysninger ikke er tilstrækkelige eller ikke er korrekte. Behovet for og omfanget af de yderligere kundekendskabsprocedurer, der gennemføres i sådanne tilfælde, kan tilrettelægges ud fra det konkrete forhold, eksempelvis:

1) Er virksomheden i tvivl om hvorvidt nogle konkrete oplysninger er tilstrækkelige, kan virksomheden vurdere, at det kun er dele af kundekendskabsproceduren, der er nødvendig at gennemføre igen.
2) Er virksomheden i tvivl om, hvorvidt de indhentede oplysninger er korrekte, kan virksomheden vurdere, at hele kundekendskabsproceduren skal gennemføres igen.

I tilfælde med utilstrækkelige oplysninger vil der ofte være tale om, at der mangler supplerende oplysninger om den pågældende kunde. Et eksempel på, hvornår de indhentede oplysninger ikke er tilstrækkelige, kan være, at virksomheden får kendskab til oplysninger om kunden, der medfører, at kundens risikoprofil forøges, eller at formålet og den tilsigtede beskaffenhed ændrer sig.

I tilfælde, hvor det viser sig, at nogle af oplysningerne ikke er korrekte, kan det ofte være nødvendigt, at virksomheden kontrollerer alle oplysninger på ny for at sikre sig, at alle oplysninger er korrekte. Det beror dog på, hvilke typer af oplysninger der ikke er korrekte. Har kunden f.eks. afgivet et forkert husnummer ved en fejl, vil det ikke nødvendigvis give anledning til, at hele kundekendskabsproceduren skal gennemføres igen. Er virksomheden f.eks. i tvivl om, hvorvidt de ukorrekte oplysninger er afgivet bevidst af kunden, skal kundekendskabsprocedurerne gennemføres igen. Se afsnit 13 om risikovurdering – kundekendskabsprocedurer.

Bliver en virksomhed i forbindelse med virksomhedens kundekendskab, bekendt med, at oplysninger om en kundes reelle ejere ikke stemmer overens med de oplysninger om kundens reelle ejere, som er registreret i Erhvervsstyrelsens it-system, skal virksomheden indberette dette til Erhvervsstyrelsen hurtigst muligt. Hvis kunden får korrigeret uoverensstemmelsen hurtigst muligt, skal virksomheden ikke indberette uoverensstemmelsen til Erhvervsstyrelsen.

8.8. Enkeltstående aktiviteter, der ikke er transaktioner (rådgivningsopgaver)

Henvisning til hvidvaskloven: § 13. Henvisning til 4. hvidvaskdirektiv: Artikel 2, stk. 3.

Hvis en virksomhed udfører en enkeltstående aktivitet, der ikke er en transaktion, kan kravene i hvidvasklovens § 11 om indhentning og kontrol af identitetsoplysninger på kunden fraviges på baggrund af en risikovurdering.

Et eksempel på en enkeltstående aktivitet er en rådgivningsopgave, hvor der ikke umiddelbart er udsigt til, at kunden vil henvende sig med nye opgaver, f.eks. en skatterådgivningsopgave af helt generel karakter eller en enkeltstående generel rådgivningsopgave på investeringsområdet, som ikke tager kundens konkrete indtjenings- og formueforhold i betragtning. I sådanne tilfælde vil der ikke være etableret en forretningsforbindelse. Vurderingen kan derfor foretages på baggrund af, om aktiviteten er af generel karakter, eller om virksomheden for at udføre aktiviteten skal forholde sig til kundens konkrete oplysninger, herunder kundens indtjenings- og formueforhold. Det afgørende er, at der i den konkrete situation ikke er eller bliver indgået en forretningsforbindelse.

Virksomheden skal efterfølgende kunne godtgøre, at der i det konkrete tilfælde har været tale om en enkeltstående aktivitet, og at risikovurderingen af den konkrete kunde har ført til, at kundekendskabsprocedurer kunne undlades.

Oprettelse af et selskab for en kunde eller salg af et tomt selskab kan ikke betragtes som en enkeltstående aktivitet, selvom kundeforholdet må forventes at blive kortvarigt. Udførelse af sådanne aktiviteter for en kunde vil derfor være etablering af en forretningsforbindelse.

Hvis der er mistanke om hvidvask eller finansiering af terrorisme, skal der altid gennemføres kundekendskabsprocedurer, se afsnit 8.6 om mistanke om hvidvask og finansiering af terrorisme.

9. Indholdet af kundekendskabsprocedurer

Hvidvasklovens § 11 fastsætter de almindelige krav til kundekendskabsprocedurer.

Kundekendskabsprocedurer er en forpligtelse gennem hele forløbet af forretningsforbindelsen med kunden og skal gennemføres på baggrund af en risikovurdering af kundeforholdet. Virksomheden skal således afdække relevante risikofaktorer og ændringer heri i det enkelte kundeforhold for at vurdere omfanget af de kundekendskabsprocedurer, der skal gennemføres.

Det ligger i kravene i § 11, at virksomheden skal

1) indhente identitetsoplysninger på kunden og
2) kontrollere de indhentede identitetsoplysninger ved en pålidelig og uafhængig kilde.

9.1. Indhentelse af identitetsoplysninger

Henvisning til hvidvaskloven: § 11, stk. 1 og 4.

Henvisning til 4. hvidvaskdirektiv: Artikel 13.
Henvisning til 5. hvidvaskdirektiv: Artikel 1, stk. 1, nr. 8.

Virksomheder skal altid indhente identitetsoplysninger om kunden.

Identitetsoplysningerne kan eksempelvis indhentes gennem almindelig kundekontakt, f.eks. ved kundens personlige fremmøde, ved skriftlig korrespondance mellem kunden og virksomheden, ved telefonsamtale eller via virksomhedens it-systemer, herunder f.eks. ved videokontakt via en tilstrækkelig sikker linje eller via f.eks. netbank.

Identitetsoplysninger, i form af kundens navn, kan ligeledes ud fra en konkret vurdering indhentes gennem NemID. I dette tilfælde vil virksomheden ikke også kunne anvende NemID som kontrolkilde, og virksomheden vil derfor skulle kontrollere identitetsoplysningerne via en anden kilde end NemID. Der henvises til afsnit 9.2. nedenfor.

Fysiske personer
Hvis kunden er en fysisk person, skal der indhentes navn og cpr-nr.

Hvis den pågældende kunde ikke har et cpr-nr., skal der indhentes lignende identitetsoplysning, f.eks. for udlændinge et nationalt id-nummer. Når kunden ikke har et cpr-nr. eller lignende, skal identitetsoplysninger omfatte kundens fødselsdato.

For personer, der ikke er hjemmehørende i Danmark, kan et alternativ til cpr-nr. f.eks. være et lignende nationalt id-nummer eller, hvis et sådan ikke haves, oplysning om fødselsdato. Såfremt virksomheden anvender en kundes nationale id-nummer, er det væsentligt at sikre, at der er tale om et unikt id-nummer,

og at id-nummeret er varigt (f.eks. et varigt social security number) eller i hvert fald kundens aktive nationale id-nummer (f.eks. et pasnummer), idet det i enkelte lande er muligt at få et nyt nationalt id-nummer. Det er vigtigt, at virksomheden sikrer sig, at id-nummeret rent faktisk er aktivt/gyldigt, f.eks. at passet ikke er udløbet på identifikationstidspunktet, som vil være det tidspunkt hvor kundeforholdet etableres.

Fødselsdato alene kan kun anvendes i det relativt sjældne tilfælde, hvor der ikke i øvrigt foreligger et unikt id-nummer.

De indhentede identitetsoplysninger, herunder fødselsdato, skal give virksomheden sikkerhed for, at kunden er den, vedkommende udgiver sig for at være.

Det er som udgangspunkt kunden, der skal give identitetsoplysningerne. Det er derfor som hovedregel ikke tilstrækkeligt, at kunden alene oplyser sit cpr-nr., hvorefter virksomheden selv indhenter kundens navn i CPR (Det Centrale Personregister). I tilfælde med begrænset risiko kan det dog være tilstrækkeligt, hvis identitetsoplysninger om kunden indhentes fra kundens arbejdsgiver, f.eks. i tilfældet med arbejdsmarkedspensioner.

Virksomheden skal indhente kundens fulde navn for at sikre, at kontrollen af, at kunden er den, som kunden udgiver sig for at være, er effektiv. Virksomheden kan dog i konkrete tilfælde anlægge en risikobetragtning i forhold til den procedure, virksomheden benytter ved indhentelse af identitetsoplysningerne fra kunden.

Udgangspunktet er, at det af kunden oplyste navn og cpr-nr. skal stemme overens med kontrolkilden, som f.eks. kan være kørekort eller pas. Ved åbenlyse slåfejl kan virksomheden dog acceptere de indhentede oplysninger fra kunden. Mangler dele af kundens fulde navn f.eks. en af kundens fornavne, skal virksomheden indhente identitetsoplysninger igen hos kunden. I praksis vil det eksempelvis skulle ske, hvis virksomheden ikke møder kunden fysisk ved etableringen af forretningsforbindelsen, og kunden udfylder en formular med sine identitetsoplysninger, som derefter vil blive kontrolleret af virksomheden i CPR-registreret. Har kunden f.eks. kun angivet to af sine fire navne, skal virksomheden indhente oplysninger om kundens fulde navn fra kunden.

Hvis virksomheden f.eks. indhenter identitetsoplysningerne via en formular og benytter sig af to kontrolkilder, som fremsendes af kunden samlet, kan virksomheden vurdere, at kunden har fremsendt sit fulde navn ved de to kontrolkilder, og der er ikke tvivl om, at kunden er den, som kunden udgiver sig for at være. Et eksempel på to kontrolkilder kan som nævnt være kørekort og pas.

Ved etableringen af en forretningsforbindelse til en kunde skal virksomheden registrere kundens fulde navn.

Virksomheden skal altid kunne godtgøre over for den myndighed, der fører tilsyn med virksomhedens overholdelse af hvidvaskloven, at virksomheden har et tilstrækkeligt kendskab til kunden.

Juridiske personer
Hvis kunden er en juridisk person, skal der indhentes navn og cvr-nr.

Hvis den pågældende kunde ikke har et cvr-nr., skal der indhentes lignende identitetsoplysninger. Ved udenlandske virksomheder kan anden form for identifikationsoplysning være et registreringsnummer,

f.eks. TIN (Tax Identification Number), LEI (Legal Entity Identifier) eller et andet unikt registreringsnummer.

Hvis kunden ikke har et cvr-nr. eller lignende, er det et krav, at virksomheden som minimum har oplysninger om kundens juridiske status (virksomhedsform), f.eks. om der er tale om et selskab med begrænset ansvar, en fond, trust eller andet.

9.2. Kontrol af identitetsoplysninger

Henvisning til hvidvaskloven: § 11, stk. 1, nr. 2 og stk. 4.

Henvisning til 4. hvidvaskdirektiv: Artikel 13, stk. 1, litra a.
Henvisning til 5. hvidvaskdirektiv: Artikel 1, stk. 1, nr. 8, litra a.

Om elektroniske identifikationsmidler og relevante tillidstjenester henvises til:
Europa-Parlamentets og Rådets forordning 910/2014/EU af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (eIDAS-forordning).

De identitetsoplysninger, som virksomheden har indhentet på en kunde, skal kontrolleres ved dokumenter, data eller oplysninger, der er indhentet fra en pålidelig og uafhængig kilde. Det betyder, at kontrol af kundens identitet skal ske gennem en anden kilde end kunden.

Den pålidelige kilde kan være en offentlig myndighed, men det kan også være en anden pålidelig ekstern kilde. Det er samtidig vigtigt, at der er tale om en aktuel kilde. Dette er særlig relevant i forhold til fysiske id-dokumenter, hvor virksomheden skal være opmærksom på, om dokumentet stadig er gyldigt.

Elektroniske identifikationsmidler kan benyttes i forbindelse med kundekendskabsprocedurer. Pålidelig og uafhængig kilde kan eksempelvis omfatte elektroniske identifikationsmidler, relevante tillidstjenester, eller enhver anden sikker form for fjernidentifikationsproces eller elektronisk identifikationsproces, der er reguleret, anerkendt, godkendt eller accepteret af de kompetente nationale myndigheder.

Det er relevant at sikre, at dokumentet, der bruges til kontrol, er gyldigt, da personens identitetsoplysninger kan have ændret sig, f.eks. oplysninger om nationalitet, ændring af unikt id-nummer mv.

Virksomheden skal ud fra en risikobetragtning vurdere, om identitetsoplysningerne bør ajourføres på et senere tidspunkt, herunder om identitetsbeviser skal indhentes igen, fordi tidligere identitetsbeviser er udløbet i mellemtiden.

Virksomheden skal indhente et nyt legitimationsdokument, hvis der er opstået tvivl om dokumentets ægthed.

Det er en konkret vurdering, hvor megen dokumentation, data eller oplysninger der skal til, for at der er tale om en tilstrækkelig kontrol af en kundes identitetsoplysninger. Der må dog ikke være anledning til

tvivl om, at kunden er den person, som kunden udgiver sig for at være. Virksomheden skal i den forbindelse risikovurdere sine kunder, og denne vurdering kan medføre, at der skal gennemføres skærpede kundekendskabsprocedurer.

Hvis virksomheden vurderer, at der er øget risiko ved forretningsforbindelsen, skal virksomheden foretage yderligere handlinger, uanset om kundens identitetsoplysninger er kontrolleret. Virksomheden kan kræve yderligere dokumenter fra kunden, foretage opslag i eksterne kilder eller kræve, at første betaling sker fra en bankkonto i kundens navn mv. Virksomheden skal således vurdere, hvilke procedurer den vil benytte for at sikre, at der ikke er tvivl om, at kunden er den, som kunden udgiver sig for at være. Se afsnit 14 om skærpede kundekendskabsprocedurer.

9.3. Eksempler på kontrol ved en pålidelig og uafhængig kilde

En kontrol ved en pålidelig og uafhængig kilde kan f.eks. være en søgning i et pålideligt og uafhængigt register eller database eller et dokument udstedt af en offentlig myndighed.

Udgangspunktet er, at virksomheden skal have forevist originale fysiske legitimationsdokumenter, når kunden er fysisk til stede. Hvis kunden er fysisk til stede, bør kunden som udgangspunkt også være i stand til at fremvise legitimationsdokumenter og ikke kun en kopi af disse.

Fysiske personer

For fysiske personer kan kontrollen f.eks. bestå af opslag i CPR (Det Centrale Personregister), oplysninger fra Skatteforvaltningen, offentligt udstedte legitimationsdokumenter, som f.eks. pas, kørekort, NemID, legitimationskort, sundhedskort, dåbs- eller navneattest.

Der er ikke krav om, at kunden fremviser billedlegitimation. I de tilfælde, hvor kunden møder fysisk op hos virksomheden, vil kontrol i form af billedlegitimation, f.eks. pas eller kørekort, dog give virksomheden en øget sikkerhed for, at kunden er den person, som kunden udgiver sig for at være. Det vil især være aktuelt i tilfælde, hvor der er tale om høj risiko.

Juridiske personer

For juridiske personer kan kontrollen f.eks. bestå af opslag i CVR (Det Centrale Virksomhedsregister), oplysninger fra Skatteforvaltningen, kopi af stiftelsesdokument og vedtægter.

Hvis kunden er etableret uden for Danmark, kan lignende oplysninger fra tilsvarende offentlige myndigheder eller registre benyttes til at kontrollere den juridiske persons identitetsoplysninger.

For juridiske personer uden et cvr-nr., f.eks. visse foreninger, kan kontrol ske ved indhentelse af kopi af foreningens stiftelsesdokument og vedtægter, hvis sådanne findes, samt oplysninger om de personer, der kan handle på vegne af foreningen. Stiftelsesdokumentet kan f.eks. være kopi af referat fra den stiftende generalforsamling. Oplysninger om, hvem der kan handle på vegne af foreningen, vil typisk fremgå af vedtægterne, f.eks. formand og kasserer i forening, og disses navne vil typisk fremgå af referat af foreningens sidste afholdte generalforsamling.

Der findes mange forskellige typer foreninger, herunder interesseforeninger og frivillige foreninger. Disse foreninger dækker et bredt spektrum, også i forhold til risiko, og virksomheden bør derfor i forbindelse med deres kundekendskabsprocedurer tage højde for dette. Virksomheden skal på den baggrund ud fra

en risikovurdering fastlægge, hvilke oplysninger virksomheden har behov for. Virksomheden kan eksempelvis vurdere den enkelte forening på baggrund af en række faktorer, som f.eks. foreningens formål, herunder medlemskredsen, om foreningen er medlem af et anerkendt hovedforbund eller hovedforening, om foreningen er godkendt som en folkeoplysende forening og offentlige tilgængelig information om foreningen, samt hvordan foreningen finansieres.

Når kunden er en juridisk person, skal virksomheden være opmærksom på kravet om kontrol af de reelle ejeres identitet, se afsnit 9.6 om reelle ejere.

Praktiske eksempler:
Uanset nedenstående eksempler er det altid en konkret vurdering i det enkelte kundeforhold, hvilke oplysninger der skal indhentes fra kunden, og hvornår disse er tilstrækkeligt kontrolleret ved uafhængige og pålidelige kilde(r). Virksomheden skal dog altid indhente navn og som udgangspunkt cpr-nr. eller lignende, hvis den pågældende ikke har et cpr-nr., se nærmere herom i afsnit 9.6.2.

Et eksempel på en proces for hvordan indhentning af oplysninger og kontrol af en fysisk kunde kan foregå, ud fra en risikovurdering, og hvor kontrollen sker ved brug af to kilder:

1) Kunden oplyser sit navn og cpr-nr. til virksomheden.
2) Kunden foreviser virksomheden sit kørekort.
3) Virksomheden kontrollerer navn og cpr-nr. ved opslag i CPR.
4) Virksomheden kontrollerer, at oplysningerne på kørekortet stemmer overens med kundens oplyste navn og cpr-nr. Samtidig kontrollerer virksomheden, at billedet på kørekortet stemmer overens med kundens udseende.
5) Virksomheden opbevarer dokumentation for kontrollen af identitetsoplysningerne, dvs. i dette tilfælde kopi af kørekort og revisionsspor for opslag i CPR.

For nogle kunder kan det være svært at fremskaffe standard legitimationsdokumenter som f.eks. sundhedskort og kørekort. Denne type kunder kan f.eks. være arbejdstagere fra udlandet, udenlandske studerende, asylansøgere, flygtninge, hjemløse og mindreårige.

Virksomheden bør i den forbindelse have en tilgang til kunden, der kompenserer for de udfordringer, som kunden har ved at skulle fremskaffe dokumentation for hans/hendes identitet.

Det kan derfor i nogle tilfælde være nødvendigt for en virksomhed at benytte sig af andre kontrolkilder end sædvanligt. Det kan være i form af andre kilder, som kunden er i besiddelse af, men som virksomheden almindeligvis ikke benytter sig af. Det kan f.eks. være en forevisning af et brev fra en offentlig myndighed til kunden sammenholdt med en opholdstilladelse.

Det kan i nogle tilfælde også være nødvendigt at kontakte en offentlig myndighed og bede denne om at bekræfte personens identitet.

Udenlandske arbejdstagere og studerende vil ikke altid fra starten af deres ophold i Danmark have et cpr-nr., og personer, der har fået tildelt et administrativt personnummer af f.eks. Skatteforvaltningen eller Styrelsen for International Rekruttering og Integration (SIRI), vil ikke altid på tidspunktet for henvendelsen til banken være blevet folkeregisterregistreret med bopæl i CPR (bopælsregistreret). Dog kan visse kunder have behov for at oprette en dansk bankkonto til brug for at opfylde betingelserne for deres opholds-

tilladelse, selv om de endnu ikke er blevet bopælsregistreret i CPR. Dette er f.eks. tilfældet ved arbejdstagere fra ikke EU-lande, hvor udlændingeloven i visse tilfælde stiller krav til, at de får deres løn udbetalt til en konto i Danmark som betingelse for opholdstilladelse. I disse tilfælde kan virksomheden f.eks. benytte kundens foreløbige arbejdstilladelse eller opholdstilladelse, der for tredjelandes statsborgere indeholder vedkommendes tildelte administrative personnummer, som kontrolkilde af kundens identitetsoplysninger sammen med andre kilder som f.eks. pas. I tvivlstilfælde om f.eks. gyldigheden af opholdstilladelsen for arbejdstagere fra ikke EU-lande kan virksomheden rette henvendelse til SIRI, der kan bekræfte denne.

9.4. Distancekunder

Der er bedre mulighed for, at virksomheden kan sikre sig, at kunden er den person, som kunden udgiver sig for at være, når virksomheden møder kunden fysisk. Når kunden ikke er fysisk til stede (distanceforhold), skal virksomheden forholde sig til den potentielt øgede risiko ved dette. Billedlegitimation vil ikke give den samme sikkerhed som ved fysisk fremmøde, medmindre virksomheden f.eks. benytter sig af digitale systemer, der giver virksomheden mulighed for, at kunden fremviser sin billedlegitimation, samtidig med at virksomheden kan se kunden via digitale systemer, f.eks. via et live videolink. Dette vil være med til at sikre en øget sikkerhed for, at kunden er den, som kunden udgiver sig for at være.

Omfanget af kontrollen af identitetsoplysninger om kunder, der ikke er fysisk til stede, afhænger også af egenskaber og karakteristika ved det produkt eller den ydelse, som forretningsforbindelsen angår i forhold til risikoen for hvidvask og finansiering af terrorisme. Virksomheden skal således altid ud fra en risikovurdering vurdere, hvilke kontrolkilder der er nødvendige for at sikre sig, at kendskabet til kunden er tilstrækkeligt, herunder om der skal anvendes mere end én kilde til kontrol af identitetsoplysninger eller risikobegrænsende tiltag. Et eksempel på et risikobegrænsende tiltag kan være, at virksomheden sender et fysisk brev med en unik kode til kundens folkeregisteradresse, som kunden efterfølgende skal oplyse virksomheden om f.eks. telefonisk eller ved, at kunden logger på virksomhedens hjemmeside, se afsnit 9.5. nedenfor om brug af NemID for yderligere eksempler på risikobegrænsende tiltag.

9.5. Brug af NemID eller anden form for elektronisk ID

NemID kan bruges i forbindelse med kontrol af kundens identitetsoplysninger ved brug af PID cpr-match til kontrol af cpr-nr. og offentlig digital signatur (OCES) til kontrol af navn.

NemID er en pålidelig og uafhængig kilde, men i de tilfælde, hvor der ikke kun er tale om begrænset risiko, vil det være nødvendigt for virksomheden at benytte sig af andre kontrolkilder eller risikobegrænsende tiltag sammen med NemID for at kunne opnå tilstrækkeligt kendskab til kunden i forbindelse med gennemførelse af kundekendskabsproceduren. Virksomheden skal i den forbindelse være opmærksom på den potentielt øgede risiko, der er for kundeforhold, hvor kunden ikke møder fysisk frem. Se afsnit 9.4. ovenfor om distancekunder.

Virksomheder, der er omfattet af hvidvaskloven, kan anvende oplysninger, der eksempelvis er indhentet gennem elektroniske identifikationsmidler, relevante tillidstjenester i henhold til eIDAS-forordningen, eller enhver anden sikker form for fjernidentifikationsproces eller elektronisk identifikationsproces, der er reguleret, anerkendt, godkendt eller accepteret af de kompetente myndigheder. Det følger af eIDAS-forordningen, at virksomheder og personer er forpligtet til at anerkende elektronisk identifikationsmiddel

(eID) fra andre EU- eller EØS-lande. De former for eID, der ønskes anerkendt, skal anmeldes til Kommissionen. De vil derefter blive opført på Kommissionens liste over anmeldte eID, jf. eIDAS-forordningen artikel 9.

Virksomheden kan kun bruge NemID eller anden form for elektronisk ID, som den eneste kontrolkilde i de tilfælde, hvor virksomheden har foretaget en risikovurdering af det konkrete kundeforhold og vurderet, at der kan gennemføres lempede kundekendskabsprocedurer, og at virksomheden kan opnå tilstrækkeligt kendskab til kunden ved brug af NemID eller anden form for elektronisk ID. Virksomheden skal dog også være opmærksom på, at der i forhold til det konkrete kundeforhold kan være behov for at indhente andre oplysninger, f.eks. om forretningsforbindelsens formål og tilsigtede beskaffenhed.

Hvis forretningsforbindelsen med kunden indeholder produkter eller ydelser, hvor det fremgår af den nationale risikovurdering for henholdsvis hvidvask og finansiering af terrorisme, at der er tale om produkter eller ydelser med en høj risiko, vil kundeforholdet som udgangspunkt ikke udgøre en begrænset risiko. Det betyder, at i sådanne kundeforhold vil NemID eller anden form for elektronisk ID ikke være tilstrækkeligt til at sikre det fornødne kendskab til kunderne.

NemID eller anden form for elektronisk ID som kontrolkilde kan suppleres med andre kontrolkilder eller risikobegrænsende tiltag. Sådanne tiltag kan f.eks. være:

1) Den første transaktion sker via kundens Nemkonto eller en anden bankkonto registreret i kundens navn.
2) Virksomheden sender en unik kode til et mobiltelefonnummer, som virksomheden har kontrolleret tilhører kunden, eller med fysisk post til kundens folkeregisteradresse.
3) Virksomheden kontrollerer kundens IP-adresse i forhold til geolokation.
4) Virksomheden stiller kunden spørgsmål, hvor virksomheden efterfølgende kan kontrollere rigtigheden af svarene ved en pålidelig og uafhængig kilde, f.eks. oplysninger fra kundens personlige skattemappe.

Ovenstående eksempler skal ikke anses som en udtømmende liste, da der kan være flere måder, hvorpå virksomheden kan benytte sig af risikobegrænsende tiltag. Samtidig skal virksomheden være opmærksom på, at virksomheden selv skal foretage en konkret vurdering af, hvilke eventuelle risikobegrænsende tiltag der er tilstrækkelige i forhold til kendskab til kunden.

Virksomheden skal kunne godtgøre over for den myndighed, der fører tilsyn med overholdelsen af hvidvaskloven på området, at virksomhedens kendskab til kunden er tilstrækkeligt i forhold til risikoen for hvidvask og finansiering af terrorisme. Virksomhedens kundekendskabsprocedurer og herunder kontrollen af identitetsoplysninger skal derfor være tilrettelagt på en sådan måde, at virksomheden har et tilstrækkeligt kendskab til den konkrete kunde.

9.6. Reelle ejere

Henvisning til hvidvaskloven: § 11, stk. 1, nr. 3, § 2, stk. 1, nr. 1 og 9 samt § 15 a.

Henvisning til 4. hvidvaskdirektiv: Artikel 13, stk. 1, litra b.
Henvisning til 5. hvidvaskdirektiv: Artikel 1, stk. 1, nr. 8, litra b.

Henvisning til Erhvervsstyrelsens vejledning: Reelle ejere, vejledningen handler om reelle ejere, herunder hvem, hvad og hvor der skal registreres.

Begrebet reelle ejere anvendtes i den tidligere hvidvasklovgivning og anvendes nu både i hvidvasklovgivningen og i regelsættet om registrering af reelle ejere. Begrebet i de to lovgivninger har nu samme baggrund i 4. hvidvaskdirektiv, og der er dermed tale om et fælles begreb. I regelsættet om registrering af reelle ejere er der krav om, at forskellige juridiske personer mv. skal registrere deres reelle ejere i et register. I hvidvasklovgivningen er der krav om, at virksomheder, som er omfattet af hvidvaskloven, skal identificere og kontrollere kunders reelle ejere.

Nogle juridiske personer mv. er ikke omfattet af kravet om registrering af reelle ejere i regelsættet om registrering af reelle ejere, men denne undtagelse gælder ikke for hvidvasklovens krav, til at virksomheder skal identificere og kontrollere deres kunders reelle ejere som led i virksomhedens kundekendskabsprocedurer. Virksomheder skal derfor også identificere reelle ejere, hvis deres kunde f.eks. er en frivillig forening eller en andelsboligforening, selvom disse ikke er omfattet af reglerne om registrering af reelle ejere.

Da reglerne om reelle ejere har samme baggrund, kan en virksomhed, der efter hvidvaskloven skal identificere sine kunders reelle ejere, benytte Erhvervsstyrelsens Vejledning om reelle ejere som hjælp til fortolkning af begrebet og vurdering af, hvem der skal identificeres, samt til fastlæggelse af ejer- og kontrolstruktur. Virksomhederne skal dog være opmærksomme på, at hvidvasklovens krav om, hvilke oplysninger der skal indhentes i henhold til kundekendskabsprocedurerne, adskiller sig fra de oplysninger, der skal registreres om reelle ejere i CVR.

Virksomheden skal som led i sine kundekendskabsprocedurer identificere kundens reelle ejere.

Virksomheden skal:

1) indhente identitetsoplysninger om den eller de reelle ejere,
2) gennemføre rimelige foranstaltninger for at kontrollere den eller de reelle ejeres identitet og
3) hvis kunden er en juridisk person, skal virksomheden klarlægge den juridiske persons ejer- og kontrolstruktur.

9.6.1. Definition af reelle ejer

En kundes reelle ejer er den eller de fysiske personer, der i sidste ende ejer eller kontrollerer kunden, eller den eller de fysiske personer, på hvis vegne en transaktion eller aktivitet gennemføres.

Reelle ejere kan kun være fysiske personer, og virksomheden skal klarlægge hele kundens ejer- og strukturkæde og finde frem til, hvem der i sidste ende ejer eller kontrollerer kunden.

Hvis en kunde eksempelvis er et selskab A, som ejes 100 pct. af et andet selskab B, skal virksomheden identificere den eller de fysiske personer, der ejer og kontrollerer selskab B.

Når virksomheden skal identificere, hvem der er kundens reelle ejere, skal virksomheden vurdere hvilke personer, der har en tilstrækkelig del af kapitelandele, stemmerettigheder eller kan kontrollere virksomheden på anden vis. En indikator for, hvad der er en tilstrækkelig del, vil som udgangspunkt være, at personen har mere end 25 pct. af ejerandele og/eller kontrollen. Det er dog vigtigt at fremhæve, at procentgrænsen kun er en indikator for reelt ejerskab eller kontrol.

Udgangspunktet er, at kunden har reelle ejere og kan identificere dem. Der er dog tilfælde, hvor der ikke er fysiske personer, der ejer og/eller kontrollerer kunden i tilstrækkelig grad til, at de bliver omfattet af definitionen af reelle ejere. I disse tilfælde skal kundens daglige ledelse i stedet betragtes som den eller de reelle ejere. Dette kan for eksempel være, når en kunde er en forening, som ikke har reelle ejere, hvorefter det er den daglige ledelse, der må betragtes som foreningens reelle ejere.

Hvis virksomheden har identificeret en eller flere reelle ejere, men der alligevel er tvivl om, hvorvidt de pågældende personer rent faktisk er de reelle ejere, skal både de identificerede personer og den daglige ledelse betragtes som reelle ejere af kunden.

Virksomheden skal notere de foranstaltninger, som virksomheden har iværksat i forsøget på at identificere de reelle ejere. Noteringen skal ske, inden virksomheden betragter den daglige ledelse som kundens reelle ejere.

Virksomheden skal gemme de oplysninger, som virksomheden har indhentet og brugt til at identificere kundens reelle ejere. Det kan f.eks. være hvis virksomheden har udformet et diagram over den "ejerkæde", der er fra virksomhedens kunde og frem til kundens reelle ejere, eller hvis virksomheden f.eks. har klarlagt kundens ejer- og kontrolstrukturen ved en udskrift af Erhvervsstyrelsens register over reelle ejere.

Virksomheden kan i kundeforhold, som indebærer en begrænset risiko, også indhente de oplysninger og noteringer, som kunden har benyttet i forbindelse med, at kunden har identificeret sine reelle ejere. Dog bør virksomheden forholde sig til kundens oplysninger og noteringer, inden disse eventuelt lægges til grund som del af virksomhedens undersøgelse af kunden.

Kravet om indhentning og kontrol af reelle ejere gælder ikke for selskaber, hvis ejerandele handles på et reguleret marked eller et tilsvarende marked, som er undergivet oplysningspligt i overensstemmelse med EU-retten eller tilsvarende internationale standarder, der sikrer passende gennemsigtighed. I situationer, hvor kundens ejerandele handles på et sådant reguleret marked indenfor EU/EØS eller et tilsvarende marked udenfor EU/EØS, der er underlagt tilsvarende oplysningspligt som indenfor EU/EØS, skal virksomheden således ikke identificere og kontrollere reelle ejere af kunden. Ved vurderingen af tilsvarende oplysningspligt i markeder udenfor EU/EØS skal der i denne forbindelse forstås de krav til oplysningspligt, der følger af relevante artikler i markedsmisbrugsforordningen (2014/596/EU), transparensdirektivet (2004/109/EF) og prospektdirektivet (2003/71/EF) samt med anden EU-regulering, der følger af disse relevante artikler.

9.6.2. Indhentelse af identitetsoplysninger

Virksomheder skal altid indhente oplysninger om den eller de reelle ejeres identitet (bortset fra ejere af børsnoterede selskaber).

Kravet om at indhente oplysninger om den eller de reelle ejeres identitet gælder f.eks., når kunden er en juridisk person, eksempelvis et selskab, en fond, en forening eller en anden juridisk enhed. Det gælder også i forbindelse med en nominee-ordning, hvor det er den person, på hvis vegne nomineen optræder, der er den reelle ejer.

Virksomheden skal indhente oplysninger, således at virksomheden med sikkerhed ved, hvem de reelle ejere er. Det beror på en konkret vurdering, hvordan og hvilke oplysninger virksomheden skal indhente om kundens reelle ejere, men vurderingen kan aldrig føre til, at der ikke indhentes nogle identitetsoplysninger. Vedrørende identitetsoplysninger på reelle ejere henvises der i øvrigt til vejledningens afsnit 9.1. om fysiske personer.

Virksomheden skal indhente navn og som udgangspunkt CPR-nr., eller andre lignende oplysninger, hvis personen ikke har et CPR-nr., på de reelle ejere.

Uanset hvilke oplysninger virksomheden indhenter, bør fødselsdato altid være en del af de indhentede oplysninger.

I visse situationer kan det være muligt at undlade at indhente CPR-nummer på den eller de reelle ejere. Dette vil dog kun være tilfældet, hvis virksomheden på anden måde vil kunne opnå en lige så sikker identifikation af de reelle ejere, som hvis virksomheden blev oplyst om CPR-nummeret.

Dette kan eksempelvis være tilfældet, hvis der er tale om en offentligt kendt person. Med ”offentlig kendt” menes, at personen skal være alment kendt i den brede offentlighed i ind- eller udland. Det kan f.eks. være borgmestre, ejere af, direktører i eller bestyrelsesformænd for store almenkendte virksomheder, erhvervsfolk, departementschefer eller styrelsesdirektører.

Hvis den eller de reelle ejere ikke er bosat i Danmark og ikke har et dansk CPR-nummer, skal oplysningerne som udgangspunkt indeholde et unikt og varigt eller et unikt og aktivt id-nummer for den reelle ejer. Hvis den eller de reelle ejere hverken har et unikt og varigt eller et unikt og aktivt id-nummer, skal fødselsdato indgå i de oplysninger, som virksomheden indhenter.

For så vidt angår udenlandske reelle ejere vil der i visse tilfælde være mulighed for at undlade at indhente id-nummer, hvor virksomheden vil kunne opnå en lige så sikker identifikation af den reelle ejer, som hvis virksomheden udbad sig et id-nummer. Dette vil være tilfældet, hvis der er tale om en offentligt kendt person.

Den pågældende offentligt kendte reelle ejer skal kunne identificeres – og identiteten skal kunne kontrolleres, jf. nærmere afsnit 9.6.3. – ved pålidelige kilder, f.eks. på internettet. En pålidelig kilde på internettet kan f.eks. være en hjemmeside fra en offentlig myndig eller en større virksomhed.

Virksomheden skal sørge for at indhente tilstrækkelige oplysninger for at sikre, at den reelle ejer er den person, som kunden har oplyst. Virksomheden skal altid kunne godtgøre overfor den myndighed, der fører tilsyn med virksomhedens overholdelse af hvidvaskloven, at virksomheden har identificeret og kontrolleret oplysningerne om den reelle ejer tilstrækkeligt, jf. nærmere afsnit 9.6.3. Hvidvasklovens krav om

opbevaring af dokumentation for udførte kundekendskabsprocedurer gælder i alle tilfælde, også hvor kilder er hentet fra eksempelvis internettet.

Bliver virksomheden opmærksom på væsentlige ændringer i kundeforholdet, skal virksomheden tage stilling til, om den skal indhente nye oplysninger om, hvem de reelle ejere er. Væsentlige ændringer kan både omfatte virksomhedens forretningsforbindelse til kunden, f.eks. en større udvidelse af kundeengagementet, eller ændringer i kundens virksomhed, f.eks. ny ledelse, nye forretningsforbindelser eller nye reelle ejere. Bliver virksomheden opmærksom på, at en reel ejer er en politisk eksponeret person, skal virksomheden vurdere, om dette skal have indflydelse på risikovurderingen af kunden, herunder om virksomheden i den forbindelse skal indhente yderligere oplysninger om kunden og de reelle ejere. Hvis virksomheden vurderer, at kundens risiko er blevet forøget, skal den altid vurdere, om virksomhedens oplysninger om de reelle ejere er tilstrækkelige.

9.6.3. Kontrol af reelle ejeres identitetsoplysninger

Kontrollen af de indhentede identitetsoplysninger skal foretages ud fra en risikovurdering af, hvad der er rimelige foranstaltninger i forhold til den konkrete kunde.

Virksomheden skal dermed altid indhente identitetsoplysninger og derefter foretage en risikovurdering af, hvorledes og i hvilket omfang disse skal kontrolleres. Se afsnit 9.6.2. om indhentelse af identitetsoplysninger. Virksomheden skal endvidere indhente et registreringsbevis eller et ekstrakt af oplysningerne i Erhvervsstyrelsens it-system, når den etablerer en forretningsforbindelse med et selskab eller en anden juridisk enhed eller en trust eller et lignende juridisk arrangement, som er forpligtet til at registrere oplysninger om reelle ejere hos Erhvervsstyrelsen. Ved ekstrakt af oplysninger i Erhvervsstyrelsens it-system menes den pdf-oversigt, som kan hentes vedrørende den pågældende virksomhed, hvor virksomhedens reelle ejere fremgår.

At der skal gennemføres "rimelige foranstaltninger" for at kontrollere en reel ejers identitetsoplysninger betyder, at virksomheden f.eks. ud fra en risikovurdering kan vurdere det tilstrækkeligt at anvende oplysninger om de reelle ejere, der udleveres af kunden, og sammenholde disse med oplysningerne indhentet fra Erhvervsstyrelsens it-system, et tilsvarende EU/EØS-register over reelle ejere eller et tilsvarende udenlandsk register udenfor EU/EØS som i eksempelvis USA, England, Canada eller Australien. Det vil være tilstrækkeligt, hvis virksomheden har vurderet, at kundeforholdet udgør begrænset risiko. Virksomheden kan også i konkrete tilfælde vurdere, at kontrollen kan undlades helt eller kun skal foretages over for nogle af de reelle ejere i en kundes ejerkreds. Et eksempel herpå er en forening med begrænset risiko, hvor virksomheden ud fra en risikovurdering konkret kan vælge kun at foretage en kontrol af identifikationsoplysningerne for de tegningsberettigede medlemmer af foreningens bestyrelse.

Virksomheden skal altid foretage kontrol af kundens egne oplysninger. Se afsnit 9.2 om kontrol af identitetsoplysninger.

Hvis den eller de reelle ejer(e) er bosat her i landet, kan virksomhedens risikovurdering føre til, at det anses tilstrækkeligt at sammenholde de fra kunden modtagne identitetsoplysninger med oplysningerne i CPR-registeret eller på anden måde, eventuelt via oplysninger fra Skatteforvaltningen, f.eks. årsopgørelse.

Hvis virksomheden vurderer, at et kundeforhold udgør en begrænset risiko, kan virksomheden benytte Erhvervsstyrelsens register over reelle ejere som kilde til at kontrollere, hvem kundens reelle ejere er.

Det skal dog bemærkes, at den offentligt tilgængelige del af registeret over reelle ejere ikke indeholder oplysninger om den reelle ejers cpr-nr. Brug af registeret som kilde til kontrol er derfor kun muligt i tilfælde med begrænset risiko, hvor det er vurderet, at dette er tilstrækkeligt som rimelig foranstaltning for at kontrollere den reelle ejer. Det vil som udgangspunkt være i tilfælde, hvor både kunden og produktet udgør en begrænset risiko.

Hvis virksomheden vurderer, at der er en øget risiko ved kundeforholdet, vil det ikke være tilstrækkeligt alene at kontrollere identitetsoplysningerne udleveret af kunden i forhold til oplysningerne indhentet fra Erhvervsstyrelsens it-system. Her kan der være behov for, at den eller de reelle ejeres identitet kontrolleres ved en eller flere uafhængige kilder, f.eks. ved kopi af et offentligt udstedt identifikationsdokument, se afsnit 9.3 om eksempler på kontrol ved en pålidelig og uafhængig kilde.

9.6.4. Klarlæggelse af ejer- og kontrolstruktur

Når kunden er en juridisk person, herunder en forening, skal virksomheden altid klarlægge den juridiske persons ejer- og kontrolstruktur. Dette gælder også for ikke-juridiske personer, hvis kunden f.eks. er en trust eller et lignende juridisk arrangement. Med ejer- og kontrolstruktur forstås, at virksomheden indhenter oplysninger om eksempelvis kundens ejere, ledelse, tegningsregler, ejeraftaler, kapitalklasser eller lignende. Virksomheden skal selv vurdere, hvilke oplysninger der er relevante for at klarlægge kundens ejer- og kontrolstruktur.

Virksomhedens klarlæggelse af en kundes ejer- og kontrolstruktur bidrager til at afdække, hvem der er kundens reelle ejere. Virksomheden kan derfor ofte med fordel klarlægge ejer- og kontrolstrukturen først for at få klarhed over, hvem virksomheden skal identificere og eventuelt kontrollere som kundens reelle ejere.

Det er nødvendigt, at virksomheden altid klarlægger hele kundens ejer- og kontrolstruktur, dvs. at virksomheden skal klarlægge hele ejerkæden af eventuelle juridiske personer (virksomheder) for at finde frem til de personer, der i sidste ende ejer eller kontrollerer kunden. En klarlæggelse af ejer- og kontrolstukturen omfatter derfor også eventuelle udenlandske juridiske eller fysiske ejere.

Virksomheden kan ud fra en risikovurdering beslutte, hvilke undersøgelser der er nødvendige at iværksætte for at klarlægge ejer- og kontrolstrukturen. Det kan derfor i tilfælde med begrænset risiko, f.eks. hvor ejer- og kontrolstrukturen er transparent, og hvor der ud fra en konkret risikovurdering ikke er identificeret risikofaktorer, som direkte eller indirekte relaterer sig til ejer- og kontrolstrukturen, være tilstrækkeligt, at virksomheden klarlægger strukturen ved at udfærdige et koncerndiagram, der viser ejerandelene. Alternativt kan virksomheden anvende de oplysninger som er indhentet via CVR (Det Centrale Virksomhedsregister), herunder om virksomhedens reelle ejere.

I tilfælde med øget risiko kan det være nødvendigt, at virksomheden indhenter dokumentation for ejerandelene i form af vedtægter, aktiebog eller lignende.

Virksomheden bør dog i alle forretningsforbindelser med juridiske personer klarlægge ejer- og kontrolstrukturen, men virksomheden fastlægger herefter selv omfanget af foranstaltningerne og kontrollerne ud fra virksomhedens risikovurdering af forretningsforbindelsen.

Konkrete eksempler på identifikation af reelle ejere

Nedenfor følger en række eksempler på identifikation af reelle ejere. Hvordan en forretningsforbindelses reelle ejere skal identificeres, er i henhold til hvidvaskloven altid en konkret vurdering, som virksomheden selv skal foretage ved etablering af en forretningsforbindelse. Virksomheden skal som minimum altid indhente navn og som udgangspunkt cpr-nr. eller lignende, hvis kundens reelle ejere ikke har et cpr-nr.

Offentligt ejet
I forretningsforbindelser, hvor kunden er eller ejes 100 pct. af en offentlig myndighed, herunder en kommune, statsejet virksomhed mv., vil der ikke være fysiske personer, der ejer eller kontrollerer kunden i et sådant omfang, at vedkommende omfattes af definitionen af reel ejer. Derfor skal den daglige ledelse betragtes som den reelle ejer.

Hvis kunden er en statslig myndighed, en styrelse eller en selvstændig offentlig ejet virksomhed, er det direktøren, der skal betragtes som reel ejer. Hvis kunden er et ministerium, er det departementschefen, der skal betragtes som reel ejer.

Hvis kunden f.eks. er et aktieselskab, der er 100 pct. ejet af en statslig myndighed, er det den daglige ledelse i aktieselskabet (direktionen), der skal betragtes som reelle ejere.

Er kunden en offentlig/kommunalt ejet daginstitution eller lignende, skal virksomheden betragte daginstitutionens daglige ledelse som den eller de reelle ejere i henhold til hvidvaskloven. Hvis en daginstitution f.eks. skal lease en opvaskemaskine, er det den, der dagligt leder og træffer beslutninger på vegne af institutionen, der skal betragtes som reel ejer.

Er det selve kommunen, der er kunden, er det en konkret vurdering, hvem der varetager den daglige ledelse. I en kommune kan det være borgmesteren eller en anden fysisk person, der har lignende beføjelser over den del af kommunen, som indgår aftalen med virksomheden, der i det konkrete tilfælde vil være den, der varetager den daglige ledelse. Kommuner kan have forskellige administrative strukturer, f.eks. hvor de har flere borgmestre eller rådmænd. Er det f.eks. Børn og unge-udvalget i Københavns Kommune, der træffer beslutning om opførsel af nye spejderhytter og dermed er bygherre, kan det vurderes, at det er borgmesteren for Børn og unge-udvalget, der skal betragtes som den reelle ejer i det konkrete eksempel.

Frivillige foreninger, andelsboligforeninger, almene boligorganisationer mv.
Når virksomheden skal identificere de reelle ejere af en kunde, kan virksomheden tage udgangspunkt i, hvilke type virksomhed eller anden juridisk enhed, som kunden ligner. Er kunden f.eks. en frivillig forening, en andelsboligforening eller en almen boligorganisation, kan virksomheden tage udgangspunkt i, hvordan virksomheden identificerer reelle ejere i andre typer foreninger, f.eks. de foreninger, som er omfattet af regelsættet om registrering af reelle ejere.

Som udgangspunkt skal virksomheden fastlægge, om der er en eller flere personer, der ejer eller kontrollerer foreningen i overensstemmelse med definitionen af reelle ejere. Er der ingen personer, der kan identificeres som reelle ejere, skal den daglige ledelse betragtes som reelle ejer(e).

I foreninger vil det ofte enten være foreningens bestyrelse eller direktionen, hvis foreningen har en sådan, der vil udgøre foreningens daglige ledelse, og som dermed skal betragtes som reelle ejere. Det beror dog på en konkret vurdering af den enkelte forening og dennes forhold.

Til brug for identifikation af de reelle ejere kan virksomheden f.eks. indhente foreningens stiftelsesdokument, vedtægter eller referater fra generalforsamlingen.

Kontrollen af oplysningerne skal foretages ud fra en risikovurdering af, hvad der er rimelige foranstaltninger i forhold til den konkrete kunde. Virksomheder skal her være opmærksom på, at der er mange forskellige typer foreninger i Danmark. Foreninger dækker derfor over et meget bredt spænd i forhold til risikoprofil, hvilket har betydning for de kontrolforanstaltninger, der skal foretages.

Ud fra en konkret risikovurdering vil det i nogle tilfælde med begrænset risiko ikke være nødvendigt at foretage en kontrol af de udleverede identitetsoplysninger. Det kan også efter en konkret vurdering være berettiget kun at foretage en kontrol af identitetsoplysningerne for de tegningsberettigede medlemmer af en forenings bestyrelse, når virksomheden har vurderet, at foreningen udgør en begrænset risiko. Det er kun de tegningsberettigede medlemmer, der kan handle og underskrive på foreningens vegne og dermed forpligte foreningen. De tegningsberettigede medlemmer vil typisk være formanden og kassereren eller formanden/kassereren og et andet bestyrelsesmedlem. Dette afhænger dog af den konkrete forenings tegningsregler. I andre tilfælde, hvor foreningen ikke udgør en begrænset risiko, vil det være nødvendigt at kontrollere alle identifikationsoplysningerne for alle medlemmer af bestyrelsen eller direktionen.

Investeringsforeninger
Når kunden er en investeringsforening eller en afdeling i en investeringsforening, skal virksomheden identificere og gennemføre rimelige foranstaltninger for at kontrollere de fysiske personer, der i sidste ende ejer og kontrollerer den juridiske enhed, som virksomheden indgår forretningsforbindelsen med. I dette eksempel vil det være investeringsforeningen som juridisk person med et CVR-nr., også selvom der f.eks. kun skal leveres en ydelse til en enkelt afdeling i investeringsforeningen.

Er der ingen personer, der ejer eller kontrollerer investeringsforeningen i en sådan grad, at de kan defineres som reelle ejere, skal foreningens daglige ledelse betragtes som reel ejer. Der kan henvises til Erhvervsstyrelsen Vejledning om reelle ejere, bilag 2.

Alternative investeringsfonde (AIF'er)
En AIF kan f.eks. være en private equity-fond, ejendomsfond eller andet. Når kunden er en AIF, skal virksomheden identificere og gennemføre rimelige foranstaltninger for at kontrollere de fysiske personer, der i sidste ende ejer og kontrollerer den juridiske enhed, som virksomheden indgår forretningsforbindelsen med. I dette eksempel vil det være AIF'en som juridisk person med et CVR-nr.

Er der ingen personer, der ejer eller kontrollerer AIF'en i en sådan grad, at de kan defineres som reelle ejere, skal AIF'ens daglige ledelse betragtes som reel ejer.

Filialer
Hvis kunden er en filial, skal virksomheden klarlægge ejer- og kontrolstrukturen og finde frem til, hvilke fysiske personer der ejer eller kontroller filialens hoved-/moderselskab.

Folkekirkens selvejende institutioner
Folkekirkens kirker og præsteembeder er som regel selvejende og bestyres af menighedsrådet. Det er derfor menighedsrådets medlemmer, der skal betragtes som reelle ejere.

Fonde
Hvis en kunde er en fond, skal virksomheden vurdere, hvem der i sidste ende direkte eller indirekte kontrollerer fonden.

Fonde, herunder erhvervsdrivende og ikke-erhvervsdrivende fonde, er kendetegnet ved, at de ikke har ejere. Som reel ejer af en fond anses den eller de fysiske personer, der i sidste ende direkte eller indirekte kontrollerer fonden eller på anden måde har ejerskabslignende beføjelser, herunder bestyrelsen og i nogle tilfælde også særligt begunstigede personer. Sidstnævnte skal dog som udgangspunkt kun anses som reelle ejere, hvis de med navns nævnelse efter fondens vedtægt har et retskrav på at modtage en ikke ubetydelig andel af fondens midler.

I dansk ret kan en stifter af en fond ikke have ejerbeføjelser over fondens midler, og stifteren er derfor som udgangspunkt ikke reel ejer. Der er dog tale om en konkret vurdering, og det kan ikke udelukkes, at der kan være situationer, hvor stifteren som følge af særlige beføjelser i fondens vedtægt, kan vurderes at være reel ejer. Stifteren kan derudover være reel ejer, hvis vedkommende er medlem af bestyrelsen i fonden.

Trusts og lignende juridiske arrangementer
Hvis en kunde f.eks. ejes af en udenlandsk trust, skal virksomheden identificere og gennemføre rimelige foranstaltninger for at kontrollere kundens reelle ejere. Virksomheden skal derfor vurdere trusten for at klarlægge, hvem der kan betragtes som den eller de reelle ejer(e). Den eller de reelle ejere af trusts og lignende juridiske arrangementer kan være følgende:

i. stifteren eller stifterne,
ii. forvalteren eller forvalterne (trustee(s)),
iii. protektoren eller protektorerne, særligt begunstigede eller, såfremt de enkeltpersoner, der nyder godt af det juridiske arrangement eller den juridiske enhed, endnu ikke kendes, den gruppe personer, i hvis hovedinteresse det juridiske arrangement eller den juridiske enhed er oprettet eller fungerer, og
iv. enhver fysisk person, der i sidste ende udøver kontrol over trusten gennem direkte eller indirekte ejerskab eller ved hjælp af andre midler.

Virksomheden skal opbevare oplysninger om de iværksatte foranstaltninger.

Dødsboer, konkursboer og virksomheder i likvidation
Ved dødsboer, konkursboer og for virksomheder i likvidation er bobestyreren, kurator eller likvidator – typisk en advokat – indsat til at opgøre og fordele midler.

For virksomheder, f.eks. pengeinstitutter, som har dødsboet, konkursboet eller virksomheden i likvidation som kunde, vil bobestyreren, kurator eller likvidatoren betragtes som værende kundens reelle ejer. Dette henset til, at bobestyrer, kurator eller likvidator betragtes som at være boets daglige ledelse.

I offentligt skiftede dødsboer er det således advokaten, der anses for at være den reelle ejer af dødsboet. I privatskiftede dødsboer har arvingerne fået boet udleveret og har fuld dispositionsret herover. I de tilfælde, hvor de privatskiftende arvinger henvender sig til en advokat/bobestyrer med anmodning om bistand til skifte, vil der foreligge et fuldmagtsforhold mellem boet og advokaten/bobestyreren, hvorefter advokaten/bobestyreren skal identificeres som reel ejer. Beholder arvingerne fuld dispositionsret over boet, vil det være arvingerne, der anses for at være reelle ejere af dødsboet. Det er tilstrækkeligt at

identificere og kontrollere den arving, som måtte have fået fuldmagt fra de øvrige til at disponere over boet, som reel ejer.

Det bemærkes, at ved dødsboer, konkursboer og virksomheder i likvidation vil det i Erhvervsstyrelsens register over reelle ejere fortsat være boets eller virksomhedens hidtidige reelle ejere, som står registreret som værende kundens reelle ejere.

For så vidt angår advokaters identifikation af reelle ejere i dødsboer, konkursboer og virksomheder i likvidation henvises nærmere til Advokatrådets vejledning om hvidvask.

Reelle ejere i andre typer juridiske personer mv.
Kunder der handles på et reguleret marked
Er kunden en børsnoteret virksomhed, dvs. ejerandelene handles på et reguleret marked, har kunden ingen reelle ejere og den daglige ledelse af kunden vil således ikke skulle betragtes som reelle ejere.

Kunder, der er ejet af et selskab med ejerandele, der handles på et reguleret marked
Er kunden ejet af en (børsnoteret) virksomhed, hvis ejerandele handles på et reguleret marked, vil det være kundens daglige ledelse, der skal betragtes som reelle ejere, da der ikke er reelle ejere af den (børsnoterede) virksomhed.

Ved identifikation af, hvem der er reel ejer i andre typer juridiske personer mv., kan henvises til Erhvervsstyrelsens Vejledning om reelle ejere, som bl.a. omhandler identifikation af reelle ejere i selskaber, fonde, visse foreninger og i virksomheder, som er omfattet af finansiel lovgivning mv. I forbindelse med udførelse af kundekendskabsprocedurer er Erhvervsstyrelsens Vejledning, bilag 2, et fortolkningsbidrag til at afgøre, hvem der skal betragtes som reelle ejere i de situationer, hvor der ikke kan identificeres fysiske personer, der ejer eller kontrollerer virksomheden i en sådan grad, at de bliver reelle ejere i hvidvasklovens forstand.

9.6.5. Indberetning om reelle ejere

Virksomheder, der er omfatter af hvidvaskloven, er forpligtet til at indberette uoverensstemmelser i forhold til de registrerede oplysninger om reelle ejere.

Dette afsnit omhandler disse virksomheders indberetningspligt til Erhvervsstyrelsens it-system. For så vidt angår hvidvasklovens krav til virksomheders indhentelse af identitetsoplysninger og kontrol heraf i forhold til en kundes reelle ejere henvises til afsnit 9.6.2. vedrørende indhentelse af identitetsoplysninger samt afsnit 9.6.3. vedrørende kontrol af reelle ejeres identitetsoplysninger.

Som led i virksomhedens kundekendskabsprocedurer skal virksomheden indhente et registreringsbevis eller et ekstrakt af oplysningerne fra Erhvervsstyrelsens it-system. Hvis der er uoverensstemmelse i oplysningerne indhentet af virksomheden om kundens reelle ejere og i Erhvervsstyrelsens it-system, skal uoverensstemmelsen indberettes til Erhvervsstyrelsen. Hvis kunden får korrigeret uoverensstemmelsen hurtigst muligt, skal virksomheden ikke indberette uoverensstemmelsen til Erhvervsstyrelsen.

Indberetningspligten omfatter uoverensstemmelser i forhold til de oplysninger, som fremgår af Erhvervsstyrelsens it-system, dvs. oplysninger om den reelle ejer og den reelle ejers rettigheder, og de oplysninger, som er tilgængelig for virksomheder omfattet af hvidvasklovens kundekendskabskrav, når de undersøger, hvem der er deres kundes reelle ejere.

Ved dødsboer, konkursboer samt virksomheder i likvidation, hvor bobestyreren, kurator eller likvidatoren betragtes som værende kundens reelle ejer, skal kundens hidtidige reelle ejere fortsat stå registreret i Erhvervsstyrelsens register over reelle ejere, og her skal der kun ske indberetning, jf. hvidvasklovens § 15 a, hvis der er uoverensstemmelser i oplysninger om kundens hidtidige reelle ejere. Der henvises i øvrigt til afsnit 9.6.4 om klarlæggelse af ejer- og kontrolstruktur vedrørende dødsboer, konkursboer og virksomheder i likvidation.

For yderligere vejledning henvises til bekendtgørelse om indberetning af uoverensstemmelser i oplysninger om reelle ejere og Erhvervsstyrelsens vejledning vedrørende indberetning om reelle ejere, se https://erhvervsstyrelsen.dk/vejledning-indberetning-om-reelle-ejere.

9.7. Forretningsforbindelsens formål og tilsigtede beskaffenhed

Henvisning til hvidvaskloven: § 11, stk. 1, nr. 4. Henvisning til 4. hvidvaskdirektiv: Artikel 13, stk. 1, nr. c.

Virksomheden skal vurdere forretningsforbindelsens formål og tilsigtede beskaffenhed. Hvis det er relevant, skal virksomheden også indhente oplysninger om formålet og den tilsigtede beskaffenhed hos kunden.

Virksomheden skal foretage en konkret vurdering af, om det er relevant at indhente oplysninger. Vurderingen kan bl.a. bero på produkttypen.

Viden om forretningsforbindelsens formål og tilsigtede beskaffenhed hjælper virksomheden til at vurdere, om forretningsforbindelsen har et legitimt formål, og til at få en dybere indsigt i forretningsforbindelsens samlede risikoprofil.

Kravet om, at virksomheden skal vurdere forretningsforbindelsens formål, betyder, at virksomheden skal kende kundens formål med, hvorfor kunden ønsker den pågældende forretningsforbindelse, f.eks. at kunden skal bruge en indlånskonto til udbetaling af løn eller at kunden ønsker at investere i aktier og andre værdipapirer.

Formålet med forretningsforbindelsen er relevant for virksomhedens vurdering af det konkrete kundeforhold, herunder i vurderingen af, om der er risiko for hvidvask eller finansiering af terrorisme. Derudover er oplysningerne relevante for virksomhedens overvågning af kundeforholdet og til virksomhedens afgørelse af, om en specifik transaktion eller lignende er usædvanlig for kunden og for kundens formål med forretningsforbindelsen.

Virksomheden skal have indsigt i, hvorfor kunden ønsker produktet eller ydelsen. Hvis virksomheden vurderer, at det er relevant at indhente oplysninger om formålet, kan virksomheden f.eks. have brug for oplysninger om:

1) Hvorfor kunden ønsker et bestemt produkt eller tjenesteydelse.

2) Hvad der er den forventede størrelse, antal eller frekvens af transaktioner, som kunden ønsker gennemført.

Hvis virksomheden ud fra en risikobaseret vurdering ikke indhenter oplysninger om formålet, kan virksomheden benytte sin overvågning af kunden til at vurdere, om kundens formål med forretningsforbindelsen er i overensstemmelse med virksomhedens viden herom. Her kan virksomheden ud fra overvågningen vurdere, hvad der er typisk eller sædvanligt for det pågældende kundetypeforhold, og om den konkrete kunde afviger fra dette.

Kravet om, at virksomheden skal vurdere forretningsforbindelsens tilsigtede beskaffenhed, betyder, at virksomheden skal kende karakteren af forretningsforbindelsen, dvs. de egenskaber og forhold, der tilsammen giver forretningsforbindelsen sin karakter.

Virksomheden vil oftere have behov for at indhente oplysninger om den tilsigtede beskaffenhed end om formålet, fordi formålet kan være fastlagt i eller følge af produkttypen. Forretningsforbindelsens tilsigtede beskaffenhed siger noget konkret om kunden og kundens anvendelse af produktet. Dette kan f.eks. være at forstå oprindelsen af kundens midler eller forstå, hvordan en virksomhedskunde opnår sin indtjening.

Hvis virksomheden vurderer, at det er relevant at indhente oplysninger om den tilsigtede beskaffenhed, kan virksomheden f.eks. have brug for oplysninger om:

1) Kundens konkrete forretningsmodel, hvis kunden er en juridisk person.
2) Kundens indtægts- og formueforhold.
3) Hvordan kunden påtænker at anvende midlerne.

9.8. Løbende overvågning af forretningsforbindelsen

Henvisning til hvidvaskloven: § 11, stk. 1, nr. 5. Henvisning til 4. hvidvaskdirektiv: Artikel 13, stk. 1, litra d.

Virksomheden skal løbende overvåge den etablerede forretningsforbindelse. Kravet gælder både i forhold til overvågning af de transaktioner, som kunden foretager, og i forhold til andre af kundens aktiviteter, generelt betegnet kundens adfærd, som virksomheden f.eks. får kendskab til gennem den almindelige kontakt med kunden.

Formålet med overvågningen er blandt andet at afdække, om den enkelte kundes adfærd, herunder kundens transaktioner og aktiviteter, er i overensstemmelse med virksomhedens kendskab til kunden. Virksomheden skal overvåge kundens adfærd for at sikre, at denne stemmer overens med kundens forretnings- og risikoprofil, og samtidig om kundens transaktioner og aktiviteter er overensstemmende med andre kunder med samme forretnings- og risikoprofil.

Ved ”kundens forretningsprofil” forstås oplysninger om kundens profil på baggrund af oplysninger om f.eks. formål med forretningsforbindelsen, omfang af transaktioner samt transaktionernes størrelse, regelmæssighed og varighed. Ved ”kundens risikoprofil” forstås, at overvågningen af forretningsforbindel-

sen skal ske ud fra den profil af kunden, som virksomheden er kommet frem til på baggrund af sin risikovurdering af forretningsforbindelsen med kunden, se afsnit 13 om risikovurdering – kundekendskabsprocedurer.

Overvågningen bør tilrettelægges efter den enkelte kundes forhold og løbende justeres på baggrund af kundens historik og virksomhedens viden om kunden. Dog kan virksomheder med en simpel forretningsmodel vælge at overvåge alle eller en gruppe af deres kunder på samme måde, f.eks. en pengeoverførselsvirksomhed, der har samme kundetyper og kun overfører penge til ét geografisk område.

Virksomheden skal ved overvågningen sikre sig, at de transaktioner og aktiviteter, som kunden foretager, er i overensstemmelse med virksomhedens viden om kunden og dennes forretnings- og risikoprofil. Hvis en kundes forretnings- og risikoprofil ændrer sig, skal virksomheden justere overvågningen af kunden. Hvis der er tale om, at virksomheden har foretaget en undersøgelse af kunden på baggrund af mistænkelige forhold, kan det være relevant at udvide overvågningen, se afsnit 24.1 om udvidet overvågning.

Virksomheden skal ud fra en risikovurdering søge oplysning om oprindelsen af kundens midler, hvis en transaktion er usædvanlig ud fra virksomhedens viden om kundens indtjenings- og formueforhold, herunder likviditet. Virksomheden skal i sådanne tilfælde kende oprindelsen af de midler, som vedrører forretningsforbindelsen. Det vil typisk ikke være tilstrækkeligt for at afkræfte en mistanke blot at indhente yderligere oplysninger fra kunden om midlernes oprindelse. Virksomheden skal indhente dokumentation f.eks. i form af en salgsaftale, lønsedler, boopgørelse eller lignende.

Begrebet midlernes oprindelse dækker over, hvor følgende har oprindelse:

1) Kundens formue.
2) Midler, der indgår i transaktionen.
3) Midlerne, der er en del af forretningsforbindelsen.

Ønsker en kunde f.eks. at indsætte/har indsat et stort beløb, som virksomheden vurderer er usædvanligt for kunden, kan virksomheden eksempelvis indhente oplysninger og dokumentation for oprindelsen af de midler, som kunden ønsker at indsætte/har indsat.

I forhold til kunder med en øget risiko kan det være nødvendigt at kende midlernes oprindelse, inden virksomheden foretager en transaktion eller anden aktivitet for kunden. Det vil f.eks. være relevant i tilfælde, hvor virksomheden ud fra sin risikovurdering af forretningsforbindelsen har vurderet, at der er tale om et kundeforhold med øget risiko for hvidvask og finansiering af terrorisme. Se afsnit 14 om skærpede kundekendskabsprocedurer.

I forhold til forretningsforbindelser, der handler om rådgivnings- og formidlingsopgaver, skal virksomheden overvåge, om kundens forespørgsler er usædvanlige i forhold til virksomhedens oplysninger om kunden og dennes forretnings- og risikoprofil.

Da kravet om overvågning både gælder for transaktioner og aktiviteter, kan det være relevant både at have en manuel og en systembaseret overvågning. En manuel overvågning kan f.eks. være, at virksomheden har fastlagt, hvordan de ansatte rapporterer mistænkelig adfærd til den hvidvaskansvarlige. Den systembaserede overvågning kan f.eks. være et IT-system, der overvåger kundernes transaktioner og aktiviteter og ved usædvanlig eller mistænkelig adfærd udløser en alarm.

Der er ikke krav om, at virksomheder har et IT-system til overvågning, men i virksomheder med et stort antal kunder og komplekse produkter og transaktioner, kan det være nødvendigt for at sikre den fornødne overvågning. Det kan f.eks. være aktuelt i forbindelse med et pengeinstituts overvågning af sine kunder.

9.9. Løbende ajourføring af oplysninger om kunden

Henvisning til hvidvaskloven: § 11, stk. 1, nr. 5. Henvisning til 4. hvidvaskdirektiv: Artikel 13, stk. 1, litra d.

Oplysninger, dokumenter og data, der er indhentet om en kunde, skal løbende ajourføres med henblik på, at virksomheden kan vurdere, om forretningsforbindelsens risiko er ændret. Det betyder, at der kan være behov for, at oplysninger, som virksomheden indhenter som led i sine kundekendskabsprocedurer, bliver opdateret i løbet af kundeforholdet.

Virksomheden kan fastsætte procedurer for ajourføringen. Virksomheden kan f.eks. beslutte, at ajourføring af oplysninger om kunder, der er inddelt i forskellige risikoklassifikationer, kan ske med forskellige intervaller, afhængig af om risikoen er begrænset, mellem eller høj.

Se afsnittene 8.2 om ændring af en kundes relevante omstændigheder og 8.3 om kundekendskabsprocedurer på passende tidspunkter.

10. Når en person handler på vegne af en kunde

Henvisning til hvidvaskloven: § 11, stk. 2. Henvisning til 4. hvidvaskdirektiv: Artikel 13, stk. 1.

Når en person handler på vegne af en kunde, eller når der er tvivl om, hvorvidt en person handler på egne vegne, skal virksomheden:

1) identificere personen og
2) kontrollere personens identitet ved en pålidelig og uafhængig kilde.

Kravet opstår i de tilfælde, hvor en person selv oplyser, at vedkommende handler på vegne af en anden, eller hvor virksomheden er i tvivl om, hvorvidt personen handler på egne vegne.

Den fysiske eller juridiske person, som en anden person handler på vegne af, er kunden, og det er derfor denne person, som virksomheden skal gennemføre kundekendskabsprocedurer på.

Virksomheden er alene forpligtet til at identificere og kontrollere identiteten af den person, der handler på vegne af kunden. Det betyder, at virksomheden ikke skal gennemføre andre kundekendskabsprocedurer på denne person, herunder f.eks. formål og tilsigtede beskaffenhed.

Når fysiske eller juridiske personer handler på vegne af en kunde, skal virksomheden sikre, at den fysiske eller juridiske person har beføjelse til dette.

Anvendelsesområdet for bestemmelsen vedrører tredjeparter, og på denne baggrund er stillingsfuldmagter ikke omfattet af hvidvasklovens § 11, stk. 2, fordi indehaverne af en stillingsfuldmagt handler som en del af virksomheden og ikke som en uafhængig tredjepart på vegne af virksomheden. Det kan dog følge af anden lovgivning, at virksomheden bør sikre sig, at den pågældende person handler på baggrund af en stillingsfuldmagt og inden for rammerne af denne.

Hvis virksomheden er i tvivl, om en person handler på egne vegne, kan det i nogle tilfælde være tilstrækkeligt at spørge personen. Hvis virksomheden ikke herved kan afkræfte tvivlen, eller hvis der er tvivl om, hvorvidt personens oplysninger er korrekte, skal virksomheden kontrollere personens identitet.

Ved fuldmagtsforhold er det virksomheden, der skal vurdere, hvilken dokumentation der er nødvendig. Der er nogle produkter, hvor der naturligt foreligger et fuldmagtsforhold, f.eks. børneopsparinger. Dette produkt er af begrænset risiko, og barnet som kunde kan f.eks. identificeres og kontrolleres ved sin dåbsattest. Forældrene eller bedsteforældrene skal identificeres og kontrolleres som fuldmagtshavere, der handler på vegne af barnet.

Der er andre fuldmagtsforhold, hvor alene ét dokument kan være tilstrækkelig dokumentation. Dette kan f.eks. være en kommunalt ansat, som kan fremvise sit identitetskort, der er udstedt af kommunen, og som dokumenterer ansættelsesforholdet.

I situationer, hvor fuldmagtsforholdet ikke er klart, eller hvor der er tvivl om fuldmagtsforholdet, skal virksomheden have oplysninger eller dokumentation fra personen, som skal bevise, at personen har den nødvendige beføjelse til at handle på kundens vegne.

Kravet om, at virksomheden sikrer, at den fysiske eller juridiske person, der handler på vegne af kunden, har beføjelse til dette, gælder ikke, hvis den pågældende person er en advokat med beskikkelse i Danmark eller i et andet EU- eller EØS-land.

11. Begunstigede ved livs- og pensionsforsikringer

Henvisning til hvidvaskloven: § 12, stk.1 og 2. Henvisning til 4. hvidvaskdirektiv: Artikel 13, stk. 5.

Ved livs- og pensionsforsikringer skal der indhentes identitetsoplysninger på den, der er begunstiget i forhold til policen. Livs- og pensionsselskaber skal således som led i deres kundekendskabsprocedurer indhente navn på begunstigede.

Hvis der er tale om en unavngiven person eller en gruppe af unavngivne personer, skal virksomheden have tilstrækkelige oplysninger til at kunne identificere de begunstigede på udbetalingstidspunktet.

”Tilstrækkelige oplysninger” betyder, at livs- eller pensionsforsikringsselskabet vurderer, at selskabet kan identificere den begunstigede på det tidspunkt, hvor udbetalingen finder sted. Indsættelse af nærmeste

pårørende som begunstiget vil være tilstrækkeligt, da den begunstigede ved udbetalingstidspunktet vil kunne identificeres ud fra de gældende regler for nærmeste pårørende.

Så snart den begunstigede er identificeret eller udpeget, skal virksomheden indhente identitetsoplysninger om vedkommende. Indhentning af identitetsoplysninger på den begunstigede kan f.eks. ske ved, at kunden (forsikringstager) oplyser virksomheden om navnet på den pågældende.

Formålet med at indhente oplysninger om navn på den begunstigede er, at disse oplysninger skal inddrages i risikovurderingen af kundeforholdet, herunder om der skal iværksættes skærpede kundekendskabsprocedurer.

Hvis en begunstiget er en PEP, skal der gennemføres skærpede kundekendskabsprocedurer, se afsnit 15 om politisk eksponerede personer.

Kontrol af identitetsoplysninger for begunstigede
Begunstigedes identitetsoplysninger skal kontrolleres på samme måde som kunder efter § 11, stk. 2. For fysiske personer vil identitetsoplysningerne være navn og cpr.nr.

Kontrollen skal ske på grundlag af dokumenter, data eller oplysninger indhentet fra en pålidelig og uafhængig kilde, se afsnit 9.2 om kontrol af identitetsoplysninger.

Kontrollen af identitetsoplysninger skal ske før udbetaling til den begunstigede finder sted.

Det betyder, at kontrollen af identitetsoplysninger kan vente med at blive gennemført til et tidspunkt inden udbetalingen til den begunstigede, men oplysning om navn kan ikke vente til dette tidspunkt.

12. Korrespondentforbindelser

Henvisning til hvidvaskloven: § 2, nr. 4 og §§ 19, 20.

Henvisning til 4. hvidvaskdirektiv: Artikel 19 og 24.
Henvisning til 5. hvidvaskdirektiv: Artikel 1, stk. 1, nr. 12.
Henvisning til: European Banking Authority, Retningslinjer for risikofaktorer, JC 2017 37, 04.01.2018.

Indgåelse af en korrespondentforbindelse med en respondent er omfattet af hvidvaskloven. Dette gælder både for korrespondentforbindelser i EU- og EØS-lande såvel som korrespondentforbindelser udenfor EU/EØS.

Korrespondentforbindelser defineres i hvidvasklovens § 2, nr. 4, som:

a) Levering af pengeinstitutydelser fra et pengeinstitut (korrespondenten) til et andet pengeinstitut (respondenten), herunder oprettelse af løbende konto eller passivkonto, samt øvrige ydelser som likviditetsstyring (cash management), international overførsel af midler mv.
b) En forbindelse mellem en virksomhed omfattet af § 1, stk. 1, nr. 1-13 eller 19, (korrespondenten) til en anden virksomhed omfattet af § 1, stk. 1, nr. 1-13 eller 19, (respondenten), hvor der leveres lignende ydelser, herunder forbindelser indgået med henblik på værdipapirtransaktioner eller overførsler af midler.

En korrespondentforbindelse omfatter ikke kun forretningsforbindelser mellem banker, men også forretningsforbindelser mellem de virksomheder, der er oplistet i bestemmelsen i § 2, nr. 4, litra b, f.eks. udbydere af betalingstjenester, hvis der leveres en pengeinstitutydelse eller en lignende ydelse. I en korrespondentforbindelse er korrespondenten den, der leverer (sælger) de finansielle ydelser, mens respondenten er den, der modtager (køber) de finansielle ydelser.

Der vil i almindelighed være tale om en korrespondentforbindelse omfattet af hvidvaskloven, når to finansielle virksomheder udveksler finansielle ydelser af løbende karakter. Der vil derfor i almindelighed ikke være etableret en korrespondentforbindelse ved gennemførelse af en enkeltstående transaktion.

Ved vurderingen af, om der er tale om en enkeltstående transaktion eller etablering af en korrespondentforbindelse, kan virksomheden tage højde for risikoen i transaktionen, herunder i forhold til beløbsstørrelse og det finansielle produkt. Virksomheden bør have klare procedurer herfor, herunder for hvordan det sikres, at der er tale om en enkeltstående transaktion.

Udveksling af SWIFT-nøgler
Internationale elektroniske pengeoverførsler understøttes af et meddelelsessystem, der udbydes af SWIFT (Society for Worldwide Interbank Financial Telecommunication), via en RMA (Relationship Management Application) også kaldet en RMA-nøgle.

For at kunne kommunikere meddelelser om pengeoverførsler ved brug af SWIFT-systemet er det en forudsætning, at virksomhederne har oprettet og udvekslet en RMA-nøgle (autorisationsnøgle) med hinanden.

Det er i SWIFT-systemet muligt at styre, hvilke typer beskeder (MT-typer) der kan udveksles gennem RMA'en. Åbning af en RMA og/eller udveksling af SWIFT-beskeder mellem to virksomheder, medfører ikke i sig selv, at der etableres en korrespondentforbindelse. At sende meddelelser via SWIFT-systemet er alene en kommunikationskanal, der gør det muligt for to virksomheder at sende meddelelser via et sikret system. Virksomheden skal dog i sådanne situationer vurdere, hvornår der er tale om etablering af en forretningsforbindelse, der kræver gennemførelse af kundekendskabsprocedurer.

12.1. Kundekendskabsprocedurer
Hvis der er tale om en korrespondentforbindelse indenfor EU/EØS er hovedreglen, at virksomheden kan gennemføre almindelige kundekendskabsprocedurer, herunder foretage en konkret risikovurdering af den konkrete forretningsforbindelse med respondenten mv. Den konkrete risikovurdering kan medføre, at virksomheden kommer frem til, at virksomheden skal gennemføre skærpede kundekendskabsprocedurer på respondenten, se afsnit 12.2.1. om korrespondentforbindelser indenfor EU/EØS.

Er der tale om en korrespondentforbindelse med en respondent udenfor EU/EØS, som ikke involverer gennemførelse af betalinger, er udgangspunktet, at virksomheden kan gennemføre almindelige kundekendskabsprocedurer, herunder foretage en konkret risikovurdering af den konkrete forretningsforbindelse med respondenten mv.

Så snart virksomheden etablerer en korrespondentforbindelse, der involverer gennemførelse af betalinger med et respondentinstitut beliggende i et land udenfor EU/EØS, som der ikke er indgået aftale med

på det finansielle område, skal virksomheden gennemføre skærpede kundekendskabsprocedurer på respondenten, se afsnit 12.2.2. om korrespondentforbindelser udenfor EU/EØS.

Forpligtelsen til at gennemføre kundekendskabsprocedurer påhviler korrespondenten, idet korrespondenten er den virksomhed, der leverer (sælger) finansielle ydelser til den anden virksomhed, mens respondenten er den virksomhed, der modtager (køber) finansielle ydelser direkte fra korrespondenten. Det er derfor alene korrespondenten, som skal udføre kundekendskabsprocedurer på respondenten. I tilfælde af, at de finansielle ydelser er gensidige (går begge veje) vil begge virksomheder skulle gennemføre kundekendskabsprocedurer, se herom under pkt. 12.2.

Kundekendskabsproceduren skal være gennemført inden en virksomhed, omfattet af hvidvasklovens § 1, stk. 1, nr. 1-13 og 19, etablerer en korrespondentforbindelse.

12.2. Korrespondentens forpligtelser

Hvis virksomhederne gensidigt udveksler (køber og sælger) finansielle ydelser med hinanden, skal hver virksomhed (korrespondenten) udføre kundekendskabsprocedure på sin kunde (respondenten). Det betyder, at begge virksomhed skal udføre kundekendskabsprocedure på modparten ved gensidig udveksling af ydelser.

Hvis det vurderes, at forholdet mellem to virksomheder er en korrespondentforbindelse omfattet af hvidvaskloven, er korrespondenten forpligtet til at udføre kundekendskabsprocedurer på respondenten, inden forbindelsen etableres.

12.2.1. Korrespondentforbindelse indenfor EU/EØS

I de tilfælde, hvor der er tale om en korrespondentforbindelse med en respondent beliggende i et land indenfor EU/EØS, skal virksomheden/korrespondenten gennemføre kundekendskabsprocedurer, herunder foretage en konkret risikovurdering af den konkrete forretningsforbindelse med respondenten. Den konkrete risikovurdering kan medføre, at virksomheden/korrespondenten kommer frem til, at virksomheden/korrespondenten skal gennemføre skærpede kundekendskabsprocedurer på respondenten.

Korrespondenten vil i en sådan situation skulle gennemføre almindelige kundekendskabsprocedurer efter hvidvasklovens § 11 og eventuelt supplere med skærpede kundekendskabsprocedurer efter § 17 på baggrund af risikovurderingen af respondenten.

Der er visse faktorer, der kan indikere en øget risiko, som korrespondenten skal være opmærksom på, bl.a. følgende:

1) Hvis kontoen kan benyttes af andre enheder i respondentbankens koncern, dvs. andre enheder, der ikke selv har været underlagt korrespondentbankens kundekendskabsprocedurer.
2) Hvis kontoen kan bruges af andre banker eller kunder, der har et direkte forhold til respondenten, men som ikke har et direkte forhold til korrespondenten. I sådanne tilfælde vil det betyde, at korrespondenten leverer tjenesteydelser til andre banker end den respondent, der er indgået en korrespondentforbindelse med.

Omvendt er der faktorer, der kan bidrage til at begrænse risikoen, bl.a.:

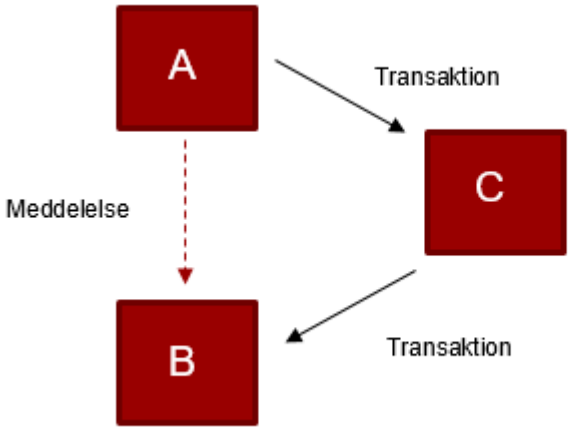
1) Når virksomheder handler på egne vegne og derfor ikke håndterer transaktioner på vegne af deres kunder, f.eks. i forbindelse med valutatransaktioner mellem to banker, hvor bankerne er

ejerne, og afviklingen af transaktionerne ikke involverer en tredjemand. Dvs. transaktionen sker for respondentbankens egen regning.
2) Når transaktionen vedrører salg, køb eller pantsætning af værdipapirer på regulerede markeder, f.eks. når respondentbanken optræder som eller bruger en depotbank med direkte adgang, normalt gennem en lokal deltager til et værdipapirafviklingssystem i EU eller i et tredjeland.

Virksomheder, der indgår korrespondentforbindelser, kan bl.a. søge vejledning om konkrete risikovurderinger og risikofaktorer i EBA's retningslinjer for risikofaktorer.

Virksomheden skal kunne godtgøre over for den tilsynsmyndighed, der fører tilsyn med virksomhedens overholdelse af hvidvaskloven, at virksomheden har et tilstrækkeligt kendskab til respondenten i forhold til at begrænse risikoen for hvidvask og finansiering af terrorisme.

Nedenstående figur illustrerer et eksempel, hvor en kunde hos et pengeinstitut (A) ønsker at sende penge til en kunde hos et andet pengeinstitut (B). A har imidlertid ikke et kontoforhold hos B. A kan derfor ikke sende penge på vegne af sin kunde direkte til en konto hos B. I nedenstående tilfælde er alle tre pengeinstitutter etableret indenfor EU/EØS.



Pengeinstitut A bruger sin korrespondentforbindelse pengeinstitut C (kaldet "intermediary bank"), som har en korrespondentforbindelse med pengeinstitut B. A kan dermed nøjes med at sende en (SWIFT) meddelelse til B om, at der er et beløb på vej til kunden hos B, illustreret ved den stiplede linjen i figuren.

I dette eksempel er C korrespondenten og A respondenten i transaktionen mellem A og C, ligesom B er korrespondent i transaktionen mellem C og B. C skal dermed gennemføre kundekendskabsprocedurer på A, mens B skal gennemføre kundekendskabsprocedurer på C. Der er ingen korrespondentforbindelse eller kundeforhold mellem A og B, hvorfor A ikke i dette scenarie skal gennemføre kundekendskabsprocedurer på B.

12.2.2. Korrespondentforbindelse udenfor EU/EØS

I de tilfælde, hvor en virksomhed/korrespondent etablerer en korrespondentforbindelse med en respondent beliggende i et land udenfor EU/EØS, som Unionen ikke har indgået aftale med på det finansielle

område, der involverer gennemførelse af betalinger, skal korrespondenten, i tillæg til de almindelige kundekendskabsprocedurer, altid gennemføre skærpede kundekendskabsprocedurer på respondenten i henhold til de krav, der følger af hvidvasklovens § 19.

Korrespondenten skal derfor udføre almindelige kundekendskabsprocedurer efter hvidvasklovens § 11 samt skærpede kundekendskabsprocedurer efter § 19.

Der henvises til sidst i afsnittet vedrørende en nærmere gennemgang af hvidvasklovens § 19.

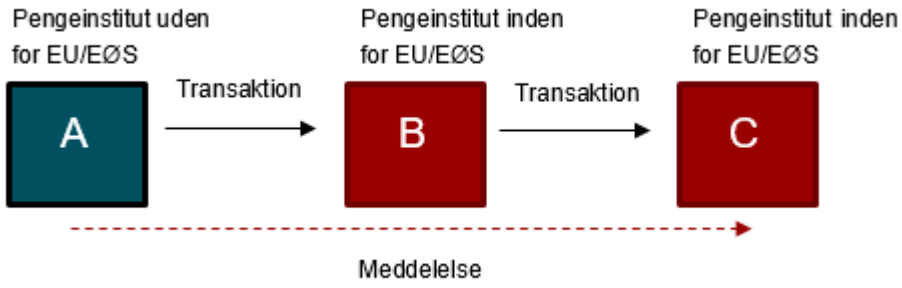
En korrespondentforbindelse falder inden for hvidvasklovens § 19, når der er tale om 1) en grænseoverskridende forbindelse med et respondentinstitut udenfor EU/EØS, som EU ikke har indgået aftale med på det finansielle område, og 2) en forbindelse, der involverer gennemførelse af betalinger. Gennemførelse af betalinger indebærer overførsel af midler for respondentens kunder til korrespondenten.

Betalinger skal forstås som kommercielle betalinger for detailkunder, erhvervskunder og/eller finansielle institutioner. Værdipapirhandel og udveksling af sikkerheder er således ikke omfattet af bestemmelsens anvendelsesområde.

En række finansielle ydelser vil således falde uden for anvendelsesområdet af hvidvasklovens § 19. Det kan eksempelvis være værdipapirhandel og/eller bekræftelse eller advisering af remburs eller garantier.

Hvis korrespondentforbindelsen mellem korrespondenten og respondenten udenfor EU/EØS ikke angår gennemførelse af betalinger, finder kravene i hvidvasklovens § 19 ikke anvendelse. Korrespondenten skal dog fortsat opfylde kravene i hvidvasklovens § 11 og eventuelt § 17 overfor respondenten.

Nedenstående figur illustrerer den situation, hvor en kunde hos et pengeinstitut (A) udenfor EU/EØS ønsker at sende penge til en kunde i et pengeinstitut (C) indenfor EU/EØS.



Pengeinstitut A har ikke en konto hos pengeinstitut C, hvorfor pengeinstitut A anvender pengeinstitut B som mellemled (kaldet ”intermediary bank”) til at sende betalingen. Pengeinstitut B er beliggende inden for EU/EØS. A har en konto hos B, og B har en konto hos C.

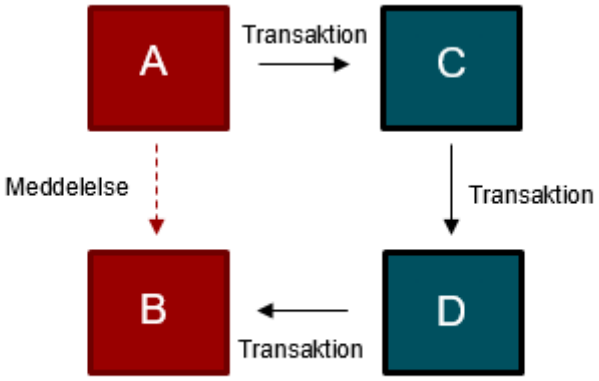
I dette scenarie skal:

C foretage kundekendskabsprocedurer efter § 11 og eventuelt § 17, ud fra en risikovurdering, på B.

B i forhold til A foretage kundekendskabsprocedurer efter § 11, ud fra en risikovurdering, og kundekendskabsprocedurer efter § 19, idet A er beliggende udenfor EU/EØS.

Forpligtelserne til at foretage kundekendskabsprocedurer gælder alene inter-partes. Der skal alene foretages kendskabsprocedure på den direkte modpart, hvorfor pengeinstitut C i dette scenarie ikke skal foretage kundekendskabsprocedurer på pengeinstitut A, idet A ikke er respondent hos C. A sender alene en meddelelse til C, der er illustreret ved den stiplede linje.

Nedenstående figur illustrerer betalinger gennem flere mellemled (kaldet "intermediary banks").



Pengeinstitut A og B er beliggende indenfor EU/EØS, mens pengeinstitut C og D er beliggende udenfor EU/EØS.

Midlerne sendes fra pengeinstitut A via først pengeinstitut C til pengeinstitut D og dernæst til pengeinstitut B. Pengeinstitut A sender en SWIFT-meddelelse til pengeinstitut B, der er illustreret ved den stiplede linje.

Der er ingen korrespondentforbindelse eller kundeforhold mellem pengeinstitut A og pengeinstitut B, hvorfor pengeinstitut A ikke i dette scenarie skal foretage kundekendskabsprocedurer eller risikovurdering på pengeinstitut B. Pengeinstitut B skal gennemføre skærpede kundekendskabsprocedurer på pengeinstitut D i henhold til de krav, der følger af hvidvasklovens § 19. Det skyldes, at der er tale om en grænseoverskridende korrespondentforbindelse med et respondentinstitut beliggende i et land udenfor EU/EØS, som EU ikke har indgået aftale med på det finansielle område, og en forbindelse, der involverer gennemførelse af betalinger.

Korrespondentens forpligtelser efter hvidvasklovens § 19 (tillæg til de almindelige forpligtelser efter § 11)
Etableres der en korrespondentforbindelse, der involverer gennemførelse af betalinger, med en respondent fra et land, som ikke er et EU- eller EØS-land, skal korrespondenten:

1) indhente tilstrækkelige oplysninger om respondenten, så korrespondenten forstår, hvori respondentens virksomhed består,
2) bedømme respondentens omdømme ud fra offentligt tilgængelige oplysninger,
3) bedømme kvaliteten af det tilsyn, som føres med respondenten i det pågældende land, hvor respondenten er etableret, f.eks. på baggrund af evalueringsrapporter fra FATF, IMF mv. eller ved at kontakte respondentens tilsynsmyndighed om dennes tilsynsvirksomhed,
4) indhente tilstrækkelige oplysninger til at sikre, at respondenten har effektive kontrolprocedurer med henblik på at overholde regler om bekæmpelse af hvidvask og finansiering af terrorisme,

5) indhente godkendelse hos den hvidvaskansvarlige,
6) dokumentere sit, henholdsvis respondentens ansvar for at opfylde reglerne i hvidvaskloven.

Ad 1-3: Tilstrækkelige oplysninger om respondentens virksomhed, omdømme og underlagte tilsyn:
Det følger af nr. 1-3, at korrespondenten skal indhente tilstrækkelige oplysninger om respondenten til at forstå, hvori dennes virksomhed består, ligesom korrespondenten ud fra offentligt tilgængelige oplysninger skal bedømme respondentens omdømme og kvaliteten af det tilsyn, der føres med respondenten i det pågældende land.

Kravet indebærer efter Finanstilsynets opfattelse, at korrespondenten bl.a. skal indhente oplysninger om respondentens forretningsmodel, kundebase samt vurdere, og hvor relevant indhente oplysninger om virksomhedens formål og tilsigtede beskaffenhed. Til brug for opfyldelse af kravet kan anvendes tilgængelige oplysninger om respondentforbindelsen, f.eks. via internettet, fra private udbydere af information om finansielle institutter verden over og oplysninger udleveret af respondenten.

Ad 4: Tilstrækkelige oplysninger til at sikre, at respondenten har effektive kontrolprocedurer med henblik på at overholde regler om bekæmpelse af hvidvask og finansiering af terrorisme:
Når virksomheden skal indhente tilstrækkelige oplysninger, skal virksomheden foretage en vurdering på baggrund af de krav, der gælder i henhold til internationale standarder, som svarer til de krav, som gælder i den danske hvidvasklov.

Korrespondenten skal altid foretage en vurdering af respondenten og i denne forbindelse vurdere omfanget af undersøgelsen af respondenten.
Som en del af undersøgelsen af respondenten kan korrespondenten eksempelvis:
1) benytte internationale AML-spørgeskemaer, f.eks. Wolfsberg Group's Standard Anti-Money Laundering Questionnaire til den potentielle respondentforbindelse med henblik på besvarelse,
2) indhente oplysninger om respondentens politik på hvidvaskområdet,
3) undersøge, om respondenten har været dømt, involveret eller mistænkt for hvidvask eller terrorfinansiering, og
4) indhente oplysninger om respondentens forretningsgange for kontrol, compliancefunktion eller lignende.

Det er af afgørende betydning, at korrespondenten, ud fra en risikovurdering, ikke alene forlader sig på information levereret af respondenten selv, f.eks. via Wolfsberg Group's Standard Anti-Money Laundering Questionnaire.

Ad 5: Godkendelse hos den hvidvaskansvarlige:
Den hvidvaskansvarlige skal i sin godkendelse af en korrespondentforbindelse foretage en reel vurdering af respondentforbindelsen på baggrund af de oplysninger, som korrespondenten har indhentet om respondenten. Der gælder ingen formkrav til godkendelsen, men virksomheden skal kunne dokumentere den.

Ad 6: Dokumentere sit, henholdsvis respondentens ansvar for opfyldelse af reglerne i hvidvaskloven:
Korrespondenten skal sikre dokumentation for, at der er klare aftaler mellem korrespondenten og respondenten om ansvaret for opfyldelse af kravene i hvidvaskloven i tilfælde, hvor midler tilhørende respondentens kunder indsættes på en konto, der er oprettet af korrespondenten i Danmark. Det betyder, at korrespondenten og respondenten skal have indgået en skriftlige aftale om, hvem der har ansvaret for

de enkelte forpligtelser, og at denne aftale om ansvaret er vedtaget af både korrespondenten og respondenten.

12.3. Gennemstrømningskonti

Hvis respondentforbindelsens kunde har direkte adgang til at disponere over midler indestående på en konto hos korrespondentforbindelsen, skal korrespondenten sikre sig, at respondenten gennemfører kundekendskabsprocedurer, samt at respondenten kan udlevere kundekendskabsoplysninger efter anmodning fra korrespondenten.

Hvis respondentforbindelsens kunde har direkte adgang til at råde over midler, der indestår på en konto hos korrespondenten, såkaldte gennemstrømningskonti, skal korrespondenten sikre sig, at respondenten i det land, som respondenten er etableret i, er underlagt krav om at gennemføre kundekendskabsprocedurer.

Korrespondenten kan f.eks. sikre dette ved at indhente stikprøver på respondentens oprettede kundeforhold. Det er ikke tilstrækkeligt, at respondenten i lovgivningen er underlagt krav om kundekendskabsprocedurer. Korrespondenten skal undersøge og dermed sikre, at respondenten faktuelt gennemfører dem.

Derudover skal korrespondenten sikre sig, at respondenten efter anmodning kan udlevere kundekendskabsoplysninger til korrespondenten. Dette kan f.eks. ske i overensstemmelse med vilkår, der er fastsat i en kontrakt.

Disse krav betyder, at korrespondenter i Danmark er ansvarlige for respondentforbindelsers kundeforbindelser på samme måde, som hvis disse kunder havde haft direkte kundeforbindelse med korrespondenten i Danmark.

12.4. Virksomheden må ikke have en korrespondentforbindelse med et tomt selskab

Et tomt selskab er i hvidvasklovens forstand et selskab, der driver samme type virksomhed som de i § 1, stk. 1, nr. 1-13 og 19, nævnte virksomheder og personer, men som ikke er til stede i det land, hvor selskabet har hjemsted, ikke ledes eller administreres i det pågældende land og ikke indgår i en reguleret finansiel koncern.

Virksomheden må ikke have direkte eller indirekte relationer med et tomt selskab, og derfor må virksomheden ikke etablere eller opretholde en sådan forbindelse. Derudover skal virksomheden træffe rimelige foranstaltninger for at undgå at etablere korrespondentforbindelser med virksomheder, hvor der foreligger offentligt tilgængelige oplysninger om, at respondentforbindelsen lader tomme bankselskaber anvende respondentforbindelsens konti.

Med rimelige foranstaltninger forstås, at virksomheden foretager en vurdering af potentielle respondentforbindelser, inden virksomheden indgår i en forretningsforbindelse med dem. I vurderingen kan bl.a. indgå en afklaring af, om den potentielle respondentforbindelse tidligere har tilladt, at den pågældende respondentforbindelse lader tomme selskaber anvende sine konti.

Virksomheden må derfor f.eks. ikke oprette en korrespondentforbindelse, før virksomheden har foretaget søgninger i offentligt tilgængelige kilder om respondentforbindelsen.

13.Risikovurdering – kundekendskabsprocedurer

Henvisning til hvidvaskloven: § 11, stk. 3. Henvisning til 4. hvidvaskdirektiv: Artikel 13, stk. 2.

Virksomheden skal gennemføre kundekendskabsprocedurer i alle forretningsforbindelser. Kravene i § 11, stk. 1 og 2, kan derfor aldrig undlades, heller ikke i tilfælde af begrænset risiko.

Det betyder, at der for enhver kunde skal indhentes identitetsoplysninger. Identitetsoplysningerne skal kontrolleres, kundens forretnings- og risikoprofil skal klarlægges, og kundeforholdet skal overvåges. Ved kunder, der er juridiske personer, skal der altid også indhentes identitetsoplysninger på reelle ejere. Se afsnit 9.6 om reelle ejere.

Virksomhedens kundekendskabsprocedurer kan gennemføres ud fra en risikovurdering af det konkrete kundeforhold.

Kundekendskabsproceduren og risikovurderingen fastlægger kundens risikoprofil på tidspunktet for indgåelsen af forretningsforbindelsen. Risikoprofilen kan ændres i løbet af kundeforholdet, og derfor er der krav om, at virksomheden gennemfører kundekendskabsprocedurer løbende med et vist interval i hele kundeforholdet, således at oplysningerne om kunden holdes ajour, se afsnit 8.3 om kundekendskabsprocedurer på passende tidspunkter.

I forbindelse med indgåelsen af forretningsforbindelsen eller ved senere kundekendskabsprocedurer kan der være behov for, at virksomheden også undersøger oprindelsen af kundens midler for at vurdere eventuelle risici forbundet med hvidvask eller finansiering af terrorisme.

Risikovurderingen omfatter overordnet en vurdering af:

1) Risikoen for hvidvask og/eller finansiering af terrorisme.
2) Om kunden er den person, som kunden udgiver sig for at være.

Virksomheden bør tilrettelægge niveauet af sine kundekendskabsprocedurer ud fra den overordnede risikovurdering, som virksomheden har foretaget af sin forretningsmodel. Se afsnit 3 om risikovurdering. Virksomheden kan også konkret vurdere den enkelte forretningsforbindelse til en kunde ud fra de samme risikofaktorer.

Risikovurderingen kan forholde sig til:

1) Hvem kunden er?
2) Hvilke produkter eller ydelser ønsker kunden?
3) Er der med forretningsforbindelsen til kunden relevante geografiske forhold, der skal tages i betragtning?
4) Hvilke leveringskanaler er der til kunden?

De oplistede faktorer er ikke udtømmende, og der er ikke krav om, at virksomheden tager dem alle i betragtning. Virksomheden skal således selv fastlægge de relevante risikofaktorer.

I risikovurderingen skal indgå forretningsforbindelsens:

1) formål
2) omfang
3) regelmæssighed
4) varighed.

Disse fire faktorer indikerer ikke i sig selv en begrænset eller høj risiko. F.eks. kan en kundes formål med forretningsforbindelsen konkret indikere en høj risiko. På den anden side kan en forretningsforbindelse til en kunde f.eks. indikere en begrænset risiko, hvis den er regelmæssig og varig. Dette beror på en konkret vurdering, og virksomheden må forholde sig til hver faktor, og hvad de tilsammen indikerer for kundens risikoprofil.

Risikovurderingen skal inddrage de faktorer, som følger af hvidvasklovens bilag 2 og 3. Bilagene opremser faktorer, der kan være tegn på henholdsvis begrænset og øget risiko.

I virksomhedens vurdering af ovenstående fire oplistede forhold kan virksomheden f.eks. vurdere omfanget af de aktiver, som kunden ønsker at indsætte, størrelsen af de transaktioner, som kunden ønsker at gennemføre eller kundens forventede varighed af forretningsforbindelsen med virksomheden.

Virksomheden kan fastlægge en model for sine indledende kundekendskabsprocedurer og risikovurderinger, f.eks. at kunderne placeres i kategorier med begrænset, mellem eller høj risiko. Dette er relevant for, at virksomheden kan vurdere, om der i forhold til den enkelte kunde skal gennemføres lempede eller skærpede kundekendskabsprocedurer, og med hvilken frekvens den løbende ajourføring af kundekendskabsprocedurerne skal foretages.

14. Skærpede kundekendskabsprocedurer

Henvisning til hvidvaskloven: § 17.

Henvisning til 4. hvidvaskdirektiv: Artikel 18.
Henvisning til 5. hvidvaskdirektiv: Artikel 1, stk. 1, nr. 10 og 11.

Skærpede kundekendskabsprocedurer skal anvendes ud over de almindelige kundekendskabsprocedurer. Det betyder, at de supplerer de almindelige procedurer i situationer, hvor forretningsforbindelsen vurderes at have en øget eller høj risiko for hvidvask og/eller finansiering af terrorisme. I vurderingen skal virksomheden tage de højrisikofaktorer i betragtning som fremgår af bilag 3 til hvidvaskloven, samt andre højrisikofaktorer, som vurderes at være relevante.

Der kan ikke gives en udtømmende liste over, hvilke situationer der medfører skærpede kundekendskabsprocedurer og hvad disse ultimativt skal omfatte. Det er virksomheden, der på baggrund af sin risikovurdering skal vurdere, hvad der kan betrygge virksomheden i kendskabet til forretningsforbindelsen og begrænse den øgede risiko for hvidvask og/eller finansiering af terrorisme.

Dette er ikke ensbetydende med, at virksomheden ikke må indgå forretningsforbindelser med kunder, som virksomheden vurderer har en øget risiko for hvidvask og/eller terrorfinansiering, men virksomheden

er forpligtet til at gennemføre skærpede kundekendskabsprocedurer. Virksomheden skal selv tilrettelægge virksomhedens skærpede kundekendskabsprocedurer ud fra en risikovurdering, jf. hvidvasklovens § 17, stk. 1.

De foranstaltninger, der iværksættes ved øget eller høj risiko, kan bl.a. fastlægges ud fra en risikovurdering. Behovet kan være forskelligt ud fra hvilken risiko virksomheden har identificeret i sin risikovurdering af forretningsforbindelsen. Der er dog ikke krav om, at virksomheden skræddersyr de skærpede kundekendskabsprocedurer til hver forretningsforbindelse. Målet er, at virksomheden i henhold til sine politikker og forretningsgange varetager og forebygger de øgede risici, som forretningsforbindelsen konkret indebærer.

De skærpede kundekendskabsprocedurer kan f.eks. være, at virksomheden:

1) Indhenter oplysninger om kundens adresse eller fødested.
2) Indhenter oplysninger fra andre kilder end fra kunden selv.
3) Indhenter yderligere oplysninger om kunden, f.eks. om kundens formål og tilsigtede beskaffenhed med forretningsforbindelsen.
4) Indhenter oplysninger om kundens formue og midlers oprindelse.
5) Kontrollerer kundens oplysninger hos flere uafhængige og pålidelige kilder.
6) Gennemfører kundekendskabsprocedurer oftere i løbet af kundeforholdet.
7) Løbende gennemgår kundens transaktioner.
8) Indhenter oplysninger om kundens forretningsaktiviteter.
9) Indhenter yderligere oplysninger om kundens reelle ejer/ejere.
10) Undersøger kundens tidligere forretningsaktiviteter.
11) Undersøger kunden eller kundens reelle ejeres relationer ved f.eks. at foretage internetsøgninger.
12) Sender en kontrakt eller et andet dokument til kundens adresse med anmodning om, at kunden returnerer det i underskrevet stand (f.eks. relevant ved forretningsforbindelser, som ikke er indgået ved fysisk kontakt).
13) Indhenter den øverste ledelses godkendelse ved etablering eller fortsættelse af forretningsforbindelsen til kunden.

Virksomheden skal allerede fra indgåelsen af kundeforholdet med kunden vurdere, om der er tale om en høj risiko. Et eksempel på et kundeforhold med potentielt højere risiko kan være en ny kunde, som ikke har bopæl eller driver virksomhed i landet (typisk en valutaudlænding), men som alligevel ønsker at oprette en konto her i landet.

Gennemførelse af skærpede kundekendskabsprocedurer kan imidlertid også være nødvendige i løbet af kundeforholdet som led i virksomhedens overvågning af kunden. Dette kan f.eks. være:

1) Hvis kunden ændrer transaktionsmønster, f.eks. ved at foretage langt større transaktioner end sædvanligt eller til geografiske områder, som kunden ikke tidligere har været forbundet med.
2) Hvis kunden har et usædvanligt mønster, eller kundens brug af transaktioner, produkter og/eller tjenesteydelser er væsentlig mere komplekse end andre lignende kunders ”normale” adfærd.
3) Hvis der opstår tvivl om, hvorvidt kundens oplysninger er korrekte, eller hvis virksomheden får kendskab til et påviseligt formål, som ikke er overensstemmende med kundens oplysninger.

Hvis virksomheden i ovenstående eller andre tilfælde vurderer, at kunden har høj risiko, skal virksomheden iværksætte skærpede kundekendskabsprocedurer, uanset at kunden ikke tidligere har været i kategori for høj risiko.

Derudover skal der altid gennemføres skærpede kundekendskabsprocedurer:

1) hvis kunden er en politisk eksponeret person (PEP). Her kræves bl.a. en godkendelse af forretningsforbindelsen af virksomhedens hvidvaskansvarlige (§ 7, stk. 2-personen) ved indgåelse af forretningsforbindelsen med kunden, se afsnit 15 om politisk eksponerede personer og
2) ved etablering af en grænseoverskridende korrespondentforbindelse med respondenter fra lande uden for Den Europæiske Union, som Unionen ikke har indgået aftale med på det finansielle område.

I disse situationer skal virksomheden følge de procedurer, der følger af hvidvasklovens §§ 18 og 19. Se afsnit 15 om politisk eksponerede personer og afsnit 12 om korrespondentforbindelser.

Uanset virksomhedens risikovurdering af et kundeforhold, skal virksomheden efter § 17, stk. 2, gennemføre skærpede kundekendskabsprocedurer, hvis kunden har hjemsted i et land, der er opført på Europa-Kommissionens liste over højrisikotredjelande. Virksomheder skal derfor løbende sikre sig, at de har kendskab til Europa-Kommissionens liste, og om deres kunder har eller får hjemsted i et land, der er eller kommer på listen.

Hvis kunden har hjemsted i et land, der er opført på Europa-Kommissionens liste over højrisikotredjeland skal de skærpede kundekendskabsprocedurer omfatte følgende:

1. Indhentelse af yderligere oplysninger om kunden og reelle ejere.
2. Indhentelse af yderligere oplysninger om forretningsforbindelsens tilsigtede beskaffenhed.
3. Indhentelse af oplysninger om midlernes oprindelse og kilden til kundens og den reelle ejers formue.
4. Indhentelse af oplysninger om årsagerne til de ønskede eller udførte transaktioner.
5. Indhentelse af godkendelse ved etablering eller videreførelse af forretningsforbindelser hos den person, der er udpeget i henhold til § 7, stk. 2 (den hvidvaskansvarlige).
6. Skærpet overvågning af forretningsforbindelsen ved at øge antallet af kontroller og ved at udvælge transaktionsmønstre, der kræver nøjere undersøgelse.

Ad nr. 1: Indhentelse af yderligere oplysninger om kunden og reelle ejere.
Yderligere oplysninger om kunden og den reelle ejer kan eksempelvis være oplysninger om adresse eller fødested.

Ad nr. 2: *Indhentelse af yderligere oplysninger om forretningsforbindelsens tilsigtede beskaffenhed.*
Yderligere oplysninger om forretningsforbindelsens tilsigtede beskaffenged kan eksempelvis være oplysninger om forretningsforbindelsens transaktioner og forventede omfang. Oplysninger om forretningsforbindelsens forventede omfang kan være oplysninger om, hvor mange transaktioner kunden forventer at have, hvor omfangsrige kunden forventer, at disse transaktioner er, og mere generelt hvad kunden forventer at bruge forretningsforholdet til. Disse oplysninger er især relevante, når virksomheden i forbindelse med sin skærpede overvågning af forretningsforbindelsen skal fastlægge, om kunden forventede adfærd og transaktionsmønstre stemmer overens med den adfærd, kunden faktisk har.

Ad nr. 3: *Indhentelse af oplysninger om midlernes oprindelse og kilden til kundens og den reelle ejers formue.*

Indhentelse af oplysninger om midlernes oprindelse og kilden til kundens og den reelle ejers formue kan være oplysninger om, hvorfra kundens eller den reelle ejers formue stammer, hvorfra de midler, der indgår i transaktionen, stammer, eller hvor midlerne, der indgår i forretningsforbindelsen, kommer fra. I den forbindelse kan relevante oplysninger eksempelvis være oplysninger om, hvordan kunden eller den reelle ejer opnår sin indtjening. Har kunden eller den reelle ejer en formue, kan relevante oplysninger om midlernes oprindelse eksempelvis være om formuen stammer fra virksomhedssalg, forsikringssum eller fra arv.

Ad nr. 4: *Indhentelse af oplysninger om årsagerne til de ønskede eller udførte transaktioner.*
Indhentelse af oplysninger om årsagerne til de ønskede eller udførte transaktioner indebærer, at virksomheder, der er omfattet af loven, skal indhente oplysninger, der yderligere understøtter kundens formål med konkrete transaktioner. Eksempler herpå kan være transaktioner til familiemedlemmer, eller hvis kunden har samarbejdspartnere eller kunder, hvortil der ønskes eller udføres transaktioner.

Ad nr. 5: *Indhentelse af godkendelse ved etablering eller videreførelse af forretningsforbindelser hos den person, der er udpeget i henhold til § 7, stk. 2.*
Indhentelse af godkendelse ved etablering eller videreførelse af forretningsforbindelse hos den, der er udpegnet i henhold til § 7, stk. 2, (den hvidvaskansvarlige) indebærer, at virksomheder, der er forpligtet til at udpege en person efter § 7, stk. 2, skal indhente godkendelse fra denne person inden enhver etablering eller videreførelse af en forretningsforbindelse, hvis forretningsforbindelsen har hjemsted i et land, der er opført på Europa-Kommissionens liste over højrisikotredjelande.

Ad nr. 6: *Skærpet overvågning af forretningsforbindelsen ved at øge antallet af kontroller og ved at udvælge transaktionsmønstre, der kræver nøjere undersøgelse.*
Virksomheden skal foretage en skærpet overvågning af den pågældende kunde, hvis kunden har hjemsted i et land, der er opført på Europa-Kommissionens liste over højrisikotredjelande. Virksomheden foretager den skærpede overvågning ved at øge antallet af kontroller og undersøge kundens transaktionsmønstre. Virksomheden skal således foretage en indgående overvågning af kundeforholdet og transaktionerne for at fastslå, om kundens tilsigtede beskaffenhed med forretningsforbindelsen stemmer overens med det kendskab, virksomheden har til kunden.

Skærpede kundekendskabsprocedurer kan på baggrund af en risikovurdering i nogle tilfælde undlades for en filial eller et majoritetsejet datterselskab af en juridisk person. Der henvises nærmere til hvidvasklovens § 17, stk. 5.

Efter hvidvasklovens § 17, stk. 3, skal virksomheden gennemføre en eller flere yderligere risikobegrænsende foranstaltninger, når fysiske personer eller juridiske enheder gennemfører transaktioner, der involverer højrisikotredjelande.

Ved transaktioner forstås en eller flere handlinger, hvorved et eller flere aktiver overføres eller overdrages. Ved transaktioner, der involverer højrisikotredjelande, forstås alle typer af transaktioner til og fra et højrisikotredjeland.

Ved risikobegrænsende foranstaltninger forstås foranstaltninger, som virksomheden iværksætter for at opnå en begrænsning af risiciene for hvidvask eller finansiering af terrorisme.
Risikobegrænsende foranstaltninger skal ifølge hvidvasklovens § 17, stk. 3, bestå i en eller flere af følgende foranstaltninger:

1. Anvendelse af supplerende elementer af skærpede kundekendskabsprocedurer.
2. Indførelse af relevante skærpede indberetningsmekanismer eller systematisk indberetning af finansielle transaktioner.
3. Begrænsning af forretningsforbindelser eller transaktioner med fysiske personer eller juridiske enheder fra de tredjelande, der er identificeret som højrisikolande.

Virksomheden skal efter nærmere vurdering vælge at gennemføre en eller flere af ovenstående risikobegrænsende foranstaltninger.

Ad nr. 1: Anvendelse af supplerende elementer af skærpede kundekendskabsprocedurer.
Virksomheden skal konkret vurdere, hvilke supplerende og skærpende elementer, der ved gennemførelse af kundekendskabsprocedurer konkret kan begrænse risikoen i forhold til virksomhedens forretningsmodel. Virksomheden vil således f.eks. kunne anvende flere af de tiltag, som er opført som eksempler på skærpede kundekendskabsprocedurer, nævnt ovenfor til § 17, stk.1.

Ad nr. 2: Indførelse af relevante skærpede indberetningsmekanismer eller systematisk indberetning af finansielle transaktioner.
Virksomheden kan eksempelvis vælge at opsætte flere parametre og indberetningsmekanismer af kundens finansielle transaktioner i virksomhedens kontrol- og overvågningssystem, som dermed skærper overvågningen af kundeforholdet og specifikke transaktionsmønstre.

Ad nr. 3: Begrænsning af forretningsforbindelser eller transaktioner med fysiske personer eller juridiske enheder fra de tredjelande, der er identificeret som højrisikotredjelande.
Virksomheder, der indgår forretningsforbindelser eller transaktioner med fysiske personer eller juridiske enheder fra de tredjelande, der er identificeret som højrisikotredjelande, kan vælge f.eks. at begrænse eller indskrænke udbuddet af produkter eller tjenesteydelser til den pågældende kunde når kunden indgår forretningsforbindelser eller transaktioner med fysiske personer eller juridiske enheder fra højrisikotredjelande.

Ved forretningsforbindelser eller transaktioner, der involverer lande, som er opført på Europa-Kommissionens liste over højrisikotredjelande, skal virksomheden – udover ovenstående risikobegrænsende foranstaltninger – vurdere, om det er relevant at sikre, at første betaling foretages gennem en konto i kundens navn i et kreditinstitut, der er underlagt krav om kundekendskabsprocedurer, der mindst svarer til de kundekendskabsprocedurer, der er fastsat efter hvidvaskloven, jf. § 17, stk. 4 i hvidvaskloven.

Virksomheden skal således foretage en vurdering af, om det vil være relevant, jf. nærmere nedenfor, at gøre brug af denne ekstra risikobegrænsende foranstaltning, når en forretningsforbindelse eller en transaktion involverer et højrisikotredjeland, således at virksomheden kan styre og begrænse risiciene yderligere.

Vurderer virksomheden, at det vil være relevant at sikre, at første betaling skal foretages gennem en konto i kundens navn i et kreditinstitut, der er underlagt krav om kundekendskabsprocedurer, der mindst svarer til de kundekendskabsprocedurer, som er fastsat efter hvidvaskloven, skal første betaling således gennemføres fra en konto i et kreditinstitut, der er underlagt samme lovgivningsmæssige krav til kundekendskabsprocedure som fastsat efter hvidvaskloven. Dette kan f.eks. være et kreditinstitut i et andet EU- eller EØS-land, der har implementeret kravene i hvidvaskdirektiverne på samme niveau som i Danmark. Det kan også være en filial eller et majoritetsejet datterselskab af et kreditinstitut i Danmark, hvor

kreditinstituttet efter hvidvasklovens § 31, stk. 2, skal sikre, at filialen eller det majoritetsejede datterselskab ligeledes overholder hvidvasklovens regler, selvom det er etableret i et ikke EU- eller EØS-land.

Eksempler på hvornår det kan vurderes relevant at gennemføre denne ekstra risikobegrænsende foranstaltning.
Et pengeinstitut etablerer et kundeforhold med en højrisikokunde, der har forretningsforbindelser til et højrisikotredjeland. Pengeinstituttet er, på baggrund af indhentelse af oplysninger om forretningsforbindelsens formål og tilsigtede beskaffenhed, fortsat ikke betrygget ved kundeforholdet forretningsforbindelse til et højrisikotredjeland og vurderer det derfor relevant for at forebygge risikoen for, at pengeinstituttet bliver misbrugt til hvidvask eller terrorfinansiering. Pengeinstituttet kan derfor kræve, at kundens første betaling foretages gennem en konto i kundens navn i et andet pengeinstitut, som er underlagt krav om kundekendskabsprocedurer, der mindst svarer til de kundekendskabsprocedurer, der er fastsat efter hvidvaskloven.

Et andet eksempel kan være, at et pengeinstitut har en kunde med begrænset risiko, som ikke tidligere har foretaget transaktioner til højrisikotredjelande. Kunden ønsker nu at foretage hyppige og/eller en stor overførsel til et højrisikotredjeland. I dette tilfælde kan pengeinstituttet vurdere det relevant at sikre, at første betaling foretages gennem en konto i kundens navn i en anden bank, som er underlagt krav om kundekendskabsprocedurer, der mindst svarer til de kundekendskabsprocedurer, der er fastsat efter hvidvaskloven, for at forebygge risikoen for, at pengeinstitut bliver brugt til hvidvask eller terrorfinansiering.

Virksomhedens vurdering af, hvornår det vil være relevant at sikre, at kundens første betaling foretages gennem en konto i kundens navn i et kreditinstitut, som er underlagt krav om kundekendskabsprocedurer, der mindst svarer til de kundekendskabsprocedurer, der er fastsat efter hvidvaskloven, kan bero på såvel forretningsforbindelsens forhold som forholdene omkring transaktionen, herunder virksomhedens egne forhold og kontrolforanstaltninger vedrørende de pågældende transaktioner og kundeforhold i øvrigt.

Nogle virksomheder omfattet af hvidvaskloven vil således have mekanismer indbygget i deres procedurer og systemer, som tager højde for den risiko, der ligger i forretningsforbindelser eller transaktioner, der involverer højrisikotredjelande. I den situation kan en virksomheds vurdering af, hvorvidt det er relevant at stille krav om, at første betaling foretages gennem en konto i kundens navn i et kreditinstitut, som er underlagt krav om kundekendskabsprocedurer, der mindst svarer til de kundekendskabsprocedurer, der er fastsat efter hvidvaskloven, falde ud til, at det ikke er relevant at stille dette krav. Det kan f.eks. være, at et pengeinstitut har en større gruppe kunder med samme risikoprofil og med samme typer af transaktioner, der involverer højrisikotredjelande, og hvor banken på anden vis har sikret sig mod at blive misbrugt til hvidvask og terrorfinansiering.

Omvendt vil andre virksomheder ikke have sådanne mekanismer indbygget i deres procedurer og systemer i forhold til denne type kunder eller transaktioner. Sådanne virksomheder vil derfor kunne vurdere det relevant at stille krav om, at første betaling foretages gennem en konto i kundens navn i et kreditinstitut, som er underlagt krav om kundekendskabsprocedurer, der mindst svarer til de kundekendskabsprocedurer, der er fastsat efter hvidvaskloven.

15.Politisk eksponerede personer (PEP'er)

Henvisning til hvidvaskloven: § 2, nr. 8, § 18.

Henvisning til 4. hvidvaskdirektiv: Artikel 3, nr. 9, artikel 21, 22 og 23.
Henvisning til 5. hvidvaskdirektiv: Artikel 1, stk. 1, nr. 13.

Politisk eksponerede personer (PEP'er) er personer, der bestrider et særligt offentligt tillidshverv, og derfor kan være modtagelige for bestikkelse og anden korruption. Det er i samfundets interesse at forebygge, at dette sker, og skulle det ske, er det i samfundets interesse, at det opdages i tide og herefter retsforfølges.

På globalt plan er bestikkelse og korruption et stort problem, og der er derfor indført fælles internationale standarder for bekæmpelsen af dette. Såvel definitionen af PEP'er som kravene til at håndtere PEP'ers transaktioner er fastlagt i internationale standarder på baggrund af erfaringer indsamlet gennem en årrække fra myndigheder verden over.

Reglerne om identifikation af PEP'er er forebyggende og skal ikke tolkes som en stigmatisering af PEP'er som personer, der deltager i kriminelle aktiviteter. Virksomhederne har derfor ikke grundlag for at afvise at indgå et kundeforhold eller lukke eksisterende kundeforhold alene med den begrundelse, at en person er PEP eller er nærtstående eller nær samarbejdspartner til en PEP.

Hvidvaskloven pålægger ikke PEP'er, deres nærtstående eller nære samarbejdspartnere forpligtelser. PEP'erne bør dog være opmærksomme på, at de selv samt deres nærtstående og nære samarbejdspartnere kan blive bedt om at forklare eller dokumentere deres økonomi eller en transaktion.

For at støtte virksomhederne i arbejdet, fører Finanstilsynet på vegne af erhvervsministeren en liste over indenlandske PEP'er, som bidrager til en entydig identifikation og afgrænsning af PEP'er. Listen er offentligt tilgængelig. De organisationer, myndigheder og virksomheder, der er omfattet af bekendtgørelsen om indberetning og offentliggørelse af oplysninger om indenlandske politisk eksponerede personer, er forpligtet til at indberette til Finanstilsynet.

15.1. Hvem er PEP?

15.1.1. Politisk eksponerede personer

En politisk eksponeret person (PEP) er en person, der bestrider et eller flere af de højtstående offentlige erhverv, der er listet nedenfor. Definitionen er fælles for hele EU. Den tager dog højde for, at de enkelte medlemslande har indrettet sig forskelligt.

Virksomheden skal have procedurer til at afgøre, om en kunde, kundens reelle ejer, den begunstigede til en livsforsikringspolice eller den begunstigedes reelle ejer er PEP.

Definitionen af de indenlandske (danske) PEP'er er afgrænset således:

1) Statschef, regeringschef, minister og viceminister eller assisterende minister. Dette omfatter i Danmark ministre samt departementschefer.

2) Parlamentsmedlemmer eller medlemmer af tilsvarende lovgivende organer. Dette omfatter i Danmark medlemmer af Folketinget og danske medlemmer af Europa-Parlamentet.
3) Medlemmer af politiske partiers styrende organer. Dette omfatter i Danmark hovedbestyrelser eller tilsvarende højtstående organer i henhold til vedtægterne i politiske partier, der er repræsenteret i Folketinget.
4) Højesteretsdommere, medlemmer af forfatningsdomstole og andre højtstående retsinstanser, hvis afgørelser kun er genstand for yderligere prøvelse under ekstraordinære omstændigheder. Dette omfatter i Danmark højesteretsdommere og danske dommere ved internationale domstole.
5) Medlemmer af revisionsretter og øverste ledelsesorgan for centralbanker. Dette omfatter i Danmark direktionen for Danmarks Nationalbank, danske statsrevisorer og det danske medlem af Den Europæiske Revisionsret.
6) Ambassadører, chargé d'affaires og højtstående officerer i de væbnede styrker. Dette omfatter i Danmark de øverste chefer i de væbnede styrker, nærmere defineret som forsvarschef, viceforsvarschef, værnschefer samt ambassadører for danske ambassader.
7) Medlemmer af statsejede virksomheders administrative, ledende eller kontrollerende organer. Dette omfatter i Danmark bestyrelsen og den administrerende direktør i selskaber, hvor staten ejer 50 pct. eller mere eller på anden måde har reel kontrol over selskabet. Datterselskaber af sådanne statsejede selskaber er ikke omfattet af begrebet. Selvejende institutioner, der helt eller delvist er finansieret via finansloven, er heller ikke omfattet af begrebet.
   Definitionen omfatter også direktøren i styrelser og medlemmer af bestyrelsen i styrelser, hvor denne personkreds har en egentlig beslutningskompetence.
8) Direktører, vicedirektører, bestyrelsesmedlemmer og personer med tilsvarende hverv i internationale organisationer. Dette omfatter i Danmark personer, der er indstillet, udpeget eller ansat af regeringen, et ministerium eller en minister i en international organisation, som er etableret ved indgåelse af en formel international politisk aftale.

Finanstilsynets liste indeholder oplysninger om navn, tilhørsforhold og fødselsdato for indenlandske PEP'er og har til formål at sikre en ensartethed i brugen af definitionen for ovenstående omfattede personer. Listen angiver aktuelle PEP'er. Listen indeholder dog også et ekstra faneblad, som angiver de personer, der er ophørt som PEP'er. Personen vil stå anført på listen i minimum 12 måneder efter, at vedkommendes status som PEP er ophørt. Listen indeholder ikke oplysninger om nærtstående, nære samarbejdspartnere eller udenlandske PEP'er, som må identificeres på anden måde.

Listen bygger på oplysninger, der bliver indberettet til Finanstilsynet, hvor virksomheder, styrelser og organisationer, der står i et arbejdsgiverlignende forhold til en PEP, har indberettet navneoplysninger og ligeledes indberetter, når der sker ændringer, indenfor en frist på tre hverdage.

Listen fastlægger, hvem der er PEP'er, og den kan lægges til grund af virksomheden. En person, der ikke fremgår af listen, kan godt være PEP givet indberetningsfristen. Hvis en virksomhed eller person har konkret viden om, at en kunde er PEP, vil denne viden gå forud for listens angivelser.

15.1.2. Nærtstående og nære samarbejdspartnere

Henvisning til hvidvaskloven: § 2, nr. 6 og 7 og § 18. Henvisning til 4. hvidvaskdirektiv: Artikel 20-23.

Nærtstående og nære samarbejdspartnere til en PEP skal ikke betragtes som PEP'er alene som følge af deres forbindelse til en PEP. Nærtstående og nære samarbejdspartnere, der er kunder i virksomheden, skal identificeres, fordi de kan drage fordel af eller blive misbrugt i forbindelse med hvidvask mv.

Nærtstående
Definitionen af en nærtstående til en PEP følger af hvidvaskloven § 2, nr. 6.

Nærtstående til en PEP omfatter:

1) ægtefælle, registreret partner eller samlever
2) børn og disses ægtefæller, registrerede partnere eller samlevere
3) forældre.

Begrebet omfatter dermed ikke f.eks. søskende eller stedbørn og stedforældre.

Nære samarbejdspartnere
Definitionen af nære samarbejdspartnere til en PEP følger af hvidvaskloven § 2, nr. 7.

Nære samarbejdspartnere til en PEP omfatter:

1) En fysisk person, som er reel ejer af en virksomhed eller anden form for juridisk person i fællesskab med en eller flere PEP'er.
2) En fysisk person, der på anden måde har en nær forretningsforbindelse med en eller flere PEP'er Dette kan f.eks. være en samhandelspartner over en længere periode.
3) En fysisk person, som er den eneste reelle ejer af en virksomhed eller anden form for juridisk person, der er oprettet til fordel for en PEP. Det betyder, at den fysiske person direkte eller indirekte kontrollerer alle ejerandelene eller stemmerettighederne mv. i den pågældende virksomhed eller anden juridisk person.

En person, der deltager i bestyrelsesarbejde med en PEP, hvor bestyrelsen er vurderet til at være den reelle ejer af en juridisk person, vil ikke af den grund skulle anses for at være en nær samarbejdspartner. Virksomheden vil i sådanne tilfælde skulle vurdere, om der er tale om en nær forretningsmæssig forbindelse med en PEP, der falder ind under punkt 2 ovenfor. I fonde og andre lignende juridiske arrangementer må det bero på en konkret vurdering, om en person, der deltager i bestyrelsesarbejde med en PEP, hvor bestyrelsen er vurderet til at være den reelle ejer, skal anses for at være en nær samarbejdspartner.

En virksomhed skal behandle PEP'ers nærtstående og nære samarbejdspartnere efter samme regler som PEP'er. Derfor er den konkrete risikovurdering af en PEP også afgørende for, hvordan en virksomhed tilrettelægger kundekendskabsproceduren for PEP'ens nærtstående og nære samarbejdspartnere. Placeres en PEP i en kategori med mellem risiko, skal PEP'ens nærtstående og nære samarbejdspartnere betragtes på samme måde, medmindre virksomhedens individuelle vurdering af de pågældende tilsiger andet.

15.2. Kundekendskab og risikovurdering

15.2.1. Fastlæggelse af om en kunde er PEP, nærtstående eller nær samarbejdspartner

Henvisning til hvidvaskloven: § 18, stk. 1. Henvisning til 4. hvidvaskdirektiv: Artikel 20-23.

Virksomheden skal ud fra en risikovurdering indhente oplysninger om PEP'er. PEP'en selv vil som regel være den primære kilde til oplysningerne, men det er muligt og somme tider nødvendigt at indhente oplysninger fra andre kilder.

Virksomheden skal have forretningsgange og systemer, der sikrer, at vurderingen sker, når et kundeforhold etableres eller udvides. En virksomhed skal ved afgørelsen iagttage følgende:

1) Virksomheden skal altid søge at fastlægge, om en kunde er PEP. Det kan ske ved at konsultere den liste, som Finanstilsynet udarbejder for indenlandske PEP'er. Virksomhedens fastlæggelse af, om en kunde er udenlandsk PEP, kan ske ved at søge på internettet eller ved at bruge en kommerciel tjenesteudbyder, der tilbyder sådanne oplysninger. Hvis det påtænkte forretningsomfang ikke er ubetydeligt, kan det være nødvendigt også at spørge nærmere ind til, hvad PEP'ens stilling indebærer.
2) Virksomheden skal træffe rimelige foranstaltninger til at identificere kunder, der er nærtstående eller nær samarbejdspartner til PEP'er. Det kan ske ved at spørge PEP'en, hvis PEP'en også er kunde i virksomheden, om denne har kendskab til, at nærtstående eller nære samarbejdspartnere også er kunder. Virksomheden kan også få kendskab til nærtstående eller nære samarbejdspartnere ved at søge på internettet eller ved at bruge en kommerciel tjenesteudbyder, der tilbyder sådanne oplysninger.
3) Hvis virksomheden i øvrigt har begrundet formodning om, at en kunde er nærtstående til eller nær samarbejdspartner med en PEP, skal virksomheden træffe rimelige foranstaltninger til at fastlægge, om det er tilfældet. Dette gælder også, selvom PEP'en ikke er kunde i virksomheden.
4) En virksomhed skal træffe rimelige foranstaltninger til at afgøre, om en kunde er en udenlandsk PEP, ved etableringen af forretningsforbindelsen. I de tilfælde, hvor virksomheden alene har en formodning om eller indikation på, at en kunde er en udenlandsk PEP, bør virksomheden undersøge dette nærmere for at få det endeligt afklaret.

"Rimelige foranstaltninger"
Ved "rimelige foranstaltninger" forstås eksempelvis følgende tiltag, idet det vil være op til virksomheden i det konkrete tilfælde at vurdere, hvad der er tilstrækkeligt til at opfylde kravene i hvidvaskloven:

14) Virksomheden indhenter oplysninger hos den pågældende PEP.
15) Virksomheden bruger den information om kunderne, der allerede er tilgængelig i virksomheden.
16) Virksomheden bruger de eksterne kilder, som virksomheden har adgang til, f.eks. internet og nyhedsmedier.
17) Virksomheden abonnerer hos en eller flere af de tjenesteudbydere, der tilbyder information om, hvem der er PEP, nærtstående til en PEP eller nær samarbejdspartner med en PEP.
18) Virksomheden verificerer aktivt oplysninger, som virksomheden er usikker på, f.eks. ved at spørge de relevante kunder.

19) Hvad udenlandske PEP'er angår, overvejer virksomheden, om den må samarbejde med lokale på stedet, f.eks. advokater, bankforbindelser mv. i det pågældende land, for at få afklaret, om der er tale om en PEP.

Hvis en virksomhed alene har et begrænset antal kunder, vil det efter en risikovurdering kunne være en tilstrækkelig procedure at få den enkelte kunde til at oplyse, om denne er PEP, og/eller rutinemæssigt at søge på kundernes navne på internettet.

Kommercielle udbydere af PEP-lister
Virksomheden kan som en del af sine forretningsgange for kundekendskab abonnere på private kommercielle udbydere af løsninger til PEP-lister og fastlæggelse af nærtstående og nære samarbejdspartnere til PEP'er. Brugen af sådanne systemer vil normalt være en hensigtsmæssig måde at skaffe oplysningerne på, men er ikke et krav. Virksomheden bør dog vurdere, om der er behov for at virksomheden (også) benytter andre kilder til informationen.

Reelle ejere
Når en virksomhed fastlægger de reelle ejere af en kunde (juridisk person), skal virksomheden fastlægge, om der er PEP'er blandt disse. Det skal ske efter de samme principper, som virksomheden skal følge, når den fastlægger, om en kunde er PEP. Hvis der blandt en kundes reelle ejere er en PEP, medfører dette dog ikke i sig selv, at kunden skal behandles på samme måde som en PEP. Virksomheden skal foretage en konkret risikovurdering med udgangspunkt i PEP'ens kontrol over kunden, og virksomheden skal vurdere, om kunden handler på vegne af PEP'en.

En forsikringsvirksomhed skal i relation til den begunstigede i henhold til en forsikringspolice fastlægge, om den begunstigedes reelle ejer i en forsikringspolice er en PEP. Fastlæggelsen heraf skal ske, inden udbetalingen finder sted eller ved hel eller delvis overdragelse af policen.

Tidspunkt for fastlæggelsen
Virksomheden skal gennemføre kundekendskabsprocedurer for alle kunder, når den etablerer forretningsforbindelser. Samtidig skal virksomheden fastlægge, om en kunde er PEP, nærtstående eller nær samarbejdspartner.

Det er tilstrækkeligt, at pensionsselskaber, firmapensionsordninger og arbejdsmarkedspensionsordninger fastlægger, om en kunde er PEP, samtidig med at etableringen af kundeforholdet er iværksat.

Det er særligt for PEP'er, deres nærtstående og nære samarbejdspartnere, at deres status kan ændre sig i løbet af kundeforholdet. En kunde, der ikke er PEP, kan f.eks. blive PEP ved at få en ny stilling eller blive valgt til Folketinget. Virksomheden skal derfor løbende overvåge, om kunder er blevet PEP'er. Det kan f.eks. ske:

1) ved tilstrækkeligt hyppigt at gennemgå tilgængelige oplysninger om, hvem der er PEP'er, herunder Finanstilsynets liste over PEP'er, og holde disse oplysninger op mod virksomhedens kunderegister,
2) når et kundeforhold i øvrigt gennemgås, f.eks. ved optagelse af nye lån, og
3) når en kundes transaktion giver anledning til nærmere undersøgelser.

Hvis en person ophører med at være PEP, skal risikovurderingen og overvågningen fortsætte i mindst 12 måneder herefter, se afsnit 15.2.6 om ophør af PEP-status.

15.2.2. Oprindelsen af midlerne og formuen

Henvisning til hvidvaskloven: § 18, stk. 2. Henvisning til 4. hvidvaskdirektiv: Artikel 20-23.

Virksomheden skal træffe passende foranstaltninger for at fastslå oprindelsen af PEP'ens midler og formue. Virksomheden kan nøjes med at indhente oplysninger om de midler og den del af formuen, der er omfattet af forretningsforbindelsen eller transaktionen. Et realkreditinstitut er eksempelvis ikke forpligtet til at spørge ind til PEP'ens beholdning af eventuelle værdipapirer. Ved optagelse af realkreditlån vil den sædvanlige låneprocedure være tilstrækkelig til at fastslå PEP'ens formueforhold. Ved førtidig tilbagebetaling af lånet skal realkreditinstituttet fastslå midlernes oprindelse. PEP'ens bankforbindelse vil dog ofte skulle fastslå en del flere forhold vedrørende oprindelsen af midlerne og formuen, fordi kundeforholdet typisk omfatter flere ydelser, som kan være forbundet med risici for hvidvask.

Virksomheden skal fastslå oprindelsen af PEP'ens midler og formue på baggrund af en risikovurdering. Den kan f.eks. indeholde oplysninger om:

1) i hvilket land kunden har bopæl,
2) dens stilling, og
3) kundens renommé.

Passende foranstaltninger kan også være, at virksomheden indlægger en risikovurdering i forhold til det produkt, en kunde har valgt. Ved produkter med høj risiko og store transaktioner må virksomheden foretage mere tilbundsgående undersøgelser end f.eks. ved en livsforsikring med en lav årlig præmie. Omvendt kan virksomheden foretage mindre tilbundsgående undersøgelser ved produkter med en begrænset risiko.

Nogle pensionsselskaber har ikke direkte kundekontakt, fordi der er tale om obligatorisk firmapension eller arbejdsmarkedspension, som kunden ikke selv kan indbetale på. I de tilfælde bør kundens økonomiske forhold ikke fastlægges med samme detaljeringsgrad som f.eks. ved andre former for forsikring.

På baggrund af risikovurderingen kan virksomheden bede kunden om at give de fornødne oplysninger. Det kan være nødvendigt at indhente oplysningerne hos den pågældende, hvis virksomheden ikke er i besiddelse af oplysningerne i forvejen, eller hvis de oplysninger, som virksomheden har, ikke længere vurderes at være aktuelle. Behovet for og omfanget af oplysningerne må vurderes på baggrund af omstændighederne, herunder kundens transaktioner. I visse situationer, eksempelvis et flerårigt kundeforhold, hvor virksomheden i forvejen har et godt indblik i kundens økonomiske forhold, vil den på baggrund af en risikovurdering kunne beslutte, at kendskabet er tilstrækkeligt til at kunne fastslå oprindelsen af de midler og den del af formuen, der er omfattet af forretningsforbindelsen. Virksomheden kan også indhente oplysningerne hos eksterne kilder.

Det vil altid være kundens midler og formue, der skal undersøges, da det er disse midler, der er omfattet af forretningsforbindelsen eller transaktionen. I tilfælde, hvor PEP'en er reel ejer af kunden (en juridisk person), er det derfor stadig kundens (den juridiske persons) midler og formue, der er omfattet af bestemmelsen, og ikke den reelle ejers midler eller formue.

De oplysninger, virksomheden kan lægge til grund, kan eksempelvis være følgende eller en kombination heraf:

- Årsopgørelse fra Skatteforvaltningen.
- Lønsedler.
- Regnskabsoplysninger.
- Eventuelle virksomhedsårsrapporter.
- Udskrifter fra selskabsbøger/virksomhedsudskrifter fra offentlige registre berigtiget af kunden til at dokumentere ejerforhold.
- Ejendomsoplysninger, herunder ejendomsskatteoplysninger og BBR-oplysninger.
- Oplysninger om værdipapirer i depot, herunder i udenlandske depoter.
- Oplysninger fra kontobevægelser mv.

Detaljerede oplysninger om PEP'ens formueforhold i forbindelse med kundekendskabsproceduren, herunder oplysninger om midlernes oprindelse, kan undlades, hvis kunden ikke får adgang til et produkt, der giver mulighed for at foretage transaktioner.

15.2.3. Godkendelse af kundeforholdet

Henvisning til hvidvaskloven: § 18, stk. 3. Henvisning til 4. hvidvaskdirektiv: Artikel 20-23.

Virksomhedens hvidvaskansvarlige (§ 7, stk. 2-personen) skal godkende et kundeforhold med en PEP samt kundeforhold med nærtstående og nære samarbejdspartnere til en PEP. Det er ikke et krav, at andre i virksomhedens ledelse godkender kundeforholdet, bortset fra de godkendelser, der følger af anden lovgivning, f.eks. ledelsesbekendtgørelsen og virksomhedens interne politikker og forretningsgange.

Med godkendelsen vurderer den hvidvaskansvarlige, at virksomheden med det påtænkte kundeforhold fortsat kan leve op til lovgivningen, og at virksomheden derfor kan indgå kundeforholdet. Ved godkendelsen bør den hvidvaskansvarlige tage højde for, i hvilket omfang produktet i sig selv indebærer en risiko for at kunne bruges til hvidvask.

Hvis den hvidvaskansvarlige finder, at risikoen for, at virksomheden kan blive misbrugt i forbindelse med bestikkelse og andre former for korruption, er for høj, skal den hvidvaskansvarlige afstå fra at godkende kundeforholdet.

Kravet om godkendelse forudsætter ikke, at den hvidvaskansvarlige skal foretage en egentlig prøvelse af alle oplysningerne i det enkelte kundeforhold. Godkendelsen skal dog ske på et tilstrækkeligt oplyst grundlag. Der ligger heller ikke i kravet, at den hvidvaskansvarlige skal kreditvurdere kunden, vurdere, om forsikringsdækning er passende, eller på anden måde vurdere, om de tjenesteydelser, virksomheden tilbyder kunden, er passende for kunden. Dog bør den hvidvaskansvarlige vurdere, om påtænkte aftaler med kunden f.eks. giver kunden særlig mulighed for at skjule bestikkelse.

Særligt hvad angår videreførelse af kundeforhold, bør virksomheden i sine procedurer fastlægge et passende interval for gennemgang og eventuel fornyet godkendelse af kundeforhold med PEP'er, nærtstående eller nære samarbejdspartnere til PEP'er. Intervallet bør fastsættes ud fra den risiko for hvidvask eller korruption, som virksomheden vurderer, at kunden potentielt udgør. Det vil derfor ofte være relevant at fastsætte forskellige intervaller, f.eks. ved at differentiere mellem PEP'er og nærtstående eller nære samarbejdspartnere til en PEP, som er henholdsvis fra eller ikke fra lande kendt for et højt korruptionsniveau.

Hvis en virksomhed vurderer, at den ikke kan godkende eller videreføre et kundeforhold, som er omfattet af bestemmelsen, må virksomheden vurdere, om den skal træffe foranstaltninger om afbrydelse eller afvikling af kundeforholdet. Hvad angår eksisterende kundeforhold, som virksomheden ikke kan godkende, henvises desuden afsnit 18.1 om virksomhedens pligt til at afbryde eller afvikle et kundeforhold.

Når virksomheden er et pensionsselskab og ikke har direkte kundekontakt, fordi der er tale om en obligatorisk firmapension eller arbejdsmarkedspension, er det ikke et krav, at den hvidvaskansvarlige godkender kundeforholdet.

15.2.4. Skærpet overvågning

Henvisning til hvidvaskloven: § 18, stk. 4. Henvisning til 4. hvidvaskdirektiv: Artikel 20-23.

Risikovurdering
Når virksomheden har identificeret kunden, skal virksomheden foretage en risikovurdering af kundeforholdet. Risikovurderingen skal bl.a. fastlægge, om PEP'en eller dennes nærtstående eller nære samarbejdspartner, kan misbruge virksomheden til at dække over hvidvask, herunder bestikkelse.

Risikovurderingen skal indeholde de relevante risikofaktorer for det pågældende kundeforhold. Det vil i høj grad være en individuel vurdering.

Ved risikovurderingen bør virksomheden lægge vægt på følgende:

1) Virksomhedens egen vurdering af de risici for hvidvask, som virksomheden er udsat for.
2) En vurdering af, i hvilket omfang risikoen ville blive øget ved et forretningsforhold med den pågældende PEP, og/eller dennes nærtstående eller nære samarbejdspartnere. Det er en sag-til-sag-vurdering og ikke en automatisk vurdering, om et kundeforhold skaber risiko for hvidvask.
3) Eventuelle oplysninger fra offentlige myndigheder. Dette omfatter såvel de nationale risikovurderinger i de pågældende lande som de internationale risikovurderinger.

PEP'ens funktion og risikoeksponering i forhold til de produkter eller tjenesteydelser, som PEP'en ønsker eller har i virksomheden, skal samlet set udgøre grundlaget for vurderingen af kundeforholdets risikokategorisering.

Kategoriseringen afhænger som nævnt af en individuel vurdering baseret på den konkrete risikovurdering af kundeforholdet. En kunde kan eksempelvis placeres i kategorier som øget risiko eller normal risiko.

Det er også muligt at placere kunder i to kategorier, f.eks. øget og normal/begrænset. Det væsentligste er her, at virksomheden identificerer kunder med høj risiko.

Om risikoen vil blive øget ved et forretningsforhold med den pågældende PEP og/eller dennes nærtstående eller nære samarbejdspartnere, kan afhænge af:

1) Den pågældendes position og mulighed for politisk og administrativ indflydelse samt kundeforholdets karakter, herunder de produkter eller tjenesteydelser, virksomheden tilbyder kunden. Dette vil variere afhængigt af arten af en persons funktion. Der vil typisk være tale om stor politisk og administrativ indflydelse, hvis den pågældende er bemyndiget til at træffe afgørende politiske eller administrative beslutninger eller kan omgøre eller ændre sådanne beslutninger. Der kan f.eks. være tale om:
    - ministre
    - departementschefer
    - direktører i organer, der kan træffe uafhængige beslutninger på væsentlige områder.
2) Karakteren af den pågældendes stilling, og om der er risiko for misbrug af stillingen. Hvis en position holdes i et land, hvor der vurderes at være begrænset risiko for omfattende korruption, vil den pågældende kunne have en fremtrædende offentlig funktion, uden at der er en forøget risiko.
3) Muligheden for, at en tjenesteydelse kan bruges til at dække over korruption, f.eks. til at placere pengebeløb eller til at kanalisere pengebeløb til andre juridiske personer eller til konti i udlandet.
4) Andre relevante risikofaktorer.

Virksomheden skal søge at fastlægge, hvilken funktion PEP'en har, og hvilken indflydelse eller potentiel indflydelse denne funktion indebærer, samt om PEP'en er i særlig risiko for at være involveret i bestikkelse eller anden form for korruption.

En minister med stor politisk og administrativ indflydelse vil alene på baggrund af sin funktion være forbundet med større risiko end et menigt medlem af Folketinget. På samme måde vil en bestyrelsesformand med større politisk og administrativ indflydelse end et almindeligt bestyrelsesmedlem alene på baggrund af sin funktion være forbundet med større risiko.

Følgende produkter og tjenesteydelser vil normalt kunne indebære en begrænset risiko for hvidvask og korruption efter hvidvasklovens bilag 2. Dette gælder ikke kun for PEP'er, men for alle kunder:

a) Livsforsikringer, hvor den årlige præmie er lav.
b) Pensionsforsikringer, hvis der ikke er nogen tidlig tilbagekøbsklausul, og policen ikke kan bruges til sikkerhedsstillelse.
c) Pensionsordninger el.lign., der udbetaler pension til ansatte, og hvor bidragene indbetales gennem fradrag i lønnen, og reglerne for den pågældende ordning ikke tillader overdragelse af et medlems rettigheder i henhold til ordningen.
d) Finansielle produkter eller tjenesteydelser, som leverer behørigt definerede og begrænsede tjenesteydelser til visse kundetyper med det formål at fremme finansiel inklusion.
e) Produkter, hvor risikoen for hvidvask af penge og finansiering af terrorisme styres af andre faktorer, f.eks. udgiftslofter eller gennemsigtighed i forhold til ejerskab (f.eks. visse former for elektroniske penge).

Følgende produkter og tjenesteydelser vil normalt i sig selv kunne indebære en øget risiko for hvidvask og korruption efter bilag 3, pkt. 2. Dette gælder ikke kun for PEP'er, men for alle kunder:

1) Private banking.
2) Produkter eller transaktioner, som kan fremme anonymitet.
3) Forretningsforbindelser eller transaktioner uden direkte kontakt og uden sikkerhedsforanstaltninger såsom elektroniske underskrifter.
4) Betalinger fra ukendte eller ikkeassocierede tredjemænd.
5) Nye produkter og nye forretningsprocedurer, herunder nye leveringsmekanismer, og brug af nye teknologier eller teknologier under udvikling til både nye og eksisterende produkter.

En PEP, der i kraft af sin stilling vurderes at have en særlig høj politisk og administrativ position, jf. ovenfor, vil normalt skulle placeres i kategorien høj risiko, hvis PEP'en ønsker at foretage andre end almindelige forretninger, som f.eks. oprettelse af lønkonti, porteføljeplejeaftaler og andre lignende normale transaktioner. Virksomheden skal være opmærksom på, at risikoen for bestikkelse og anden korruption som regel ikke afhænger af størrelsen og sammensætningen af kundens formue.

Virksomheden er ikke forpligtet til at have en særlig kategorisering af PEP'er. Den kategorisering, som virksomheden bruger til andre kunder, kan også bruges til PEP'er. Eksempelvis kan kategorien høj risiko indeholde såvel PEP'er med høj risiko som andre kunder med høj risiko. Tilsvarende vil en PEP, der vurderes at indebære en begrænset risiko, efter omstændighederne kunne placeres i en kategori med normal risiko.

Kategoriseringen er relevant for virksomhedens fastlæggelse af behovet for overvågning af PEP'en og/eller dennes nærtstående og nære samarbejdspartnere. Virksomheden skal udføre skærpet overvågning, indtil virksomheden vurderer, at personen ikke længere udgør en øget risiko for hvidvask og korruption. Hvis personens hverv er ophørt, skal faktorer som f.eks. personens fortsatte relation til sit tidligere hverv, herunder tidligere samarbejdspartnere og kolleger, indgå i vurderingen.

Kravet om, at den skærpede overvågning skal fortsætte, indtil det er vurderet, at personen ikke længere udgør en øget risiko gælder ikke for nærtstående eller nære samarbejdspartnere. Virksomheden bør dog vurdere, om også disse personer fortsat kan være forbundet med en højere risiko for hvidvask. I bekræftende fald bør virksomheden tilrettelægge kundekendskabsprocedurer og overvågning efter den vurderede risiko.

Kundeovervågning
Overvågning af PEP'ers transaktioner kan ske med samme systemer, som virksomheden bruger til at overvåge andre kunder med samme risikokategorisering. Virksomheden behøver altså ikke at have andre systemer til overvågning af PEP'er end de systemer, virksomheden bruger til overvågning af andre kunder. Systemerne skal dog være indrettet sådan, at en skærpet overvågning er mulig. Virksomheden skal løbende overvåge alle kunders transaktioner med henblik på at konstatere, om transaktionerne er usædvanlige for såvel kunden selv som for andre lignende kunder. Transaktioner kan være usædvanlige med hensyn til:
1) størrelse,
2) hyppighed,
3) afsender og modtager af en betaling til, hhv. fra PEP'en,
4) at de sker gennem komplicerede selskabskonstruktioner,
5) at de sker gennem mange led,
6) at de sker gennem led, der ikke virker naturlige for den pågældende transaktion,
7) at de foretages i valutaer, der ikke er sædvanlige for den pågældende kunde.

Overvågningen skal dog være skærpet for PEP'er og være baseret på en risikovurdering.

En skærpet overvågning vil, afhængig af virksomhedens systemer til overvågning, kunne indebære:

1) at der er en hyppigere opdatering af kundekendskabet (dvs. formål og omfang med kundeforholdet) end for kunder med begrænset risiko,
2) at overvågningen af PEP'ers transaktioner sker hyppigere end for kunder med begrænset risiko,
3) at der er øget opmærksomhed på mistænkelige transaktioner gennem intensivering af den maskinelle overvågning af kundeforholdet,
4) at kriterierne for, hvornår transaktioner bliver taget ud til individuel vurdering, er strengere end for andre kunders transaktioner,
5) at der foretages en manuel granskning af PEP'ers transaktioner i højere grad end for kunder med begrænset risiko,
6) at der er skærpede kriterier for, hvornår virksomheden spørger ind til transaktionerne, og jo mindre forklaringerne giver mening eller er sandsynlige, desto mere skal virksomheden efterspørge dokumentation, og
7) at der er skærpede kriterier (f.eks. lavere beløbsgrænser) for, hvornår virksomheden indhenter dokumentation for transaktioner og formuebevægelser. Det kan f.eks. være dokumentation for tildeling af medarbejderaktier, salg af bolig, arv, bodeling mv., idet PEP'en sædvanligvis og let vil kunne give denne dokumentation (f.eks. brev fra arbejdsgiver eller advokat).

Intensiteten af den skærpede overvågning bør være proportional med virksomhedens vurdering af risikoen. Jo større risikoen er, desto mere skal overvågningen skærpes.

Udenlandske PEP'er

Virksomheden skal altid gennemføre skærpede kundekendskabsprocedurer, når virksomheden indgår forretningsforbindelse med en udenlandsk PEP. Udenlandske PEP'er vil ofte udgøre høj risiko, fordi virksomheden ikke har samme førstehåndskendskab som i forhold til indenlandske PEP'er. Virksomheden vil som udgangspunkt ikke have samme adgang og kendskab til informationer om personens hverv, graden af personens beføjelser og kontrol i kraft af hvervet lønniveau.

En PEP kan udgøre en høj risiko, hvis den pågældende har en fremtrædende offentlig funktion i et land, der anses for at have en større risiko for korruption. Virksomheden bør træffe alle rimelige foranstaltninger til at vurdere, om landet på baggrund af foreliggende oplysninger er eller kan være karakteriseret ved f.eks.:

- Politisk ustabilitet.
- Svage statsinstitutioner.
- Svag beskyttelse mod hvidvask.
- Væbnet konflikt.
- Ikkedemokratiske regeringsformer.
- Udbredt organiseret kriminalitet.
- En politisk økonomi domineret af et lille antal personer/enheder med tætte forbindelser til staten.
- Fravær af eller mangler i en fri presse og lovlige eller andre foranstaltninger, der begrænser journalistisk undersøgelse.
- Et strafferetligt system, der er sårbart overfor politisk indblanding.
- Manglende ekspertise og færdigheder i forbindelse med bogføring, regnskab og revision, især i den offentlige sektor.

- Lov og kultur, som virker imod whistleblowers interesser.
- Svagheder i gennemsigtigheden af ejerregistre for virksomheder, jord og aktier.
- Overtrædelse af menneskerettigheder.

Omvendt kan der være mulighed for at PEP'er indgår i kategorien som almindelig risiko, hvis de besidder en stilling i et land, hvor risikoen for korruption er lav. Virksomheden skal træffe alle rimelige foranstaltninger til at vurdere, om landet på baggrund af foreliggende oplysninger er eller kan være karakteriseret ved f.eks.:

1) Politisk stabilitet og frie og retfærdige valg.
2) Stærke og uafhængige statsinstitutioner.
3) Troværdige foranstaltninger mod hvidvask.
4) En fri presse.
5) Et uafhængigt retsvæsen og et strafferetligt system uden politisk indblanding.
6) Et system, hvor politisk korruption og lignende forseelser bliver effektivt undersøgt og retsforfulgt.
7) Stærke traditioner for revision indenfor den offentlige sektor.
8) Juridisk beskyttelse af whistleblowere.
9) Veludviklede registre for ejerskab af jord, virksomheder og aktier.

15.2.5. Begunstigede i henhold til forsikringspolicer

Henvisning til hvidvaskloven: § 18, stk. 5. Henvisning til 4. hvidvaskdirektiv: Artikel 20-23.

Hvis en begunstiget eller en reel ejer af en begunstiget i henhold til en forsikringspolice er PEP, skal virksomheden på baggrund af en risikovurdering sikre, at omstændighederne omkring forsikringsforholdet afklares. Den hvidvaskansvarlige skal desuden orienteres om, at udbetaling skal finde sted i henhold til forsikringspolicen og i tilfælde af en hel eller delvis overdragelse af policen.

Kravene gælder både inden udbetaling påbegyndes og i forbindelse med hel eller delvis overdragelse af policen, når den begunstigede er PEP, eller når den begunstigedes reelle ejer er en PEP. I de tilfælde, hvor der er tale om, at den begunstigede er en juridisk person, er det relevant at afklare, om dennes reelle ejer er en PEP. Kravet gælder også, når den begunstigede eller dennes reelle ejer er en nærtstående eller en nær samarbejdspartner til en PEP.

Der er f.eks. tale om delvis overdragelse, hvis en livsforsikring bliver brugt til at stille sikkerhed for et lånearrangement. Det er helt normalt, at långiver i forbindelse med oprettelse af et lån eller efterfølgende sikrer ydelsen af lånet i tilfælde af f.eks. dødsfald. Sikkerhedsstillelse bevirker ikke, at långiver/panthaver bliver begunstiget, men en eventuel begunstiget i livsforsikringen må typisk vige for panthaverens krav. Nogle forsikringspolicer kan omsættes, og sker dette, vil der være tale om en overdragelse i henhold til hvidvasklovens § 18, stk. 5. Der er typisk kun praksis for overdragelse af privattegnede livsforsikringer, da det fremgår af betingelserne for de fleste firmapensions- og arbejdsmarkedspensionsordninger, at de ikke kan stilles til sikkerhed for lån eller overdrages til tredjemand. Det forhold, at omstændighederne omkring forsikringsforholdet skal afklares, betyder, at virksomheden bør foretage en nærmere undersøgelse af forretningsforbindelsen med forsikringstager.

Undersøgelsen bør tage udgangspunkt i, om den begunstigede eller dennes reelle ejer er PEP, med det formål at afklare, om der kan være korruption eller anden kriminalitet involveret i forsikringsforholdet. Virksomheden kan f.eks. vurdere, om det er naturligt, at den pågældende person er den begunstigede i forsikringsforholdet. Hvis virksomheden i forbindelse med undersøgelsen opdager forhold, der forekommer mistænkelige, skal virksomheden foretage underretning til Hvidvasksekretariatet, se afsnit 25 om underretningspligt.

Det er et krav, at virksomheden orienterer den hvidvaskansvarlige, inden der sker udbetaling eller hel eller delvis overdragelse af en forsikringspolice til en begunstiget, som er PEP, eller til en begunstiget, hvis reelle ejer er PEP. Der er ikke tale om, at den hvidvaskansvarlige skal godkende udbetalingen eller overdragelsen. Den hvidvaskansvarlige bør dog orienteres i så god tid, at vedkommende har mulighed for at reagere, hvis det vurderes, at udbetalingen eller overdragelsen er forbundet med en risiko for hvidvask eller korruption.

15.2.6. Ophør af PEP-status

Henvisning til hvidvaskloven: § 18, stk. 6. Henvisning til 4. hvidvaskdirektiv: Artikel 20-23.

Når en person ikke længere i medfør af sin stilling skal betragtes som PEP, skal virksomheden i minimum 12 måneder efter ophøret af personens PEP-status vurdere, om der er en øget risiko forbundet med personen.

Det gælder dog ikke for PEP'ens nærtstående eller nære samarbejdspartnere. Disse skal som udgangspunkt behandles som andre kunder, når PEP'en ikke længere er PEP. Nærtstående eller nære samarbejdspartnere vil alene skulle undergives skærpede kundekendskabsprocedurer, hvis virksomheden vurderer, at der er grundlag for at betragte kunden som værende i kategorien med højere risiko.

Kravet om vurdering i minimum 12 måneder blev indført i forbindelse med ikrafttrædelsen af den nye hvidvasklov. Virksomheder er dermed ikke forpligtet til at iagttage kravet for så vidt angår kunder, der ophørte med at være PEP'er før lovens ikrafttræden. Dette gælder uanset, om kundens status som PEP ophørte tidligere end 12 måneder før loven trådte i kraft.

16. Lempede kundekendskabsprocedurer

Henvisning til hvidvaskloven: § 21.

Henvisning til 4. hvidvaskdirektiv: Artikel 15 og 16.

Henvisning til: Bekendtgørelse nr. 311 af 26. marts 2020 om lempede krav til kundekendskabsproceduren efter lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme (hvidvaskloven).

Virksomheden kan ud fra en risikovurdering anvende lempede kundekendskabsprocedurer i forhold til de forretningsforbindelser, der vurderes at have en begrænset risiko for hvidvask og finansiering af terrorisme.

Lempede kundekendskabsprocedurer er en mulighed, som virksomheden kan benytte efter en konkret vurdering. Det er ikke et krav til virksomheden, som eksempelvis kravet om, at der i tilfælde med høj risiko skal gennemføres skærpede kundekendskabsprocedurer.

De lempede procedurer er ikke en undtagelse til kravene til kundekendskabsprocedurer i hvidvaskloven. Det er derfor alene en mulighed for at justere den videre kundekendskabsprocedure og overvågning af kunden. Det betyder, at alle kravene i § 11 skal opfyldes, men de kan opfyldes med et minimum af foranstaltninger.

Virksomheden kan fastlægge, om kunden eller transaktionen indebærer begrænset risiko. Det betyder, at virksomheden først skal vurdere konkret, om der i relation til kunden eller transaktionen er risikofaktorer, der kan indikere, at der ikke er begrænset risiko, før virksomheden må gennemføre de lempede kundekendskabsprocedurer.

Vurderingen skal være en objektiv vurdering af kundens omstændigheder, herunder.

a) produktet eller ydelsen, som kunden ønsker
b) formålet, omfanget, regelmæssigheden og varigheden af forretningsforbindelsen med kunden.

I vurderingen skal virksomheden tage de faktorer, der følger af hvidvasklovens bilag 2, i betragtning.

Eksempler på lempede kundekendskabsprocedurer kan være:

1) At virksomheden indhenter begrænsede identitetsoplysninger om kunden, dog skal det sikres, at kundens identitet kontrolleres - ved begrænsede identitetsoplysninger forstås, at lovens minimumskrav, som er indhentelse af navn og cpr-nr. eller lignende, opfyldes, men at der f.eks. ikke indhentes yderligere identitetsoplysninger.
2) At virksomheden gennemfører kundekendskabsprocedurer med henblik på at opdatere kundens identitetsoplysninger sjældnere end for andre kunder, f.eks. sjældnere end for kunder med mellem og høj risiko.
3) At virksomheden ikke indhenter oplysninger om kundens formål med forretningsforbindelsen, fordi det er givet i selve produkttypen, og fordi produkttypen ikke har høj risiko.

4) At virksomheden overvåger kunden i et mere begrænset omfang, end virksomheden f.eks. overvåger kunden med en højere risikoprofil. Overvågning af forretningsforbindelsen med kunden kan dog ikke undlades.

Undtagelse for udstedere af elektroniske penge
Udsteder af elektroniske penge kan i visse tilfælde undtages fra kravene til kundekendskabsprocedurer i hvidvasklovens §§ 11, 14 og 18.

Følgende kumulative betingelser skal være opfyldt:

1) Betalingsinstrumentet er ikke genopfyldeligt eller har en maksimal månedlig betalingstransaktionsgrænse på 150 euro, som udelukkende kan anvendes i Danmark.
2) Det maksimale elektronisk lagrede beløb må ikke overstige 150 euro.
3) Betalingsinstrumentet kan udelukkende anvendes til køb af varer eller tjenesteydelser.
4) Betalingsinstrumentet kan ikke finansieres med anonyme elektroniske penge, og
5) Udstederen skal foretage tilstrækkelig overvågning af transaktioner eller forretningsforbindelser til at kunne opdage usædvanlige eller mistænkelige transaktioner.

Der henvises i øvrigt til afsnit 1.4.2. om lempede krav til kundekendskabsproceduren for udstederen af elektroniske penge.

17. Tidspunkt for gennemførelse af kundekendskabsprocedurer

Henvisning til hvidvasklovens: § 14, stk. 1-4. Henvisning til 4. hvidvaskdirektiv: Artikel 10, stk. 1 og 14, stk. 1-3.

Virksomheden skal altid identificere og kontrollere kunden og eventuelle reelle ejere inden, at virksomheden etablerer forretningsforbindelsen til kunden eller gennemfører en enkeltstående transaktion.

Virksomheden kan dog godt etablere forretningsforbindelsen til kunden eller gennemføre transaktionen i forbindelse med, at virksomheden opfylder kravene om indhentelse af oplysninger om kundens formål og forretningsforbindelsens tilsigtede beskaffenhed.

Dette forudsætter dog, at de indledende kundekendskabsprocedurer, der skal sikre kontrol af identiteten af kunden eller transaktionen, ikke har vist at kunden eller transaktionen har øget risiko. Er dette tilfældet, skal virksomheden gennemføre skærpede kundekendskabsprocedurer, inden forretningsforbindelsen etableres eller transaktionen gennemføres.

Virksomheden skal fastsætte kravene til de indledende kundekendskabsprocedurer i forhold til den risiko for hvidvask og finansiering af terrorisme, der er forbundet med den enkelte forretningsforbindelse eller transaktion.

Hvis forretningsforbindelsen eller transaktionen indebærer en øget risiko, skal virksomheden gennemføre yderligere foranstaltninger. Virksomheden skal følge de krav, som hvidvaskloven stiller til skærpede kundekendskabsprocedurer, f.eks. ved en forretningsforbindelse til en PEP. Hvis forretningsforbindelsen ikke

er omfattet af hvidvasklovens skærpede kundekendskabskrav i §§ 18 eller 19, skal virksomheden gennemføre skærpede kundekendskabsprocedurer, som efter virksomhedens vurdering er nødvendige for at imødegå den øgede risiko for hvidvask og finansiering af terrorisme.

Kundekendskabsprocedurer skal gennemføres i hele kundeforholdet, dvs. fra etableringen til den endelige afvikling af forretningsforbindelsen. Kundekendskabsprocedurer kan derfor aldrig afsluttes, før forretningsforbindelsen er afviklet. Ved kundeforhold med begrænset risiko har virksomheden mulighed for at gennemføre dele af kundekendskabsprocedurerne, herunder indhente oplysninger om formål og tilsigtet beskaffenhed, efter at etableringen er sket.

Virksomhedens kundekendskabsprocedurer skal altid gennemføres på baggrund af en risikovurdering.

17.1. Kontrol af identitetsoplysninger under etablering af forretningsforbindelsen

Kravet om, at virksomheden altid skal foretage identifikation og kontrol af en kunde, inden forretningsforbindelsen etableres eller inden en enkeltstående transaktion gennemføres, kan undtagelsesvist fraviges.

Kontrollen af identitetsoplysninger kan gennemføres under etableringen af forretningsforbindelsen, hvis:

1) det er nødvendigt for ikke at afbryde den normale forretningsgang, og
2) der er begrænset risiko for hvidvask eller finansiering af terrorisme.

De to betingelser skal begge være opfyldt, før undtagelsesmuligheden er gældende, og kontrollen af identitetsoplysninger skal i disse tilfælde gennemføres hurtigst muligt.

Hvis det viser sig, at det ikke er muligt at gennemføre kontrollen, kan der være pligt for virksomheden til at afbryde eller afvikle forretningsforbindelsen. Undtagelsen giver alene adgang til, at de indledende kundekendskabsprocedurer kan foretages under eller efter etableringen af forretningsforbindelsen, men der er ikke mulighed for, at de kan undlades.

Ad: Det er nødvendigt for ikke at afbryde den normale forretningsgang

Med ”den normale forretningsgang” forstås den procedure, der i normale tilfælde foregår, når virksomheden etablerer en forretningsforbindelse med en kunde. Det er vigtigt at bemærke, at det kræver en vurdering af, at det i den konkrete situation er nødvendigt at udskyde kontrollen af identitetsoplysninger.

Undtagelsen giver virksomheden mulighed for f.eks. at påbegynde etablering af en forretningsforbindelse ved f.eks. at oprette en konto eller indhente oplysninger til at påbegynde en rådgivningsopgave. Virksomheden kan dog ikke gå videre og f.eks. foretage en transaktion eller udføre rådgivningsopgaven, før forretningsforbindelsens identitetsoplysninger er indhentet og kontrolleret.

Ad: Der ikke er risiko for hvidvask eller finansiering af terrorisme

Denne betingelse skal ses i sammenhæng med den risikovurdering, som virksomheden foretager i forbindelse med etablering af en ny forretningsforbindelse og de indledende kundekendskabsprocedurer. For at en eventuel etablering af en forretningsforbindelse kan påbegyndes, uden at identitetsoplysninger er kontrolleret, er det er en ufravigelig betingelse, at forretningsforbindelsen indebærer en begrænset risiko.

17.2. Transaktioner med værdipapirer for en kunde

Der gælder en særlig undtagelse til kravet om, at identitetsoplysninger indhentes og kontrolleres, inden en forretningsforbindelse etableres, når der er tale om oprettelse af konto, depot eller lignende, der tillader transaktioner i værdipapirer for en kunde.

Hvis virksomheden har indført passende sikkerhedsforanstaltninger, der sikrer, at transaktionerne ikke gennemføres, før identitetsoplysningerne er indhentet og kontrolleret, kan virksomheden f.eks. oprette kontoen til transaktioner i værdipapirer.

18. Utilstrækkelige oplysninger eller oplysninger, der ikke kan ajourføres

Henvisning til hvidvaskloven: § 14, stk. 5 og 15. Henvisning til 4. hvidvaskdirektiv: Artikel 14, stk. 4.

Hvis virksomheden bliver bekendt med, at de indhentede oplysninger er utilstrækkelige og ikke kan ajourføres, skal virksomheden træffe passende foranstaltninger for at imødegå risikoen for hvidvask og finansiering af terrorisme, herunder skal virksomheden overveje, om forretningsforbindelsen skal afvikles.

Dette kan f.eks. være tilfældet, hvis virksomheden i sine løbende kundekendskabsprocedurer bliver bekendt med, at de indhentede oplysninger om en kunde ikke er tilstrækkelige, eller hvis virksomheden som led i sine kundekendskabsprocedurer vil ajourføre de indhentede oplysninger, og kunden ikke ønsker at udlevere dem, eller hvis virksomheden ikke kan få kontakt til kunden.

Med passende foranstaltninger forstås, at virksomheden konkret skal vurdere hvilke foranstaltninger, der skal iværksættes. Virksomheden bør altid forsøge at gennemføre kundekendskabsprocedurerne på en anden måde, hvis der ikke er en konkret risiko for hvidvask eller finansiering af terrorisme.

Passende foranstaltningerne kan f.eks. være, at virksomheden:

b) nægter at tilbyde kunden nye produkter,
c) intensiverer overvågningen af kunden,
d) sætter beløbsgrænser på kundens transaktioner eller
e) inddrager kundens engagement eller dele heraf, f.eks. nogle af kundens produkter.

De foranstaltninger, som virksomheden iværksætter, skal altid være passende i forhold til den konkrete risiko for hvidvask og finansiering af terrorisme i forhold til kundeforholdet.

Hvidvaskloven indeholder ikke regler for afvikling af et kundeforhold eller afslag på indgåelse af nye kundeforhold. I tilfælde hvor virksomheden vurderer, at kundekendskabsproceduren ikke konkret kan gennemføres på en anden måde, og at risikoen for hvidvask og finansiering af terrorisme er høj, kan virksomheden enten afbryde eller afvikle forretningsforbindelsen. Se afsnit 18.1 nedenfor om virksomheders pligt til at afbryde eller afvikle et kundeforhold.

18.1. Virksomhedens pligt til at afbryde eller afvikle et kundeforhold

Virksomheden har kun en forpligtelse til på hvidvaskområdet at afbryde eller afvikle en forretningsforbindelse, hvis virksomheden har udtømt alle muligheder for at gennemføre kundekendskabsprocedurer, og virksomheden på denne baggrund må konkludere, at det ikke er muligt at gennemføre kundekendskabsprocedurerne i forhold til den konkrete forretningsforbindelse.

Dette betyder, at virksomheden først skal forsøge at gennemføre kundekendskabsprocedurerne på en anden måde end den, der er virksomhedens normale procedure.

Det er f.eks. ikke tilstrækkelig årsag til afvikling af kundeforholdet, at kunden ikke ønsker at udlevere oplysninger, eller at kunden ikke er i besiddelse af den type identifikationsoplysninger, som virksomheden indsamler normalt i henhold til sine interne procedurer.

I sådanne tilfælde skal virksomheden vurdere, om årsagen til at kunden nægter at udleverer oplysningerne medfører en risiko for hvidvask og finansiering for terrorisme. Hvis dette ikke er tilfældet, skal virksomheden forsøge at indhente oplysninger på anden vis. Det kunne eksempelvis være en situation, hvor en kunde ikke har et offentligt udstedt legitimationsdokument. I dette tilfælde kan virksomheden i stedet bl.a. indhente kundens dåbsattest.

Hvidvasklovens pligt til at afbryde eller afvikle en forretningsforbindelse er derfor betinget af, at kundekendskabsprocedurerne ikke kan gennemføres, og at der vurderes at være en risiko for hvidvask og finansiering af terrorisme. Anvendelsesområdet for bestemmelsen er meget begrænset. Virksomheden vil i langt de fleste af sådanne tilfælde efterfølgende skulle foretage underretning til Hvidvasksekretariatet.

Hvis virksomheden vurderer, at en forretningsforbindelse skal afbrydes eller afvikles, må virksomheden ikke foretage yderligere transaktioner eller aktiviteter for kunden. Hvis der er tale om et fast lån, skal dette afvikles i forhold til den afviklingsprofil, der er er aftalt med kunden. Kreditrammen skal inddrages, eventuelt også i forhold til afviklingsaftalen.

Særligt i forhold til advokaters klientforhold

Ovenstående afsnit om muligheden for at afbryde eller afvikle et kundeforhold gælder ikke for advokater, når de fastslår en klients retsstilling eller forsvarer eller repræsenterer en klient under eller i forbindelse med en retssag, herunder rådgiver om indledning eller undgåelse af et sagsanlæg.

Undtagelsen gælder ikke i disse tilfælde, fordi klientens ret til advokatbistand og retssikkerhed vejer tungere end hensynet til et tilstrækkeligt kundekendskab.

Det er dog ikke formålet med denne bestemmelse at undtage advokater fra at gennemføre kundekendskabsprocedurer. Advokaten har samme pligt til at forsøge at gennemføre kundekendskabsprocedurerne på anden vis og derved også udtømme alle muligheder for dette.

19. Behandling af personoplysninger

Henvisning til hvidvaskloven: § 16.

Henvisning til 4. hvidvaskdirektiv: Artikel 43.
Henvisning til 5. hvidvaskdirektiv: Artikel 1, stk. 1, nr. 26.

Henvisning til anden lovgivning: Databeskyttelsesforordningens artikel 5, stk. 1, litra b 13 og 14.

Personoplysninger, der er indhentet med henblik på at opfylde kravene i hvidvaskloven, skal behandles i overensstemmelse med de databeskyttelsesretlige regler, der som udgangspunkt finder anvendelse ved behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling. Ved personoplysninger forstås enhver form for information om en identificeret eller identificerbar fysisk person.

Det betyder bl.a., at kravet i databeskyttelsesforordningens artikel 5, stk. 1, litra b, skal overholdes. De indsamlede oplysninger må således ikke viderebehandles på en måde, der er uforenelig med de udtrykkeligt angivne og legitime formål, hvortil oplysningerne er indsamlet.

Endvidere skal f.eks. reglerne i databeskyttelsesforordningens artikel 13 og 14 om oplysningspligt overholdes. Hvis der indsamles personoplysninger om en registreret person – eksempelvis en kunde – skal virksomheden bl.a. give den registrerede oplysninger om formålene med den behandling, som personoplysningerne skal bruges til, retsgrundlaget for behandlingen samt oplysninger om eventuelle modtagere eller kategorier af modtagere af personoplysningerne.

Hvis kunden er en fysisk person skal virksomheden, inden den etablerer en forretningsforbindelse eller gennemfører en enkeltstående transaktion, informere kunden om de regler, der gælder for behandling af personoplysninger med henblik på forebyggelse af hvidvask og finansiering af terrorisme. Kravet gælder ikke, når kunden er en juridisk person.

Alle personoplysninger, herunder f.eks. om kundens navn og cpr-nr. eller om kundens reelle ejere, som virksomheden indhenter i henhold til hvidvaskloven, må kun behandles af virksomheden i overensstemmelse med hvidvaskloven. Personoplysningerne må derfor ikke også benyttes i andre sammenhænge i virksomheden.

Virksomheden skal således oplyse den registrerede om, hvorfor virksomheden indhenter oplysninger om den pågældende, når virksomheden gennemfører kundekendskabsprocedurer.

Del 4 – Bistand fra tredjemand og outsourcing

20. Bistand fra tredjemand

Henvisning til hvidvaskloven: § 22 (også jf. § 9, stk. 2).

Henvisning til 4. hvidvaskdirektiv: Artikel 25-27.
Henvisning til 5. hvidvaskdirektiv: Artikel 1, stk. 1, nr. 14.

Henvisning til anden lovgivning: Databeskyttelsesforordningens artikel 28, stk. 3 og kapitel 5.

Virksomheder kan overlade indhentelse og kontrol af oplysninger i henhold til hvidvasklovens § 11, stk. 1, nr. 1-4, til en tredjemand. Se afsnit 23 om sondringen mellem §§ 22, 23 og 24. Muligheden for bistand fra tredjemand forudsætter, at visse betingelser er opfyldt, jf. nedenfor.

Virksomheden kan få bistand fra en tredjemand, hvis denne:

1) er omfattet er hvidvasklovens § 1, stk. 1, eller
2) er en virksomhed eller person, som svarer til de virksomheder eller personer, der er oplistet i § 1, stk. 1, som er etableret i et EU/EØS-land eller en tilsvarende virksomhed eller person i øvrige lande, der er underlagt krav om bekæmpelse af hvidvask og finansiering af terrorisme, der svarer til de krav, der følger af 4. hvidvaskdirektiv, og virksomheden/virksomheden er underlagt tilsyn af en myndighed, eller
3) er en medlemsorganisation eller sammenslutning af virksomheder og personer som nævnt i nr. 1 og 2, og er underlagt krav om bekæmpelse af hvidvask og finansiering af terrorisme, der svarer til de krav, der følger af 4. hvidvaskdirektiv, og medlemsorganisationen eller sammenslutningen er underlagt tilsyn af en myndighed.

Ad 1: Hvidvasklovens § 1, stk. 1:
En virksomhed kan få bistand fra en tredjemand, hvis denne tredjemand er omfattet af hvidvasklovens § 1, stk. 1. Det betyder, at alle de virksomheder og personer, der er omfattet af hvidvaskloven, kan indgå i en aftale om at yde bistand til § 11, stk. 1, nr. 1-4. Dette omfatter oplysninger, der ud fra en risikovurdering indhentes fra/om kunden for at gennemføre kundekendskabsprocedurerne.

Det betyder, at de oplysninger, som tredjemand har indhentet for at opfylde § 11, stk. 1, nr. 1-4, er omfattet af bestemmelsen om bistand fra tredjemand, og oplysningerne kan derfor benyttes af virksomheden.

Ad 2: Bistand fra en tredjemand etableret i EU/EØS:
Virksomheden kan også modtage bistand fra en tredjemand, hvis denne er etableret i et andet EU/EØS-land eller i øvrige lande, der er underlagt krav om bekæmpelse af hvidvask og finansiering af terrorisme. Det er dog på den betingelse, at tredjemanden er en virksomhed eller person, der svarer til de virksomheder og personer, der er omfattet af hvidvaskloven, og at virksomheden er underlagt krav om bekæmpelse af hvidvask og finansiering af terrorisme, der svarer til kravene i 4. hvidvaskdirektiv. Endvidere skal tredjemanden være underlagt et tilsyn med overholdelse af reglerne.

Er disse krav opfyldt, kan virksomheden benytte sig af de oplysninger, der er indhentet om en kundes identitet, på samme vis som hvis tredjemanden var etableret i Danmark. Virksomheden skal dog være opmærksom på, at virksomheden selv bærer ansvaret for at vurdere, hvorvidt tredjemanden er underlagt krav, der svarer til 4. hvidvaskdirektiv. Se afsnit 20.2 om ansvar. Derudover skal virksomheden kunne begrunde en sådan vurdering over for den tilsynsmyndighed, der fører tilsyn med virksomheden i Danmark, og virksomheden bør derfor også dokumentere tredjemandens vurdering.

Ad 3: Bistand fra en tredjemand, der er en medlemsorganisation/sammenslutning af virksomheder/personer:
Virksomheden kan også modtage bistand fra en tredjemand, som er en medlemsorganisation eller en sammenslutning af virksomheder eller personer af samme type, som de under nr. 1 og 2 nævnte. Virksomheden skal i tilfælde af, at virksomheden modtager bistand fra en sådan tredjemand, sikre, at denne er underlagt krav om bekæmpelse af hvidvask eller finansiering af terrorisme, der svarer til kravene i 4. hvidvaskdirektiv. Virksomheden skal sikre dette, inden virksomheden lægger oplysninger til grund, der er indhentet af medlemsorganisationen eller sammenslutningen.

Hvornår kan virksomheden få bistand fra en tredjemand?
Virksomheden kan få bistand fra tredjemand i de situationer, hvor kunden er kunde hos tredjemanden og også er/skal være kunde hos virksomheden, og hvor tredjemanden derfor allerede har foretaget kundekendskabsprocedurer i relation til kunden. Det betyder, at de oplysninger, som tredjemanden har indhentet om kunden, kan genbruges af virksomheden.

Det er ikke et krav, at tredjemanden er samme virksomhedstype som virksomheden selv. F.eks. kan et pengeinstitut lægge oplysninger om en kundes identitet til grund, som er indhentet af en revisor eller en udbyder af betalingstjenester. Det afgørende er, at denne tredjemand overholder hvidvaskloven, og at tredjemanden også har den pågældende fysiske eller juridiske person som kunde.

Virksomheden kan få bistand til at indhente oplysninger til de almindelige kundekendskabsprocedurer i § 11, stk. 1, nr. 1-4. Det betyder, at virksomheden ikke kan få bistand til at indhente yderligere oplysninger til at opfylde de skærpede kundekendskabsprocedurer, herunder §§ 17, 18 og 19. Virksomheden skal derfor selv, når en kunde efter virksomhedens vurdering udgør en høj risiko, indhente oplysninger, der supplerer de oplysninger, som tredjemanden har stillet til rådighed samt gennemføre andre relevante skærpede foranstaltninger.

I henhold til § 18 kan tredjemand dog godt oplyse virksomheden om, at en kunde er PEP eller er nærtstående eller nær samarbejdspartner til en PEP, hvorefter virksomheden selv skal gennemføre skærpede procedurer i overensstemmelse med § 18.

Det bemærkes, at hvis en virksomhed benytter kommercielle udbydere af PEP-lister, er det ikke bistand fra tredjemand i henhold til § 22. Se afsnit 15 om politisk eksponerede personer (PEP'er).

Virksomheden skal selv fortage risikovurderingen af kunden
Virksomheden skal selv foretage risikovurderingen af kunden, og derfor skal virksomheden være opmærksom på, at den samme kunde kan have forskellige risikoprofiler i forhold til tredjemanden og i forhold til virksomheden. Det kan være begrundet i forskelle i tredjemandens og virksomhedens forretningsmodel, geografiske placering mv.

Virksomheden kan derfor have behov for at indhente identitets- eller kontroloplysninger, der supplerer de oplysninger, som virksomheden modtager fra tredjemanden.

Virksomheden skal også være opmærksom på, at en tredjemands vurdering af, om der i forhold til kundens forretningsforbindelse til tredjemandens virksomhed er behov for at indhente oplysninger om kundens formål og tilsigtede beskaffenhed, ikke nødvendigvis er identisk med virksomhedens egen vurdering og forhold til kunden.

Forretningsforbindelsens formål og den tilsigtede beskaffenhed vurderes bl.a. ud fra den ydelse eller det produkt, som kunden ønsker. Vurderingen, af om der er behov for kendskab til kundens formål og den tilsigtede beskaffenhed, skal foretages konkret.

Det kan derfor være tilfældet, at virksomheden skal indhente oplysninger om formålet og den tilsigtede beskaffenhed selv, hvis tredjemanden ikke har indhentet sådanne oplysninger, eller indhente oplysninger, der supplerer de oplysninger, som virksomheden har modtaget fra tredjemanden.

20.1. Betingelser

Hvis virksomheden ønsker at lade en tredjemand indhente oplysninger om virksomhedens kunde/kunders identitet, skal virksomheden inden en aftale herom indgås:

- Indhente tilstrækkelige oplysninger om tredjemand,
- Sikre, at tredjemand forpligter sig til efter anmodning straks til virksomheden omfattet af loven at fremsende kopi af identitets- og kontroloplysninger om kunden/kunderne og eventuelle reelle ejere samt anden relevant dokumentation og data.

Ad: Indhente tilstrækkelige oplysninger om tredjemand:
Virksomheden skal indhente tilstrækkelige oplysninger til at afgøre, om tredjemanden opfylder kravene til kundekendskabsprocedurer og opbevaring af oplysninger. Det er virksomhedens ansvar at fastlægge, hvad der er tilstrækkeligt.

Ved tilstrækkelige oplysninger skal forstås, at virksomheden f.eks. indhenter en redegørelse fra tredjemand, hvori tredjemand beskriver de procedurer, som tredjemanden har indført med henblik på at opfylde kundekendskabsprocedurerne. Virksomheden kan f.eks. også indhente tredjemandens politikker og forretningsgange, der vedrører kundekendskab i henhold til § 11, stk. 1-4, og opbevaring af oplysninger i henhold til § 30.

Derudover vil det være relevant at indhente oplysninger om, hvorvidt tredjemand har modtaget påbud fra tilsynsmyndigheden i relation til kundekendskabskravene. Hvis dette er tilfældet, kan virksomheden undersøge, om påbuddet er opfyldt.

Det kan også være relevant, at virksomheden foretager stikprøver af tredjemandens forretningsforbindelser.

Ad: Sikre, at tredjemand forpligter sig til efter anmodning straks til virksomheden omfattet af loven at fremsende kopi af identitets- og kontroloplysninger om kunden/kunderne og eventuelle reelle ejere samt anden relevant dokumentation:

Denne betingelse er relevant, fordi virksomheden, som skal bruge oplysningerne inden oprettelsen af et kundeforhold, skal foretage en selvstændig risikovurdering af kunden. Risikovurderingen skal bl.a. tage de produkter eller ydelser, som kunden tilbydes, i betragtning.
Derudover skal tredjemanden forpligte sig til efter anmodning straks at fremsende relevante kontroldokumenter og anden relevant dokumentation og data til virksomheden eller personen omfattet af loven samt dokumentation for, at denne overholder kravene til opbevaring i 4. hvidvaskdirektiv.

Det betyder, at virksomheden skal have stillet de oplysninger, der er indhentet i henhold til § 11, stk. 1, nr. 1-4, til rådighed, når virksomheden skal foretage en risikovurdering af kunden. Det er dog ikke nødvendigt, at virksomheden også får stillet kontroldokumenterne til rådighed på dette tidspunkt, da disse til enhver tid skal kunne fremsendes af tredjemand efter anmodning fra virksomheden.

Behovet for, at de nævnte oplysninger straks skal stilles til rådighed, har baggrund i formålet med reglerne om kundekendskabsprocedurer. Kundekendskabsprocedurer skal hjælpe til at sikre en effektiv efterforskning bl.a. ved, at virksomheden eller personen hurtigt kan stille de nødvendige oplysninger om kundens eller dennes reelle ejeres identitet mv. til rådighed for efterforskningsmyndighederne.

Det er derfor nødvendigt, at tredjemands forpligtelser fremgår af den kontrakt, som virksomheden omfattet af loven indgår med tredjemand.

20.2. Ansvaret

Virksomheden, som benytter identitetsoplysninger, der er indhentet af tredjemand, er ansvarlig for sine egne forpligtelser til at overholde hvidvasklovens krav. Virksomheden kan ikke fritages for ansvar ved bistand fra tredjemand, og virksomheden bærer derfor selv ansvaret for, at der gennemføres kundekendskabsprocedurer, herunder at indhentelse af oplysninger om kunden gennemføres i overensstemmelse med hvidvaskloven.

Virksomheden er endvidere ansvarlig for, at der foretages en korrekt risikovurdering af virksomhedens kunder, herunder stillingtagen til, hvad risikovurderingen kræver i forhold til kundekendskab, overvågning af kunden mv. i overensstemmelse med hvidvaskloven.

Hvis en kunde eller kundegruppe risikovurderes til at være høj risiko, skal virksomheden sikre, at virksomheden gennemfører skærpede kundekendskabsprocedurer. Det vil som udgangspunkt medføre, at der er behov for at indhente tilstrækkelige supplerende oplysninger om den pågældende kunde eller kundegruppe.

Virksomhedens ansvar betyder derfor, at virksomheden skal sikre et tilstrækkeligt kendskab til tredjemanden, som betrygger virksomheden i, at tredjemandens opfyldelse af hvidvasklovens § 11, stk. 1, nr. 1-4, er effektiv. Det er således virksomheden, der over for tilsynsmyndigheden skal redegøre for kundekendskabets tilstrækkelighed.

Hvis virksomheden indgår en længerevarende aftale med en tredjemand om at bruge de oplysninger, som tredjemanden indhenter i henhold til § 11, stk. 1, nr. 1-4, bør virksomheden foretage løbende kontroller, som sikrer, at tredjemanden indhenter tilstrækkelige identitetsoplysninger om kunderne. Derudover skal virksomheden kontrollere, at oplysningerne er brugbare og praktisk let tilgængelige, og at virksomheden kan modtage kopi heraf efter anmodning fra virksomheden uden forsinkelser.

Virksomheden, som bistår som tredjemand, er fortsat ansvarlig for sin egen overholdelse af hvidvaskloven.

Endelig skal virksomheden være særlig opmærksom på, at de databeskyttelsesretlige regler skal overholdes i forbindelse med behandling af personoplysninger hos tredjemand. Hvis tredjemand er databehandler – hvorved forstås en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne – skal virksomheden således være opmærksom på de særlige krav, der indeholdt i de databeskyttelsesretlige regler.

Dette indebærer bl.a., at der skal indgås en databehandleraftale med databehandleren. Databehandleraftaler skal indgås mellem den dataansvarlige og databehandleren og skal leve op til kravene i databeskyttelsesforordningen.

Der henvises til Datatilsynets vejledninger om "Dataansvarlige og databehandlere" samt "Tilsynet med databehandlere og underdatabehandlere", der er tilgængelige på tilsynets hjemmeside (www.datatilsynet.dk).

20.3. Tredjemand etableret i land med høj risiko

Virksomheden kan ikke benytte muligheden for bistand fra en tredjemand, hvis tredjemanden er etableret i et land, som er opført på Europa-Kommissionens liste over højrisikotredjelande.

Dette gælder dog ikke, hvis tredjemanden er et majoritetsejet datterselskab eller en filial, der er etableret i et sådant højrisikotredjeland, men hvor den enhed, der har etableret datterselskabet/filialen, selv er etableret i et EU/EØS-land, og på betingelse af, at datterselskabet/filialen til fulde overholder koncernens politikker og forretningsgange. Se del 2 om risikovurdering og risikostyring.

Hvis virksomheden vil benytte et af virksomheden ejet datterselskab/en filial som bistand til opfyldelse af § 11, stk. 1, nr. 1-4, skal virksomheden foruden betingelserne beskrevet i afsnit 20.1 indhente oplysninger, der forsikrer virksomheden om, at datterselskabet/filialen til fulde overholder koncernens politikker og procedurer.

21. Koncernforhold

Henvisning til hvidvaskloven: § 23. Henvisning til 4. hvidvaskdirektiv: Artikel 28.

Virksomheder, der er del af en koncern, kan overlade det til en anden virksomhed i koncernen at opfylde kravene i § 11, stk. 1, nr. 1-4. Dette omfatter indhentelse af oplysninger fra/om kunden ud fra en risikovurdering for at gennemføre kundekendskabsprocedurerne. Begrebet koncern skal forstås i overensstemmelse med selskabslovens definition af koncern. Det er en forudsætning, at koncernen i overensstemmelse med 4. hvidvaskdirektiv:

1) anvender kundekendskabsprocedurer,
2) har regler om opbevaring af oplysninger og programmer til bekæmpelse af hvidvask og finansiering af terrorisme, og

3) at en myndighed fører tilsyn på koncernniveau med at kravene, der svarer til kravene i 4. hvidvaskdirektiv, overholdes.

Hvis en virksomhed i en koncern benytter en anden virksomhed i koncernen som tredjemand, skal koncernen overholde de ovenfor tre oplistede punkter, og derved anses virksomheden for at overholde de krav, der er til bistand fra tredjemand i hvidvaskloven. Ud over koncerner gælder samme muligheder internt i virksomheder bestående af hovedselskab og en eller flere filialer etableret i andre lande, sådan at en enhed udenfor Danmark står for opfyldelse.

Med programmer til bekæmpelse af hvidvask og finansiering af terrorisme forstås koncernens politikker og forretningsgange på hvidvaskområdet. Se afsnit 4 om politikker, forretningsgange og kontroller.

Kravet om, at der føres et tilsyn på koncernniveau skal forstås således, at en eller flere tilsynsmyndigheder fører tilsyn med, at kravene om kundekendskabsprocedurer, regler om opbevaring af oplysninger og programmer til bekæmpelse af hvidvask og finansiering af terrorisme overholdes. Herunder at tilsynsmyndigheden i moderselskabets hjemland fører tilsyn med, at koncernens politikker og forretningsgange effektiv overholder disse krav.

Bestemmelsen har til formål, at gentagne kundekendskabsprocedurer i en koncern ikke medfører unødige forsinkelser eller administrative omkostninger. Bestemmelsen om bistand fra en anden virksomhed indenfor en koncern betyder derfor, at betingelserne i nogen grad adskiller sig fra kravene i § 22. Se afsnit 20 om bistand fra tredjemand.

De oplysninger, som en anden virksomhed i koncernen har indhentet for at opfylde § 11, stk. 1, nr. 1-4, er omfattet af bestemmelsen, og oplysningerne kan derfor også benyttes til virksomhedens opfyldelse af kravene til kundekendskabsprocedure.

En anden virksomhed i koncernen kan efter denne bestemmelse bistå med at gennemføre skærpede kundekendskabsprocedurer efter §§ 17-19. Den anden virksomhed i koncernen kan også bistå med at foretage en risikovurdering af kunden. Det er dog vigtigt at bemærke, at risikovurderingen altid skal foretages i forhold til den konkrete kunde, herunder med inddragelse af risikofaktorer som bl.a. produktet eller tjenesteydelsen, som kunden tilbydes, geografiske forhold, omfang og varighed af forretningsforbindelsen med kunden mv. Se afsnit 13 om risikovurdering – kundekendskabsprocedurer.

Den virksomhed, som bistår med gennemførelse af kundekendskabsprocedurerne er en del af koncernen, og da virksomheden, der benytter sig af bistand fra koncernvirksomheden, har sikret, at koncernen opfylder de tre betingelser oplistet i dette afsnit, er der ikke et krav om, at virksomheden indhenter yderligere oplysninger om koncernvirksomheden.

22. Outsourcing

Henvisning til hvidvaskloven: § 24.

Henvisning til 4. hvidvaskdirektiv: Artikel 29.

Henvisning til anden lovgivning: Bekendtgørelse nr. 877 af 12. juni 2020 om outsourcing for kreditinstitutter m.v.

Henvisning til anden lovgivning: Databeskyttelsesforordningens artikel 28, stk. 3, og kapitel 5.

En virksomhed kan vælge kontraktmæssigt at outsource opgaver til en anden virksomhed, i det følgende kaldet leverandøren, med henblik på at overholde kravene i hvidvaskloven. Se afsnit 23 om forskellene mellem §§ 22, 23 og 24.

Det kan f.eks. være opgaver som:

1) Indhentelse af identitets- og kontroloplysninger til brug for virksomhedens kundekendskabsprocedurer.
2) Overvågning af kundetransaktioner.
3) Opbevaring af oplysninger mv.
4) Underretninger.

Leverandøren behøver ikke være omfattet af hvidvaskloven.

Alle opgaver, der følger af hvidvaskloven, kan som udgangspunkt outsources. Virksomheden kan dog aldrig outsource det ansvar, som følger af hvidvaskloven. Se afsnit 20.2 om ansvar. Virksomheden skal være opmærksom på, at opgaven i hvidvasklovens § 7, stk. 2, ikke kan outsources, dvs. at virksomhedens forpligtelse til at udpege en hvidvaskansvarlig kun kan opfyldes af virksomheden selv. Ligeledes kan den hvidvaskansvarliges ansvar heller ikke outsources. Se afsnit 6.1 om den hvidvaskansvarlige.

Virksomheder, der er underlagt outsourcingbekendtgørelsen, skal være opmærksom på, at bekendtgørelsen i nogle tilfælde kan stille højere krav end kravene i hvidvaskloven, som virksomheden skal opfylde. Virksomheder, der er underlagt outsourcingbekendtgørelsen, skal vurdere, om aktiviteten er omfattet af bekendtgørelsen.

22.1. Betingelser

Muligheden for, at en virksomhed kan outsource opgaver med henblik på at opfylde kravene i hvidvaskloven, er betinget af nogle krav, som skal være opfyldt, før en kontrakt indgås med en leverandør.

Inden virksomheden indgår en aftale om outsourcing med leverandøren, skal virksomheden være sikker på:

1) at leverandøren har fornøden evne og kapacitet til at varetage opgaven på tilfredsstillende vis
2) at leverandøren har den eller de nødvendige tilladelser.

Det betyder, at leverandøren skal have relevant og fagligt kendskab til at løse opgaven og have tilstrækkelige ressourcer til at løse opgaven.

Hvis leverandøren ikke er etableret i Danmark, skal virksomheden særligt have fokus på at sikre, at leverandøren har de fornødne tilladelser, der kræves for virksomhed af den pågældende art. Derudover er det relevant at være betrygget i, at leverandøren har det fornødne kendskab til den nationale lovgivning, så leverandøren kan leve op til betingelserne på samme vis som en leverandør, der er etableret i Danmark.

22.2. Hvem kan en virksomhed outsource til i henhold til hvidvaskloven?

Der stilles ikke krav i hvidvaskloven til, hvem en virksomhed outsourcer opgaver til. Det betyder, at der ikke er et krav om, at leverandøren er omfattet af hvidvaskloven.

Leverandøren er derfor ikke en afgrænset kreds af personer og virksomheder, som det gælder i hvidvasklovens §§ 22 og 23.

En leverandør kan f.eks. være en forhandler af varer, hvor kunden/køberen tilbydes finansiering hos virksomheden. Her kan virksomheden f.eks. indgå en aftale med forhandleren om, at denne i forbindelse med salget indhenter oplysninger om kundens identitetsoplysninger og kontrolkilder, som virksomheden skal bruge i sin risikovurdering af kunden.

22.3. Kontrol af leverandøren

Når virksomheden har indgået en aftale med en leverandør om outsourcing af opgaver, skal virksomheden løbende føre kontrol med leverandøren.

Det er derfor vigtigt, at virksomheden, inden aftalen bliver indgået, sikrer, at det er muligt for virksomheden løbende at gennemføre de relevante kontroller.

Kontrollen skal sikre:

1) at leverandøren lever op til de forpligtelser, som følger af aftalen med virksomheden og
2) at aftalen om outsourcing med leverandøren fortsat er forsvarlig.

Når virksomheden skal vurdere, om aftalen om outsourcing fortsat er forsvarlig, skal virksomheden vurdere dette ud fra de forpligtelser, som påhviler virksomheden. Dvs. at virksomheden skal være sikker på, at virksomheden ved brug af leverandøren til fulde lever op til hvidvasklovens krav på samme måde, som hvis virksomheden selv varetog opgaverne i overensstemmelse med hvidvaskloven.

22.4. Ansvar

Virksomheden kan aldrig outsource sit ansvar. Det betyder, at virksomheden altid bærer det fulde ansvar for at de forpligtelser, som virksomheden har i henhold til hvidvaskloven og anden relevant lovgivning på området, vil virksomheden altid bærer det fulde ansvar for at overholde.

Med anden relevant lovgivning menes bl.a. EU's forordninger på hvidvaskområdet, databeskyttelseslovgivningen mv.

Når en virksomhed vælger at outsource en opgave med henblik på overholdelse af hvidvaskloven, vil leverandøren blive betragtet som en del af virksomheden. Ansvaret, for at opgaven varetages i overensstemmelse med kravene i hvidvaskloven, påhviler virksomheden.

Virksomheden er derfor også ansvarlig for, at leverandøren følger fornødne procedurer til bekæmpelse af hvidvask og finansiering af terrorisme i sin udførelse af opgaven for virksomheden.

Virksomheden skal ved outsourcing være opmærksom på, om outsourcing har en betydning for virksomhedens risici, og hermed den residuale risiko virksomheden har efter at have fastlagt sine politikker på hvidvaskområdet. F.eks. kan det have betydning for risikoprofilen, hvis virksomheden eksempelvis outsourcer en opgave til en virksomhed etableret uden for Danmark, som har et lavere niveau i deres regulering end Danmark, og hvor der ikke er et tilstrækkeligt tilsyn med bekæmpelse af hvidvask og finansiering af terrorisme, eller omvendt hvis virksomheden eksempelvis outsourcer en opgave til en virksomhed, som er specialiseret i at løse den pågældende opgaver, og som derfor kan løse opgaven mere effektivt end virksomheden selv.

Endelig skal virksomheden være særlig opmærksom på, at de databeskyttelsesretlige regler skal overholdes i forbindelse med behandling af personoplysninger hos tredjemand. Hvis tredjemand er databehandler – hvorved forstås en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne – skal virksomheden således være opmærksom på de særlige krav, der indeholdt i de databeskyttelsesretlige regler.

Dette indebærer bl.a., at der skal indgås en databehandleraftale med databehandleren. Databehandleraftaler skal indgås mellem den dataansvarlige og databehandleren og skal leve op til kravene i databeskyttelsesforordningen.

Der henvises til Datatilsynets vejledninger om "Dataansvarlige og databehandlere" samt "Tilsynet med databehandlere og underdatabehandlere", der er tilgængelige på tilsynets hjemmeside (www.datatilsynet.dk).

23. Oversigt af mulighed for bistand fra tredjemand, anden virksomhed og ved outsourcing

Nedenfor følger et skema, som sammenligner mulighed for bistand fra tredjemand til de almindelige kundekendskabsprocedurer og outsourcing til en anden virksomhed (leverandør) til udførelse af opgaver på baggrund af krav i hvidvaskloven.

	§ 22: Bistand fra tredjemand til kundekendskabsprocedurer.	**§ 23:** Bistand fra en anden virksomhed i koncernen til kundekendskabsprocedurer.	**§ 24:** Outsourcing af opgaver til opfyldelse af hvidvaskloven.
Hvornår er muligheden relevant?	Når virksomheden og tredjemand har samme kunde(r), og identitets- og kontroloplysninger mv. kan genbruges.	Når to/flere virksomheder i samme koncern har samme kunde(r), og identitets- og kontroloplysninger mv. kan genbruges.	Når virksomheden ser fordel i, at en anden virksomhed varetager bestemte opgaver.

Indhold	Virksomheden kan overlade det til en anden virksomhed (tredjemand) at indhente og kontrollere oplysninger efter § 11, stk. 1. nr. 1-4. Virksomheden skal selv foretage en risikovurdering af kunden og f.eks. gennemføre skærpede kundekendskabsprocedurer, hvis det er nødvendigt.	Virksomheden kan overlade det til en anden virksomhed i koncernen at indhente og kontrollere oplysninger efter § 11, stk. 1. nr. 1-4. Den anden virksomhed i koncernen kan også bistå med en risikovurdering af kunden og eventuelt med at gennemføre skærpede kundekendskabsprocedurer.	Virksomheden kan outsource opgaver til en anden virksomhed (leverandør) med henblik på overholdelse af hvidvaskloven.
Formål	Virksomheden kan genbruge oplysninger indhentet til brug for kundekendskabsprocedurer.	Kundekendskabsprocedurer skal ikke unødvendigt foretages dobbelt inden for en koncern.	Virksomheden kan optimere sin drift ved at outsource relevante opgaver.
Til hvem og hvornår	Tredjemanden skal være en virksomhed eller person, der er omfattet af hvidvasklovens § 1, stk. 1 eller en tilsvarende virksomhed/person i et andet land, der er underlagt tilsvarende krav om bekæmpelse af hvidvask og finansiering af terrorisme.	Tredjemanden skal være en virksomhed i koncernen, som har indhentet oplysningerne, og som følger koncernens forretningsgange og poltikker.	Der er ikke krav til, hvilken virksomhed eller person, som leverandøren er.
Forpligtelser	Virksomheden skal indhente tilstrækkelige oplysninger om tredjemand og sikre, at tredjemand kan stille identitets- og kontroloplysninger til rådighed.	Virksomheden skal sikre, at koncernen bruger kundekendskabsprocedurer, har regler om opbevaring og programmer til bekæmpelse af hvidvask og finansiering af terrorisme og er underlagt tilsyn på området.	Virksomheden skal kontrollere leverandøren. Virksomheden skal sikre, at leverandøren har evne, kapacitet, tilladelse og kendskab både fagligt til opgaven og til lovgivningen.
Ansvar	Virksomheden bærer ansvaret.	Virksomheden bærer ansvaret.	Virksomheden bærer ansvaret.

Del 5 – Undersøgelses-, noterings-, underretnings- og opbevaringspligt

24. Undersøgelsespligt

Henvisning til hvidvaskloven: § 25, stk. 1 og 2. Henvisning til 4. hvidvaskdirektiv: Artikel 18, stk. 2. Henvisning til 5. hvidvaskdirektiv: Artikel 1, stk. 10, litra b.

Hvidvasklovens § 25, stk. 1, omhandler virksomheders pligt til at undersøge baggrunden for og formålet med transaktioner, transaktionsmønstre og aktiviteter, hvor der kan være mistanke om eller rimelig grund til at formode, at disse har eller har haft tilknytning til hvidvask eller finansiering af terrorisme.

Formålet med undersøgelsen er at fastslå, om der er mistanke om eller rimelig grund til at formode, at en transaktion eller aktivitet har eller har haft tilknytning til hvidvask eller finansiering af terrorisme. Dette betyder, at virksomheder skal have forretningsgange og systemer på plads, der gør det muligt at identificere sådanne transaktioner og aktiviteter.

Virksomheder skal således undersøge baggrunden for og formålet med alle transaktioner, transaktionsmønstre og usædvanlige aktiviteter, der er komplekse, usædvanlige store, foretages i et usædvanligt mønster eller ikke har et åbenbart økonomisk eller lovligt formål.

Kriteriet: "er komplekse"
Virksomheden kan i vurderingen af, om transaktionen er kompleks, f.eks. lægge vægt på, om transaktionen involverer flere parter eller flere jurisdiktioner, eller om transaktionen giver kunden mulighed for at modtage betalinger fra en ukendt tredjemand.

Kriteriet: "er usædvanligt store"
Virksomheden kan vurdere, om en transaktion er usædvanligt stor ud fra f.eks. kendskabet til den konkrete kunde, herunder kundens transaktionsmønstre og produktportefølje.

Kriteriet: "foretages i et usædvanligt mønster"
Virksomheden kan tage udgangspunkt i kundens og kundetypens sædvanlige adfærdsmønstre i vurderingen af, om en transaktion foretages i et usædvanlige mønster. Her kan bl.a. lægges vægt på størrelsen af kundens sædvanlige transaktioner, hvor store de modtagne midler er mv.

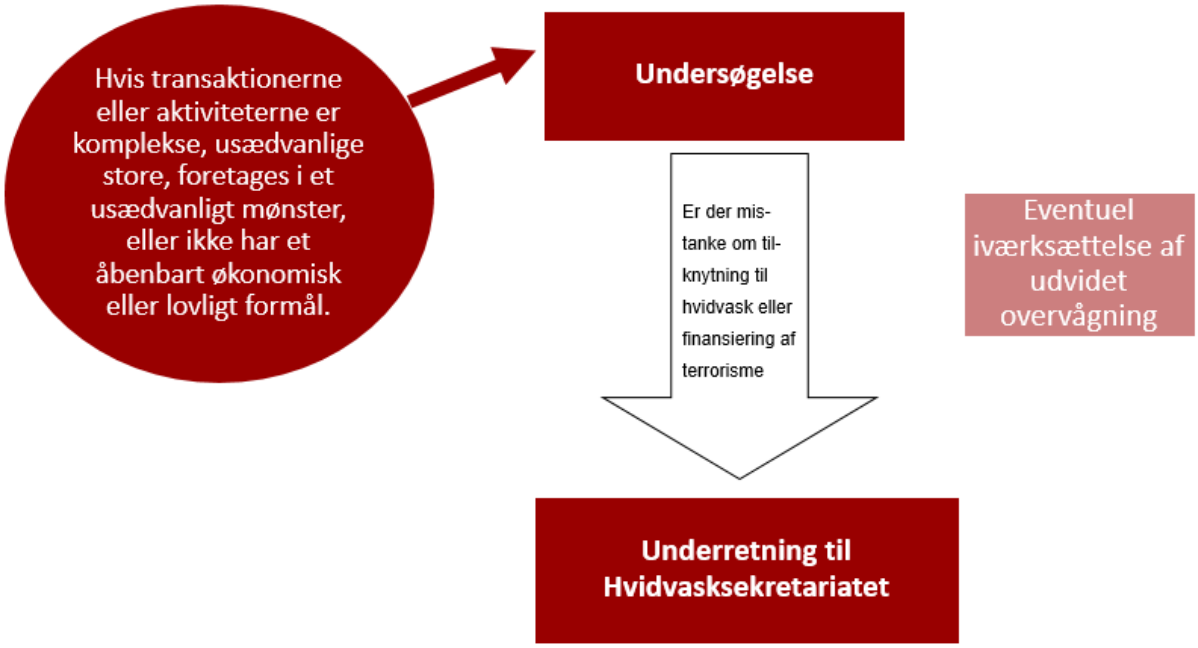
Kriteriet: "ikke har et åbenbart økonomisk eller lovligt formål"
Har transaktionen eller aktiviteten ikke et klart økonomisk eller lovligt formål, skal virksomheden undersøge baggrunden herfor. Virksomheder kan eksempelvis lægge vægt på, hvem kunden sædvanligvis modtager midler fra, hvem kunden overfører penge til og kundens transaktionsmønster. Videreformidler eller modtager kunder midler, hvor det ikke er klart, hvad det økonomiske formål er hermed, kan dette resultere i en undersøgelse af hvor midlerne skal hen eller stammer fra.

Et eksempel herpå kan være en kunde, som normalt kun modtager midler fra sin arbejdsgiver, men som pludselig modtager midler fra en ukendt tredjemand, og hvor det ikke er klart, at der er tale om løn eller lignende midler.

Ligeledes kan et eksempel være, at en kunde pludseligt begynder at foretage en række investeringer, der klart afviger fra kundens hidtidige investeringsmønster, f.eks. fordi investeringerne er meget større i mængde eller beløb end de investeringer, som kunden normalt foretager. En kundes manglende villighed til at give oplysninger eller en forklaring på f.eks. en stigende mængde investeringer eller et ændret investeringsmønster kan også indgå i vurderingen af, om der er tale om usædvanlige aktiviteter.

Virksomheden skal have procedurer og systemer, der gør det muligt at identificere de ovenstående transaktioner og aktiviteter.
Hvis det på baggrund af kundens adfærd står virksomheden klart, at der er tale om hvidvask eller finansiering af terrorisme, kan der ske underretning direkte uden, at virksomheden foretager en egentlig undersøgelse.

Nedenstående figur illustrerer processen fra undersøgelsespligten til underretningspligten samt eventuel iværksættelse af en udvidet overvågning af kunden.



Virksomheden skal ved vurderingen af den usædvanlige adfærd tage udgangspunkt i de oplysninger, den har om kunden, herunder eventuelle oplysninger om forretningsforbindelsens formål og tilsigtede beskaffenhed. Heri kan oplysninger om omfang og forventet grænseoverskridende aktivitet også blive inddraget. Disse oplysninger skal virksomheden sammenholde med det, der virker mistænkeligt. I pengeinstitutter og andre virksomheder med kundeansvarlige, kan det være relevant at inddrage den kundeansvarlige i forhold til viden om kunden.

Virksomheden kan også inddrage oplysninger fra offentligt tilgængelige kilder, f.eks. via internetsøgninger, hvis virksomheden vurderer, at der er tale om en pålidelig og uafhængig kilde.

Det kan være nødvendigt, at virksomheden kontakter kunden for at indhente yderligere oplysninger om formålet med transaktionen eller aktiviteten. Kundens verbale forklaring kan dog i mange tilfælde ikke være tilstrækkelig til at afkræfte en mistanke. Det kan derfor være nødvendigt at bede kunden om at underbygge sin forklaring, f.eks. med dokumentation i form af:

1) En salgsaftale ved bilsalg.
2) En skifteretsattest eller boopgørelse ved arv.
3) En købsaftale ved ejendomssalg.
4) En salgsaftale ved virksomhedssalg.
5) En årsopgørelse ved opsparing/formue.
6) En eller flere lønsedler ved indkomst fra ansættelsesforhold.

Virksomhedens undersøgelse kan med fordel bygges op omkring fastlæggelse af følgende:

1) **Hvem** er kunden?
2) **Hvordan** fremstår kunden?
3) **Hvad** ønsker kunden udført?
4) **Hvor** foregår transaktionen/aktiviteten?
5) **Hvornår** skal virksomheden udføre transaktioner eller aktiviteter for kunden?
6) **Hvordan** skal transaktionen/aktiviteten udføres?
7) **Hvorfor** gør kunden, som han/hun gør?

Hvis virksomheden vurderer, at en forespørgsel vil give kunden viden om, at virksomheden har mistanke og er i gang med at foretage en undersøgelse, eller hvis virksomheden finder det uhensigtsmæssigt at kontakte kunden om sagen, skal virksomheden foretage en underretning til Hvidvasksekretariatet. Hvis virksomheden ikke kan afkræfte mistanken helt, skal der også ske underretning. Virksomheden skal være opmærksom på, at det ligger i kravet, at mistanken skal afkræftes helt, hvis der ikke skal ske underretning. Det er således ikke tilstrækkeligt, at mistanken kun er blevet svækket. Se afsnit 25 om underretningspligten til Hvidvasksekretariatet.

Kravet om undersøgelsespligt skal ses i sammenhæng med underretningspligten til Hvidvasksekretariatet. Virksomheden skal basere sin underretning til Hvidvasksekretariatet på vurderinger i den konkrete situation i forhold til:

1) handlingernes karakter og afvigelse fra normale kundehandlinger
2) fortielser og andre særegne og atypiske forhold hos kunden.

Hvis virksomhedens undersøgelse, herunder virksomhedens spørgsmål om formål mv., giver kunden anledning til at afstå fra transaktionen eller aktiviteten, er mistanken ikke blevet afkræftet. Derimod kan dette underbygge mistanken, og virksomheden bør dermed foretage en underretning til Hvidvasksekretariatet.

24.1. Udvidet overvågning

Virksomheden skal, hvor det er relevant udvide overvågningen af forretningsforbindelsen, hvis der er mistanke om eller rimelig grund til at formode, at en kundes transaktioner eller aktiviteter har eller har haft tilknytning til hvidvask eller finansiering af terrorisme.

Virksomheden skal således, hvor det er relevant, udvide overvågningen af kunden for at afgøre, om transaktionerne eller aktiviteterne virker mistænkelige. Det betyder, at virksomheden på baggrund af risikoen skal vurdere, om der er behov for at iværksætte en skærpet overvågning af kunden. Det vil bl.a. gøre sig gældende, hvor der er givet underretning til Hvidvasksekretariatet.

En udvidelse af overvågningen af en kunde kan f.eks. være:

1) At virksomheden justerer den automatiserede overvågning af kunden, således at tærskelværdierne for, hvornår en alarm bliver udløst i virksomhedens overvågningssystem, bliver sat lavere.
2) At virksomheden har en skærpet opmærksomhed på kundens adfærd, herunder forespørgsler, aktiviteter mv. Det kan f.eks. være et notat på kundens profil hos virksomheden, der skærper medarbejdernes opmærksomhed på en bestemt type adfærd hos kunden.
3) At virksomheden manuelt gennemgår kundens relevante transaktioner med jævne mellemrum.

I nogle specifikke kundeforhold kan den løbende overvågning ske som led i den ydelse, der udbydes, hvis selve ydelsen medfører en indsigt i kundens forhold. Dette gør sig eksempelvis gældende for en godkendt revisors afgivelse af erklæringer, hvor bl.a. kundens økonomiske forhold gennemgås. Oplysninger, som indhentes i forbindelse med udførelse af sådanne opgaver, vil kunne indgå i virksomhedens opfyldelse af hvidvasklovens krav om løbende overvågning. Virksomheden skal i sådanne tilfælde notere og opbevare materiale, dokumentation mv., i overensstemmelse med hvidvasklovens krav herom.

Virksomheden skal samtidig være opmærksom på, at virksomheden skal gennemføre kundekendskabsprocedurer, når en kundes relevante omstændigheder ændrer sig, se afsnit 8.2.

24.2. Noteringspligten

Henvisning til hvidvaskloven: § 25, stk. 3.

Henvisning til 4. hvidvaskdirektiv: Artikel 40.
Henvisning til 5. hvidvaskdirektiv: Artikel 1, stk. 1, nr. 25.

Virksomheden skal notere og opbevare resultaterne af de undersøgelser, der foretages i forbindelse med forretningsforbindelsen eller den enkeltstående transaktion samt eventuelle oplysninger, som modtages fra kunden. Se afsnit 26 om opbevaringspligten.

Noteringspligten omfatter faktuelle oplysninger om kunden og transaktionen samt en konklusion på virksomhedens undersøgelse. Notatet skal være tilstrækkeligt til at genopfriske hukommelsen og give andre, herunder andre medarbejdere og politiet, en forståelse af sagen. Det er således ikke tilstrækkeligt i forbindelse med en undersøgelse af en transaktion eller aktivitet at notere et enkelt ord, som f.eks. ”rejse” eller ”kasino”.

De noterede oplysninger kan f.eks. være:

1) Kundens forklaring om formålet med transaktionen eller aktiviteten.
2) Dokumentation for kundens forklaring.
3) Forklaring fra andre relevante medarbejdere i virksomheden, eksempelvis den kundeansvarlige.

Forpligtelsen til at notere resultaterne af undersøgelser gælder både undersøgelser, hvor virksomheden underretter Hvidvasksekretariatet, og undersøgelser, hvor virksomheden har afkræftet mistanken helt og derfor ikke foretaget underretning.

24.3. Begrænsning i retten til indsigt

Henvisning til hvidvaskloven: § 25, stk. 4. Henvisning til 4. hvidvaskdirektiv: Artikel 40.

I forhold til undersøgelser har den registrerede person ikke ret til indsigt i personoplysninger, der er eller vil blive behandlet i forbindelse med en undersøgelse ved mistanke om hvidvask og finansiering af terrorisme. Det vil sige, at personens indsigtsret i virksomhedens undersøgelser efter hvidvaskloven er afskåret i både igangværende og allerede foretagne undersøgelser. Se afsnit 31 om tavshedspligt.

25. Underretningspligt

Henvisning til hvidvaskloven: § 26, stk. 1 og 5. Henvisning til 4. hvidvaskdirektiv: Artikel 33.

Der skal ske underretning til Hvidvasksekretariatet[10], hvis virksomheden er vidende om, har mistanke om eller rimelig grund til at formode, at en transaktion, midler eller aktivitet har eller har haft tilknytning til hvidvask eller finansiering af terrorisme. Dette gælder også virksomheder omfattet af hvidvasklovens § 1, nr. 9, om udenlandske virksomheders filialer mv. Eksempelvis skal en underretning vedrørende en kunde i en filial i Danmark af en udenlandsk virksomhed indgives til Hvidvasksekretariatet.

Hvidvasksekretariatet skal underrettes omgående. Virksomheden skal således tilrettelægge behandlingen af mistænkelige transaktioner og aktiviteter sådan, at processen fremskyndes mest muligt. Med processen forstås stadiet fra overvågning af kundetransaktioner og konstatering af noget mistænkeligt til undersøgelse og afklaring af, om mistanken kan anses for afkræftet.

Underretningspligten gælder også i forbindelse med *forsøg* på at foretage en transaktion eller ved en henvendelse fra en potentiel kunde med ønske om gennemførelse af en transaktion eller aktivitet. Der skal således også gives underretning om kundeforhold, der bliver afvist, hvis virksomheden vurderer, at der er tale om forsøg på hvidvask eller finansiering af terrorisme.

Hvor der er tale om en ny potentiel kunde, skal virksomheden ikke gennemføre kundekendskabsprocedurerne, hvis der er fare for, at kunden bliver bekendt med, at der bliver foretaget en underretning til Hvidvasksekretariatet. Det kan dog alligevel være muligt at identificere den pågældende på andet

[10] Hvidvasksekretariatet er en operationel uafhængig og selvstændig enhed, som organisatorisk er placeret hos Statsadvokaten for Særlig Økonomisk og International Kriminalitet. Hvidvasksekretariatet har bl.a. til opgave at modtage og analysere underretninger om mistænkelige transaktioner og andre oplysninger af relevans for hvidvask af penge, tilknyttede underliggende forbrydelser eller finansiering af terrorisme.

grundlag i nogle tilfælde, f.eks. på baggrund af oplysninger eller dokumenter, der er modtaget fra den potentielle kunde.

Det er ikke hensigten, at den underretningspligtige skal gå ind i en nærmere strafferetlig vurdering af forholdet. De af loven omfattede virksomheder og personer skal derimod se på, om der er forhold, der er atypiske i forhold til normale kundeforhold, herunder om transaktionen vedrører beløbsstørrelser eller betalingsmåder, der i den konkrete sammenhæng forekommer atypiske.

Der kan opstå situationer, hvor der ikke i forbindelse med den konkrete transaktion eller aktivitet forekommer noget atypisk, men hvor virksomheden er i besiddelse af andre oplysninger, der alligevel giver anledning til mistanke.

En underretning er ikke en anmeldelse, og underretningspligten kan ikke opfyldes ved, at virksomheden sender en underretning til politiet. Hvis der er tale om egentlig anmeldelse af et strafbart forhold, kan der derimod ske anmeldelse til den relevante politikreds.

Virksomheden har tavshedspligt om, at der er givet underretning, eller at dette overvejes. Det betyder, at den registrerede person ikke har ret til indsigt i, at der er sket underretning til Hvidvasksekretariatet vedrørende den pågældende person. Se afsnit 31 om tavshedspligt.

Hvidvaskloven går forud for revisorlovens § 22, stk. 1.
For godkendte revisorer, finder reglerne i revisorlovens § 22, stk. 1, ikke anvendelse på forhold, der er omfattet af hvidvaskloven.

Det bemærkes, at hvidvasklovens regler om tavshedspligt medfører, at revisorer i disse tilfælde ikke må underrette ledelsen eller indføre underretningen i revisionsprotokollen, som foreskrevet i revisorlovens § 22, stk. 1, 1. og 2. pkt.

25.1. Overtrædelse af kontantforbuddet

Hvis en virksomheds kunde overtræder kontantforbuddet, vil det som udgangspunkt være en usædvanlig eller mistænkelig aktivitet. Virksomheden skal derfor i sådanne tilfælde foretage en undersøgelse af aktiviteten for at vurdere, om virksomheden skal underrette Hvidvasksekretariatet. Hvis virksomheden ikke kan afkræfte, at der er tale om hvidvask eller finansiering af terrorisme, skal der ske underretning. Se afsnit 2.3 om kontantforbuddet.

25.2. Begrænsning i retten til indsigt

I forhold til underretninger har den registrerede person ikke ret til indsigt i personoplysninger, der er eller vil blive behandlet i forbindelse med en underretning til Hvidvasksekretariatet ved mistanke om hvidvask eller finansiering af terrorisme. Det vil sige, at personens indsigtsret i virksomhedens underretninger efter hvidvaskloven er afskåret med hensyn til oplysninger om, at der er givet underretning eller at dette overvejes. Se afsnit 31 om tavshedspligt.

25.3. Undtagelse til underretningspligten

Henvisning til hvidvaskloven: § 27, stk. 2-4. Henvisning til 4. hvidvaskdirektiv: Artikel 33.

Visse virksomheder, herunder revisorer, er i særlige tilfælde undtaget fra underretningspligten.

Undtagelsen gælder ikke, hvis virksomheden ved eller burde vide, at kunden søger bistand med henblik på hvidvask eller finansiering af terrorisme.

Godkendte revisorer
Revisionsvirksomheder og revisorer, som er godkendt i henhold til revisorlovgivningen, er undtaget fra underretningspligten i forhold til oplysninger, som de modtager fra eller indhenter om en kunde (klient), når de repræsenterer kunden i Landsskatteretten.

Undtagelsen gælder, uanset om oplysningerne fra kunden modtages før, under eller efter sagen.

Bistand til advokater
Virksomheder som nævnt i hvidvasklovens § 1, stk. 1, nr. 14-17, herunder bl.a. godkendte revisorer, skatterådgivere og bogholdere, er undtaget fra pligten til at underrette i samme omfang som advokater, når de bistår en advokat før, under og efter en retssag, eller bistår advokater med at fastslå advokatens klients retsstilling.

25.4. Virksomhedens pligt til at undlade at gennemføre transaktioner

Henvisning til hvidvaskloven: § 26, stk. 3 og 4. Henvisning til 4. hvidvaskdirektiv: Artikel 35.

Mistanke om hvidvask
Indtil der er sket underretning, skal virksomheden undlade at gennemføre transaktioner, hvis de har viden, mistanke om eller rimelig grund til at formode, at en transaktion eller aktivitet har tilknytning til hvidvask. Kravet gælder kun, hvis transaktionen ikke allerede er gennemført, f.eks. ved straksoverførsler, hvor transaktionen ofte vil være gennemført, inden virksomheden får viden eller mistanke om, at transaktionen har tilknytning til hvidvask.

Figuren nedenfor illustrerer processen i forbindelse med undladelse af at gennemføre transaktioner i tilfælde, hvor der er mistanke om hvidvask.

Hvis gennemførelse af transaktionen ikke kan undlades, eller hvis virksomheden vurderer, at det vil skade efterforskningen at undlade at gennemføre transaktionen, skal virksomheden i stedet indgive underretningen omgående efter gennemførelsen.

Mistanke om finansiering af terrorisme
Hvis virksomheden har viden, mistanke om eller rimelig grund til at formode, at en transaktion vedrører finansiering af terrorisme, skal virksomheden undlade at gennemføre transaktionen, indtil virksomheden har indhentet godkendelse fra Hvidvasksekretariatet.

Hvidvasksekretariatet vil hurtigst muligt beslutte, om transaktionen kan gennemføres.

Figuren nedenfor illustrerer processen i forbindelse med undladelse af at gennemføre transaktioner i tilfælde, hvor der er mistanke om finansiering af terrorisme.

25.5. Formkrav til underretning til Hvidvasksekretariatet

Henvisning til hvidvaskloven: § 26, stk. 6.

Henvisning til anden lovgivning: Bekendtgørelse nr. 1403 af 1. december 2017 om indsendelse af underretninger m.v. til Statsadvokaten for Særlig Økonomisk og International Kriminalitet.

Virksomheder skal foretage underretning om mistanke om hvidvask eller finansiering af terrorisme til Hvidvasksekretariatet digitalt.

Underretning skal som udgangspunkt ske på dansk. Hvis dette ikke er muligt, kan underretningen ske på engelsk.

Underretning skal foretages i XML-format via www.hvidvask.dk. Virksomheden skal inden udløbet af den efterfølgende bankdag kontrollere, om underretningen er accepteret eller afvist.

Ved IT-problemer, som nedbrud eller midlertidig kapacitetsnedgang, hvor hjemmesiden www.hvidvask.dk er utilgængelig 8 timer i træk i tidsrummet mellem kl. 8 og 16 på hverdage, skal underretning ske i XML-format ved e-mail eller andet elektronisk medie efter aftale med Hvidvasksekretariatet. Dette gælder dog ikke planlagte nedlukninger med henblik på opdatering, som har været annonceret forinden på hjemmesiden, og hvor annonceringens anvisninger bliver fulgt.

For nærmere information om underretningen, herunder kravene til XML-format, se Hvidvasksekretariatets brugervejledninger på www.hvidvask.dk[11].

26. Opbevaringspligten

Henvisning til hvidvaskloven: § 30. Henvisning til 4. hvidvaskdirektiv: Artikel 40-43. Henvisning til 5. hvidvaskdirektiv: Artikel 1, stk. 1, nr. 25 og 26.

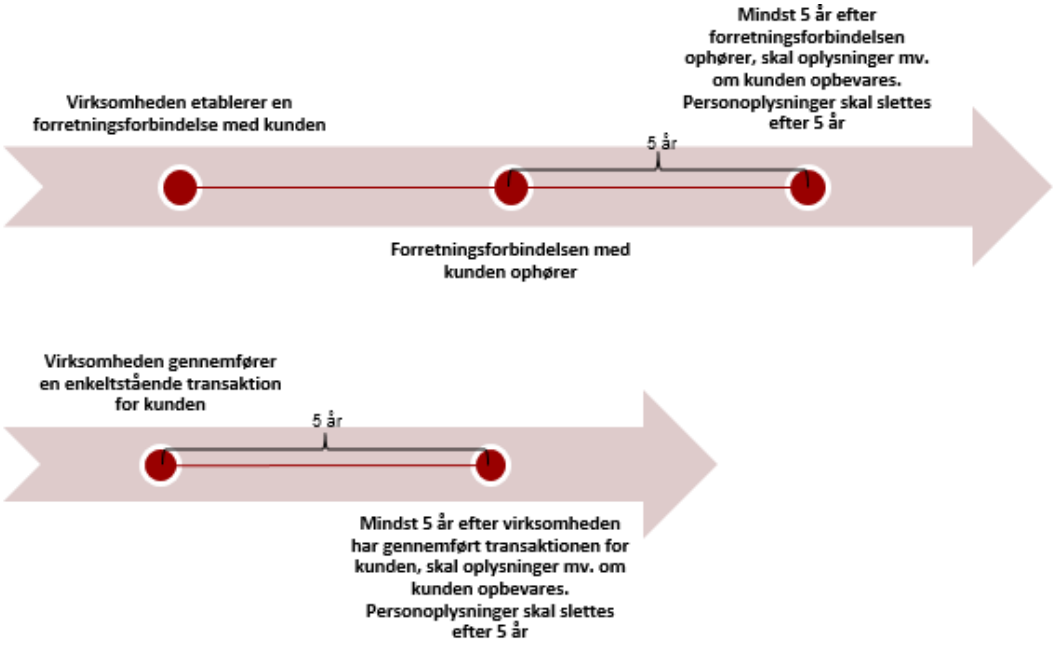
Virksomheden har pligt til at opbevare følgende oplysninger:

1) Alle oplysninger indhentet i forbindelse med kundekendskabsprocedurer, herunder de indhentede identitets- og kontroloplysninger og kopi af foreviste legitimationsdokumenter.
2) Dokumentation for og registreringer af transaktioner, når der er tale om en forretningsforbindelse eller en enkeltstående transaktion.
3) Dokumenter og registreringer i forbindelse med undersøgelses- og noteringspligten.

Virksomheden skal opbevare de pågældende oplysninger i mindst 5 år efter forretningsforbindelsens ophør og ved enkeltstående transaktioner mindst 5 år efter transaktionens gennemførelse.

Nedenstående figurer illustrerer opbevaringspligten for henholdsvis forretningsforbindelser og enkeltstående transaktioner.

[11] http://www.anklagemyndigheden.dk/da/brugervejledninger



Ad 1)
Ved ”identitetsoplysninger” er der tale om de faktiske oplysninger om en person eller virksomhed. Når kunden er en fysisk person, er der tale om navn og cpr-nr. De samme oplysninger skal opbevares om reelle ejere. Når kunden er en juridisk person, skal der ske opbevaring af navn og cvr-nr. samt oplysninger om den juridiske persons ejer- og kontrolstruktur. Virksomheden kan ud fra en risikovurdering også have indhentet yderligere identitetsoplysninger, som f.eks. oplysninger om kundens adresse.

Ved ”kontroloplysninger” er der tale om de oplysninger, som virksomheden har brugt for at kontrollere, at identitetsoplysningerne er korrekte. Ved brug af NemID, elektronisk ID eller andre digitale signaturer med OCES-standard eller elektroniske databaser skal virksomheden opbevare et revisionsspor, der dokumenterer, at der er sket kontrol af den enkelte kundes identitetsoplysninger. Oplysninger om kontrollen af en juridisk persons ejer- og kontrolstruktur, herunder reelle ejere, skal også opbevares.

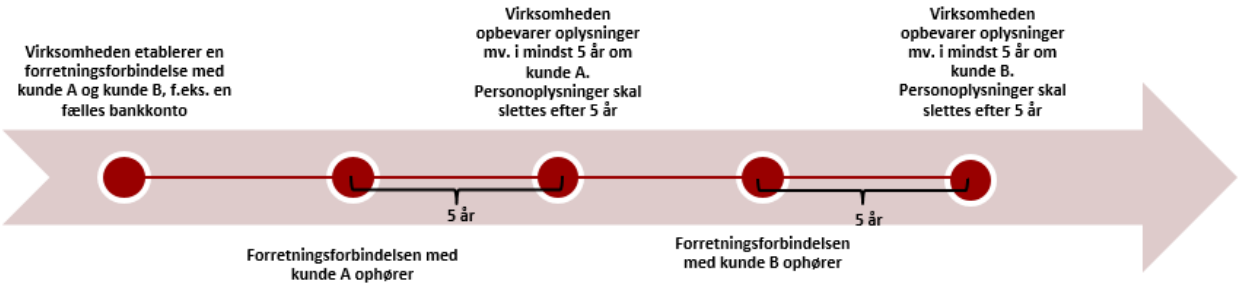
Ved ”legitimationsdokumenter” er der tale om fysiske dokumenter, som sundhedskort, pas og kørekort. Virksomheden skal opbevare en kopi af disse dokumenter. Det er ikke tilstrækkeligt alene at notere oplysninger om den dokumentation, der er forevist. Kravet om en kopi af legitimationsdokumenter kan f.eks. opfyldes ved at tage en fotokopi af dokumentet eller indscanne et billede af dokumentet.

Da alle oplysninger indhentet i forbindelse med virksomhedens kundekendskabsprocedurer skal opbevares, betyder det, at der skal ske opbevaring af oplysninger om forretningsforbindelsens formål og tilsigtede beskaffenhed, midlernes oprindelse mv. samt oplysninger, virksomheden har indhentet for at kunne risikovurdere kunden.

Virksomheden skal også opbevare andre relevante oplysninger, som f.eks. godkendelse af forretningsforbindelser med politisk eksponerede personer (PEP’er) og korrespondentforbindelser.

Hvis en kunde som del af sin forretningsforbindelse har delt produkt eller tjenesteydelse med en anden kunde, f.eks. en fælles bankkonto, og forretningsforbindelsen ophører med kunden, skal virksomheden

opbevare oplysningerne i mindst fem år efter at forretningsforbindelsen er ophørt. Virksomheden er således ikke forpligtet til at opbevare oplysninger om en forretningsforbindelse mere end fem år efter, at forretningsforbindelsen med den anden kunde, som kunden har delt produkt eller tjenesteydelse med, ophører. Se figur nedenfor.



Ad 2)
Virksomheden skal opbevare dokumentation for transaktioner og registreringer heraf, når de bliver gennemført som led i en forretningsforbindelse eller som en enkeltstående transaktion.

Det er ikke alle dokumenter og registreringer, som virksomheden skal opbevare, men alene oplysninger der har betydning for en konkret transaktion, det vil sige oplysninger om karakteren af og formålet med transaktionen. Det er f.eks. dokumenter, telefonnotater mv. af ordregivende karakter samt kontooversigter.

Hvis f.eks. et lånetilbud ikke udvikler sig til, at kunden optager et lån, er der ikke krav om, at tilbuddet bliver opbevaret.

Ad 3)
Virksomheden skal opbevare dokumenter og registreringer vedrørende undersøgelser foretaget efter kravene i hvidvaskloven, se afsnit 24 om undersøgelsespligten.

Kravet betyder, at virksomheden som minimum skal opbevare notater om undersøgelser af transaktioner og aktiviteter, herunder resultatet af undersøgelsen og grundlaget for resultatet.

Det er ikke tilstrækkeligt at anføre, at der er foretaget en undersøgelse. Notatet skal indeholde oplysninger om, hvorfor og hvordan der er foretaget en undersøgelse, og hvad konklusionen er.

Sletning af personoplysninger
De personoplysninger, som virksomheden opbevarer, skal slettes, når der er gået 5 år efter forretningsforbindelsens ophør eller 5 år fra gennemførelsen af en enkeltstående transaktion. De pågældende personoplysninger skal herefter slettes, medmindre anden lovgivning, f.eks. bogføringsloven, stiller krav om, at de skal opbevares i længere tid. Virksomheden kan fastsætte et interval for sletningen, dog må dette interval som udgangspunkt ikke være længere end en måned efter 5-års fristen, medmindre afgørende hensyn taler herimod.

Oplysninger om juridiske personer er ikke underlagt samme krav. Disse oplysninger skal virksomheden som minimum opbevare i 5 år. Herefter kan de, men skal ikke slettes. Ved oplysninger om fysiske personer, f.eks. reelle ejere af en juridisk person, er der tale om personoplysninger.

Del 6 – Grænseoverskridende virksomhed og sanktioner

27. Grænseoverskridende virksomhed

Henvisning til hvidvaskloven: §§ 31 – 31 b.

Henvisning til 4. hvidvaskdirektiv: Artikel 45, stk. 2-3 og stk. 5.

27.1. Virksomheder, der driver virksomhed i et andet EU/EØS-land

Danske virksomheder, der driver virksomhed i et andet EU- eller EØS-land, skal sikre, at den etablerede virksomhed overholder de regler om hvidvask og finansiering af terrorisme, som gælder i værtslandet (etableringslandet).

En virksomhed kan drive virksomhed i andre lande ved f.eks. at etablere et datterselskab eller en filial.

Virksomhedens ansvar for at sikre, at etablerede virksomheder overholder værtslandets lovgivning, gælder kun etablerede virksomheder, der er omfattet af 4. hvidvaskdirektiv.

Hvis virksomheden f.eks. har etableret et datterselskab i et andet land i EU, som udelukkende varetager HR-opgaver, it-drift eller administration af ejendomme, er bestemmelsen ikke relevant.

Det skal bemærkes, at grænseoverskridende virksomhed uden etablering (i værtslandet) ikke er omfattet af værtslandets regler og tilsyn på hvidvaskområdet.

Virksomheden skal sikre, at den etablerede virksomhed lever op til værtslandets regler ved at sikre, at den etablerende virksomheds politikker, forretningsgange og kontroller om risikostyring, kundekendskabsprocedurer, undersøgelses-, noterings- og underretningspligt, opbevaring af oplysninger, screening af medarbejdere og intern kontrol overholder de nationale bestemmelser i værtslandet.

Derudover skal virksomheden, som moderselskab, føre kontrol med den etablerede virksomheds overholdelse af moderselskabets politikker, forretningsgange og kontroller. Kontrollen skal udføres med passende intervaller, og kan f.eks. gennemføres ved at udtage stikprøver af den etablerede virksomheds forretningsforbindelser, dokumenterede kundekendskabsoplysninger, gennemgang af virksomhedens underretninger og/eller ved f.eks. at tage på kontrolbesøg i den etablerede virksomhed.

27.2. Hvis værtslandets regler om hvidvask og finansiering af terrorisme er lempeligere

Hvis virksomheden har etableret en virksomhed i et land, der ikke er et EU- eller EØS-land, hvis regler om hvidvask og finansiering af terrorisme er lempeligere end de regler, der gælder i den danske hvidvasklov, skal den forpligtede virksomhed i Danmark sikre, at den etablerede virksomhed opfylder den danske hvidvasklovs krav og danske krav om databeskyttelse. Dette skal dog kun overholdes i det omfang, det ikke vil stride imod den nationale ret i værtslandet.

27.3. Hvis værtslandets regler om hvidvask og finansiering af terrorisme er strengere end de danske

Hvis virksomheden har etableret virksomhed i et land, der ikke er et EU- eller EØS-land, hvis regler om hvidvask og finansiering af terrorisme er skærpede i forhold til de regler, der gælder i den danske hvidvasklov, skal den forpligtede virksomhed i Danmark kontrollere, at den etablerede virksomhed overholder etableringslandets regler. Da disse regler er skærpede i forhold til den danske hvidvasklov, er virksomheden ikke forpligtet til at foretage sig yderligere.

Virksomheden skal stadig have politikker og forretningsgange på koncernniveau, der skal tilpasses hele koncernen. Se afsnit 5 om koncerner.

27.4. Hvis værtslandets regler ikke tillader gennemførelse af kravene i hvidvaskloven

Hvis virksomheden har etableret en virksomhed i et land, der ikke er et EU- eller EØS-land, hvis regler ikke muliggør gennemførelse og overholdelse af kravene i hvidvaskloven, skal virksomheden i stedet træffer andre foranstaltninger for at sikre, at risikoen for hvidvask og finansiering af terrorisme i den etablerede virksomhed imødegås på en anden måde.

En virksomhed, der er underlagt den danske hvidvasklov, skal underrette den danske tilsynsmyndighed, som påser virksomhedens overholdelse af hvidvaskloven, om at virksomheden har etableret et datterselskab eller en filial i et land, hvor det ikke er muligt at gennemføre og overholde krav svarende til kravene i hvidvaskloven.

Virksomheden skal foretage underretningen, uanset om virksomheden har iværksat effektive foranstaltninger for at imødekomme risikoen for hvidvask og finansiering af terrorisme i den etablerede virksomhed.

Tilsynsmyndigheden vil vurdere, om de iværksatte foranstaltningerne er tilstrækkelige til, at risikoen er imødegået, eller om det er nødvendigt at iværksætte yderligere tilsynsforanstaltninger.

Virksomheden kan finde vejledning til at mitigere risici for hvidvask og finansiering af terrorisme, hvor virksomheden har etableret en virksomhed i et land, der ikke er et EU- eller EØS-land, hvis regler ikke muliggør gennemførelse og overholdelse af kravene i hvidvaskloven, i EBA's tekniske standarder på området.[12]

27.5. Udveksling af oplysninger om underretninger

Henvisning til hvidvaskloven: § 32. Henvisning til 4. hvidvaskdirektiv: Artikel 45, stk. 8.

[12] Final Report on Draft Joint Regulatory Technical Standards on the measures credit institutions and financial institutions shall take to mitigate the risk of money laundering and terrorist financing where a third country's law does not permit the application of group-wide policies and procedures: https://esas-joint-committee.europa.eu/Publications/Reports/Final%20Report%20on%20Joint%20RTS%20on%203rd%20countries.pdf

Virksomheder i en koncern, der er omfattet af hvidvaskloven, har pligt til at udveksle oplysninger om underretninger til Hvidvasksekretariatet til øvrige virksomheder i koncernen.

Pligten omfatter kun underretninger, der vedrører midler, hvor der er mistanke om, at midlerne stammer fra udbytte fra en kriminel handling eller forbundet med finansiering af terrorisme. Virksomheden skal derfor kun videregive oplysninger, når underretningen vedrører en kundes midler, og ikke hvis underretningen vedrører en kundes øvrige aktiviteter.

Virksomheder har dog mulighed for at udveksle oplysninger inden for en koncern, når en kundes øvrige aktiviteter mistænkes for hvidvask eller finansiering af terrorisme. Se afsnit 31.1 om undtagelser til tavshedspligten.

Udvekslingen af oplysninger er begrænset til, at virksomheden skal give meddelelse om, at der er mistanke om, at en kundes midler er udbytte fra en kriminel handling eller for at være forbundet med finansiering af terrorisme i tilfælde, hvor virksomheden har underrettet Hvidvasksekretariatet. Udvekslingen af oplysninger skal kun ske til relevante modtagere. Det betyder, at det kun skal ske til virksomheder i koncernen, som har samme kunde(r) og til de personer, der eksempelvis behandler mistænkelige transaktioner i koncernen.

Den eller de virksomheder, som modtager meddelelsen herom, skal på den baggrund selv vurdere og dokumentere, om virksomheden herefter vil gennemføre skærpede kundekendskabsprocedurer.

27.6. Begrænsning i retten til indsigt

I forhold til underretninger har den registrerede person ikke ret til indsigt i personoplysninger, der er eller vil blive behandlet i forbindelse med en underretning til Hvidvasksekretariatet ved mistanke om hvidvask og finansiering af terrorisme. Det vil sige, at personens indsigtsret i virksomhedens underretninger efter hvidvaskloven er afskåret med hensyn til oplysninger om, at der er givet underretning eller at dette overvejes. Se afsnit 31 om tavshedspligt.

27.7. Nødvendige oplysninger

Virksomheder i en koncern må ikke ved udvekslingen af oplysninger udveksle personoplysninger ud over det, der er nødvendigt for at opfylde kravet.

Det betyder, at den virksomhed, der sender oplysningerne, skal foretage en afvejning i det konkrete tilfælde. Afvejningen skal tage udgangspunkt i, hvilke oplysninger der er nødvendige at udveksle for at overholde kravet. Virksomheden må aldrig sende yderligere oplysninger end de oplysninger, der er indgået i underretningen til Hvidvasksekretariatet.

Oplysninger, der udveksles, kan indeholde kundens navn, adresse og cpr-nr., hvis virksomheden vurderer, at det er nødvendigt. Pligten til at udveksle oplysninger giver som udgangspunkt ikke adgang til, at virksomheden udveksler oplysninger om kundens engagement i virksomheden eller lignende oplysninger.

28. Forordninger om forhøjet risiko og finansielle sanktioner

Henvisning til hvidvaskloven: §§ 47, 51, 57, 60, 64, 65, 66 og bilag 3, pkt. 3 c.

Henvisning til 4. hvidvaskdirektiv: Artikel 9.
Henvisning til 5. hvidvaskdirektiv: Artikel 1, stk. 1, nr. 5.

Henvisning til anden lovgivning: Forordning (EU) 2016/1675 af 14. juli 2016 om identificering af højrisikotredjelande med strategiske mangler med senere ændringer.

Erhvervsstyrelsens vejledning om indefrysning offentliggjort den 1. maj 2008 med senere ændringer. https://eksportkontrol.erhvervsstyrelsen.dk/vejledning-om-indefrysning.

Det følgende kapitel om forordninger om forhøjet risiko og finansielle sanktioner beskriver overordnet, hvordan virksomheden skal overholde disse. For yderligere vejledning henvises til Erhvervsstyrelsens hjemmeside, www.eksportkontrol.erhvervsstyrelsen.dk/, ligesom der nedenfor henvises til Erhvervsstyrelsens vejledninger på området.

28.1. Forordning om tredjelande med forhøjet risiko

EU-Kommissionen har den 14. juli 2016 udstedt delegeret forordning (EU) 2016/1675 af 14. juli 2016 til supplering af 4. hvidvaskdirektiv, som er ændret ved delegeret forordning EU 2018/212. Forordningen der angiver en liste over lande, der er vurderet til at have strategiske mangler i deres internationale ordning for bekæmpelse af hvidvask og finansiering af terrorisme, herefter betegnet "højrisikotredjelande".

EU-Kommissionen kan foreslå ændringer til listen, herunder at tilføje eller fjerne lande fra listen.

Forordningen er udarbejdet for at sikre effektive beskyttelsesmekanismer for hele det indre marked med det formål at øge retssikkerheden for økonomiske aktører og berørte parter generelt i deres relationer med tredjelande.

EU-kommissionen har i 4. hvidvaskdirektiv beføjelse til at identificere højrisikotredjelande, og forordningens liste over højrisikotredjelande fastlægges på baggrund af en vurdering af kriterier i henhold til 4. hvidvaskdirektivs artikel 9.

Kriterierne omfatter bl.a. tredjelandes retlige og institutionelle rammer for bekæmpelse af hvidvask og finansiering af terrorisme, herunder bl.a. foranstaltninger vedrørende kundekendskabskrav, krav om opbevaring af registreringer m.fl.

Virksomheder, der er omfattet af 4. hvidvaskdirektiv, bør anvende skærpede kundekendskabsprocedurer i forbindelse med fysiske eller juridiske personer, der er etableret i et af de i forordningen oplistede højrisikotredjelande. Se afsnit 14 om skærpede kundekendskabsprocedurer.

Bilaget til forordningen indeholder en liste over de lande, som er vurderet til at være høj risiko.

Landene, der er opført på listen, har forpligtet sig til at afhjælpe de identificerede mangler, og de har udarbejdet en handlingsplan herfor i fællesskab med FATF.

28.2. Finansielle sanktioner i FN- og EU-systemet

FN's Sikkerhedsråd vedtager de såkaldte sikkerhedsresolutioner, også kendt som UNSCRs, på bl.a. terrorområdet, herunder restriktioner mod finansiering af terrorisme. Resolutionerne kan indeholde restriktioner mod såvel lande som personer, grupper, juridiske enheder og organer.

Sikkerhedsresolutionerne får retsvirkning i Danmark via EU-forordninger, der gennemfører resolutionerne. EU-forordningerne er direkte gældende i Danmark.

Udover sikkerhedsresolutionerne kan EU også vælge på eget initiativ at indføre sanktioner mod et land (også kaldet autonome sanktioner), herunder finansielle sanktioner mod lande, personer, grupper, juridiske enheder og organer. Dette er f.eks. tilfældet med sanktionerne mod Rusland, herunder mod russiske juridiske enheder, hvor EU har vedtaget en forordning om restriktive foranstaltninger over for Rusland.

Alle EU-forordninger, der indeholder sanktioner, kan findes på EU's hjemmeside, på www.sanctionsmap.eu. De relevante forordninger på hjemmesiden vil være markeret med et "frost-tegn", der betyder, at forordningen vedrører indefrysning, og at midler ikke må stilles til rådighed for de personer, grupper, juridiske enheder og organer, som er omfattet af indefrysningen.

Der sker jævnligt ændringer til FN's sikkerhedsresolutioner og EU-forordningerne, særligt ændringer til indefrysningslisterne. Det er derfor vigtigt, at virksomheden sikrer sig, at den altid anvender de opdaterede lister.

Hvis virksomheden vil modtage orientering direkte, hver gang EU opdaterer sanktionerne, herunder indefrysningslisterne, kan virksomheden tilmelde sig Erhvervsstyrelsens nyhedsmail, https://eksportkontrol.erhvervsstyrelsen.dk/abonner.

EU har oprettet en database, der indeholder en samlet oversigt over navnene på alle de personer, grupper, juridiske enheder og organer, som er omfattet af indefrysning i henhold til EU's sanktioner. EU opdaterer løbende databasen. På Erhvervsstyrelsens hjemmeside findes en vejledning i brug af databasen, se https://eksportkontrol.erhvervsstyrelsen.dk/vejledning-om-indefrysning.

28.3. Screening af kunder og transaktioner

I den tidligere gældende hvidvasklov var det et krav, at virksomheden havde procedurer for screening af EU-forordninger, der indeholdt finansielle sanktioner. Dette er ikke et krav efter den nye hvidvasklov. Virksomhederne skal dog stadig overholde EU-forordningerne og bl.a. sikre, at midler hverken direkte eller indirekte stilles til rådighed for de personer, grupper, juridiske enheder og organer, der står opført i indefrysningsbilagene til forordningerne.

For at sikre at virksomheden ikke stiller midler direkte eller indirekte til rådighed for personer mv., der er omfattet af indefrysning, skal virksomheden screene sine kunder og deres transaktioner. Med "screening" menes, at virksomheden skal sikre, at hverken kunden eller transaktionsmodtageren, står opført i en af EU-forordningerne.

Virksomheden kan holde sig opdateret via EU's database, se beskrivelse i afsnit 28.2 om finansielle sanktioner i FN- og EU-systemet. Der er også flere private aktører, der udbyder en service med screening mod diverse lister, der sikrer at alle de lister, der screenes mod, er opdaterede.

28.4. Navne- og identitetsmatch

Hvis virksomheden ved screening af kunden eller transaktionen får et såkaldt "match", hvor der f.eks. er navnesammenfald mellem kunden eller transaktionsmodtageren og en person, gruppe, juridisk enhed eller organ, som er omfattet af indefrysning, skal virksomheden undersøge, om der alene er tale om et navnesammenfald, eller om der også foreligger et identitetssammenfald. Ved identitetssammenfald forstås, at kunden eller transaktionsmodtageren er oplistet i en af forordningerne, og at der dermed ikke må stilles midler til rådighed for denne person, gruppe, juridiske enhed eller organ.

Hvis der er tale om et identitetssammenfald, må virksomheden derfor ikke oprette konti, investere, overføre eller på anden måde give personen adgang til det finansielle marked. Se Erhvervsstyrelsens Vejledning om indefrysning, https://eksportkontrol.erhvervsstyrelsen.dk/sites/default/files/media/2016-01-16_vejledning_om_indefrysning_da.pdf.

Virksomheden har pligt til at undersøge, hvorvidt der alene er navne sammenfald eller et identitetssammenfald. Når virksomheden har foretaget denne undersøgelse og konstateret, at kunden er oplistet i en af EU-forordningerne om sanktioner mod ISIL og Al-Qaida, terrorisme generelt, Afghanistan, Iran, Nordkorea og Syrien, skal virksomheden straks foretage en underretning til Hvidvasksekretariatet med de oplysninger, som virksomheden har om kunden. Underretningen skal først ske, når identitetssammenfald er konstateret.

28.5. Indirekte tilrådighedsstillelse

I mange af EU's forordninger om finansielle sanktioner er der fastsat en bestemmelse om, at ingen pengemidler eller økonomiske ressourcer direkte eller indirekte må stilles til rådighed for eller være til fordel for de fysiske eller juridiske personer, enheder eller organer, der er omfattet af indefrysning.

EU har offentliggjort en vejledning om ejerskab og kontrol til brug for undersøgelse af indirekte tilrådighedsstillelse. Vejledningen finder du på Erhvervsstyrelsens hjemmeside.

Del 7 – Ansatte og whistleblowerordning

29. Whistleblowerordning

Henvisning til hvidvaskloven: § 35. Henvisning til 4. hvidvaskdirektiv: Artikel 61, stk. 3. Henvisning til 5. hvidvaskdirektiv: Artikel 1, stk. 1, nr. 39, litra b. Henvisning til anden lovgivning: Lov om finansiel virksomhed § 75 a.

Virksomheder skal have en ordning, hvor virksomhedens ansatte via en særlig, uafhængig og selvstændig kanal kan indberette overtrædelser eller potentielle overtrædelser af hvidvasklovgivningen begået af virksomheden, herunder af ansatte eller medlemmer af bestyrelsen i virksomheden. Indberetninger til ordningen skal kunne foretages anonymt. Herudover skal virksomheder følge op på indberetninger til ordningen og skriftligt kunne dokumentere, hvordan det er sket.

Efter de generelle regler i lov om finansiel virksomhed skal virksomheder, der er underlagt den finansielle lovgivning, have en whistleblowerordning.

De virksomheder, der er omfattet af kravet om en whistleblowerordning i hvidvaskloven, er virksomheder omfattet af hvidvasklovens § 1, stk. 1, nr. 5, 8 og 11, for så vidt angår alternative investeringsfonde, nr. 13-20 og 22-24.

Kravet om, at virksomheden skal have en whistleblowerordning, omfatter dog kun virksomheder, der beskæftiger flere end fem ansatte. Se afsnit 29.1 nedenfor om undtagelse.

At virksomheden skal have en særlig kanal, betyder, at kanalen skal være oprettet med det formål, at ansatte skal kunne indberette overtrædelser eller potentielle overtrædelser af hvidvasklovgivningen til ordningen.

Hvis virksomheden har en whistleblowerordning i henhold til anden lovgivning, kan denne ordning også omfatte indberetninger efter hvidvasklovgivningen. Det er ikke et krav, at virksomheden opretter en særskilt whistleblowerordning for indberetning af overtrædelse efter hvidvasklovgivningen, så længe virksomheden sikrer, at ansatte kan foretage indberetninger af overtrædelser eller potentielle overtrædelser af hvidvasklovgivningen via en whistleblowerordning.

Overtrædelse af anden lovgivning som f.eks. markedsføringsloven eller straffeloven (f.eks. underslæb, bedrageri mv.) omfattes dog ikke af bestemmelsens anvendelsesområde i hvidvaskloven.

Virksomhedens ansatte skal kunne indberette såvel alvorlige som mindre alvorlige overtrædelser eller potentielle overtrædelser. Det kan f.eks. være tilfælde, som kun vil kunne medføre at virksomheden modtager et påbud eller en påtale fra tilsynsmyndigheden.

At kanalen skal være uafhængig og selvstændig, betyder, at der skal etableres en selvstændig funktion, der er uafhængig af den daglige ledelse, og hvor indberetning kan ske uden om de normale procedurer,

f.eks. direkte til den afdeling eller medarbejder, som behandler indberetningerne. Dette vil eksempelvis kunne være en complianceansvarlig.

Anonymitet
Det forhold, at indberetninger skal kunne foretages anonymt, betyder, at den, der indberetter en overtrædelse eller en potentiel overtrædelse, kan gøre dette fuldstændigt anonymt. Det kan f.eks. være via en løsning på virksomhedens intranet, hvor der kan indsendes indberetninger uden angivelse af navn og uden mulighed for sporing af computerens IP-adresse og lignende.

Indberetningerne bør som udgangspunkt alene være tilgængelige for den afdeling eller medarbejder, som behandler indberetningerne, eksempelvis den complianceansvarlige.

Det er vigtigt at sikre, at ansatte, der anvender ordningen, kan være fuldstændig anonyme, da det kan være svært for en ansat at beslutte at indberette en overtrædelse til virksomheden, hvis dette ikke kan ske anonymt. En ansat kan eksempelvis være bange for at miste sit arbejde, mens andre ansatte kan føle, at de har handlet illoyalt over for en kollega eller over for virksomheden.

En overtrædelse eller en potentiel overtrædelse begået af virksomheden, herunder af ansatte eller medlemmer af bestyrelsen, omfatter enhver overtrædelse eller potentiel overtrædelse af virksomhedens forpligtelser. Det gælder, også selvom en overtrædelse eller den potentiel overtrædelse ikke kun skyldes én enkelt person, men eksempelvis skyldes en grundlæggende systemfejl i virksomheden.
Der vil derfor også kunne blive indberettet overtrædelser, der skyldes undladelser, dvs. pligter, som virksomheder ikke opfylder.

Hvis en virksomhed eller person har valgt at outsource en del af sine opgaver til en ekstern virksomhed, vil de ansatte i virksomheden også kunne indberette den eksterne virksomheds manglende efterlevelse af forpligtelser til virksomhedens whistleblowerordning. Ansatte hos den eksterne virksomhed vil også kunne indberette overtrædelser til den relevante tilsynsmyndighed. Se afsnit 22 om outsourcing.

Outsourcing
En whistleblowerordning kan outsources til en ekstern leverandør, men virksomheden kan ikke fraskrive sig sine forpligtelser efter lovgivningen, og virksomheder, der benytter sig af outsourcing, er således fortsat ansvarlige for, at ordningerne lever op til lovgivningens krav. Se afsnit 22 om outsourcing.

En virksomhed, som varetager, administrerer eller på anden måde håndterer en ordning på vegne af en anden virksomhed, skal være opmærksom på anden speciallovgivning, der kan være til hinder herfor. En sådan ekstern virksomhed skal også være opmærksom på eventuelle lovbestemte oplysningsforpligtelser, som virksomhederne kan være underlagt.

Ansattes, herunder direktionens, indberetning til whistleblowerordningen vil ikke være i strid med tavshedspligten i selskabslovens § 132 eller speciallovgivningens tavshedsregler, herunder tavshedspligten i lov om finansiel virksomhed. Dette gælder også i tilfælde, hvor ordningen er outsourcet til en ekstern leverandør.

Kollektiv overenskomst
Whistleblowerordningen kan etableres via en kollektiv overenskomst.

I praksis betyder dette, at arbejdsmarkedets parter efter aftale med virksomhederne har mulighed for at etablere en ordning i f.eks. et fagforbund, hvortil ansatte i virksomheden kan indberette overtrædelser. En whistleblowerordning, der baserer sig på en aftale mellem de forhandlingsberettigede parter, skal leve op til kravene i § 35 stk. 1 som beskrevet lige ovenfor.

29.1. Undtagelse til whistleblowerordningen

For virksomheder, der ikke har flere end fem ansatte, er der ikke en forpligtelse i hvidvaskloven til at have en whistleblowerordning.

Dog skal virksomheder i sådanne tilfælde være opmærksomme på, at så snart de ansætter en sjette medarbejder, omfattes de af kravet.

Virksomheder skal etablere en whistleblowerordning senest tre måneder efter ansættelse af den sjette ansatte. Dette er for at sikre, at virksomheder har den fornødne tid til at etablere ordningen, når virksomheden overskrider grænsen på fem ansatte.

Ved opgørelsen af antallet af ansatte i virksomheden skal der ikke sondres mellem kategorier af ansatte i virksomheden. Det betyder, at alle ansatte, der har en ansættelseskontakt med virksomheden, herunder eksempelvis ansatte uden direkte kundekontakt, interne administrationsmedarbejdere m.fl., skal indgå i den samlede opgørelse af virksomhedens ansatte. Alle ansatte skal have mulighed for at anvende en virksomheds whistleblowerordning, og alle ansatte skal indgå i den samlede opgørelse af virksomhedens ansatte.

Bestyrelsesmedlemmer er ikke ansatte i en virksomhed, og de skal derfor ikke medregnes. Rengøringspersonale, der ikke er ansat af virksomheden, men af et særskilt rengøringsselskab, skal heller ikke medregnes.

Ansatte i virksomheder med fem ansatte eller derunder har mulighed for at indberette overtrædelser eller potentielle overtrædelser til den relevante tilsynsmyndigheds whistleblowerordning.

29.2. Ansatte, der indberetter virksomheden

Henvisning til hvidvaskloven: § 36. Henvisning til 4. hvidvaskdirektiv: Artikel 38 og 61, stk. 2, litra b. Henvisning til 5. hvidvaskdirektiv: Artikel 1, stk. 1, nr. 23.

Den ansattes indberetning omfatter bl.a. enhver anmeldelse eller meddelelse til tilsynsmyndighederne eller til en virksomheds whistleblowerordning, som kan omhandle virksomhedens, herunder en ansats eller et bestyrelsesmedlems, overtrædelse eller potentiel overtrædelse af hvidvaskloven og regler udstedt i medfør heraf. Indberetning omfatter også indberetning om overtrædelse eller potentiel overtrædelse af 2. pengeoverførselsforordning og forordninger, der indeholder regler om finansielle sanktioner mod lande, personer, grupper, juridiske enheder og organer.

Virksomheden må ikke udsætte den ansatte eller tidligere ansatte for ufordelagtig behandling eller ufordelagtige følger som følge af, at den ansatte eller tidligere ansatte har indberettet virksomhedens overtrædelse eller potentielle overtrædelse af hvidvaskloven til en tilsynsmyndighed eller til en whistleblowerordning i virksomheden.

Virksomheden må ikke udsætte ansatte eller tidligere ansatte for ufordelagtig behandling eller ufordelagtige følger som følge af, at den ansatte eller tidligere ansatte har foretaget en underretning til Hvidvasksekretariatet, heller ikke hvis det er en intern underretning på baggrund af en ansats mistanke om hvidvask eller finansiering af terrorisme.

Ufordelagtig behandling kan f.eks. være afskedigelse, degradering, forflyttelse, chikane eller lignende. Som udgangspunkt er alle former for ufordelagtig behandling omfattet.

Indberetning til whistleblowerordninger etableret via en kollektiv overenskomst er også omfattet af bestemmelsen.

Krav om årsagssammenhæng
Det er en forudsætning for bestemmelsens anvendelsesområde:

1) at den ansatte eller tidligere ansatte har indberettet en overtrædelse eller en potentiel overtrædelse til tilsynsmyndigheden og
2) at der er årsagssammenhæng mellem den ufordelagtige behandling/følge og det forhold, at den ansatte eller tidligere ansatte har indberettet en overtrædelse.

Bestemmelsen finder derfor kun anvendelse i forbindelse med ufordelagtig behandling eller ufordelagtige følger, som besluttes, efter at den ansatte eller tidligere ansatte har indberettet en virksomheds overtrædelse eller potentielle overtrædelse.

Ved en intern underretning forstås, at en ansat internt i virksomheden har underrettet f.eks. den hvidvaskansvarlige om en mistanke. Beskyttelsen af den ansatte eller tidligere ansatte gælder, uanset om den hvidvaskansvarlige afkræfter mistanken efter en nærmere undersøgelse. Se afsnit 24 om undersøgelsespligt.

Godtgørelse til den ansatte
Hvis en ansat eller tidligere ansat har indberettet og derefter oplevet en ufordelagtig behandling eller følge, kan den ansatte få tilkendt en godtgørelse i overensstemmelse med principperne i ligebehandlingsloven. Godtgørelsen vil blive fastsat under hensyn til den ansattes eller tidligere ansattes ansættelsestid og sagens omstændigheder i øvrigt, herunder med iagttagelse af det EU-retlige effektivitetsprincip.

Den ansatte eller tidligere ansatte kan ikke få ret til godtgørelse i medfør af flere forskellige regelsæt for samme hændelse. Det samme gør sig gældende, hvis den ansatte eller tidligere ansatte er berettiget til en godtgørelse i henhold til overenskomster og andre arbejdsretlige aftaler.
En ansat, der mener at have været udsat for ufordelagtig behandling eller følge som følge af, at pågældende har foretaget en indberetning om overtrædelse eller en potentiel overtrædelse, skal gøre krav på godtgørelse gældende over for virksomheden ved de almindelige domstole.

Beskyttelsen af den ansatte i hvidvasklovens § 36 kan ikke fraviges
Kravet til virksomheden om at virksomheden ikke må behandle en ansat eller en tidligere ansat ufordelagtigt på baggrund af den ansattes indberetning, kan ikke forudgående eller efterfølgende ved aftale fraviges til ugunst for den ansatte.

Det er muligt at indgå aftaler, der stiller den ansatte bedre end lovforslagets bestemmelser.

29.3. Rapporteringspligt til virksomhedens bestyrelse om advarsler om hvidvask og terrorfinansiering

Henvisning til hvidvaskloven: § 36 a. Med hensyn til definitionen på nøglepersoner henvises til § 64 c, stk. 2, i lov om finansiel virksomhed

Den daglige ledelse i virksomheder, der er omfattet af hvidvaskloven, skal rapportere om advarsler om hvidvask eller terrorfinansiering modtaget fra andre, herunder fra udenlandske myndigheder, eksterne revisorer og konsulenter samt whistleblowere. Rapporteringen skal ske til virksomhedens øverste ledelsesorgan uden unødigt ophold.

Rapporteringspligten gælder ligeledes for danske virksomheders udenlandske filialer, jf. hvidvasklovens § 1, stk. 5. Dette betyder, at danske virksomheders udenlandske filialer har pligt til at rapportere om advarsler om hvidvask eller terrorfinansiering til virksomhedens øverste ledelsesorgan i virksomhedens danske hovedkontor. Anvendelsesområdet for § 36 a er således ikke begrænset til de personer og virksomheder, som fremgår af hvidvasklovens § 1, stk. 1.

Ligeledes gælder rapporteringspligten for udenlandske virksomheders danske filialer, idet udenlandske virksomheders danske filialer er omfattet af hvidvasklovens anvendelsesområde. I udenlandske virksomheders danske filialer skal den daglige ledelse rapportere om advarsler om hvidvask eller terrorfinansiering til virksomhedens øverste ledelsesorgan i virksomhedens hovedkontor i filialens hjemland.

Den daglige ledelse

Den daglige ledelse omfatter personer, der har ansvaret for en juridisk persons eller filials daglige ledelse, herunder for drift, omsætning og øvrige resultater. En juridisk persons eller filials daglige ledelse varetages typisk af den juridiske persons eller filials direktion.

Uden unødigt ophold

Ved uden unødigt ophold forstås, at advarsler om hvidvask eller terrorfinansiering skal rapporteres til bestyrelsen hurtigst muligt efter, at advarslen om hvidvask eller terrorfinansiering modtages i virksomheden.

Rapportering
Ved rapportering forstås, at virksomhedens øverste ledelsesorgan bliver gjort bekendt med alle relevante oplysninger om advarslen om hvidvask eller terrorfinansiering, herunder advarslens indhold, afsender af advarslen, og under hvilke omstændigheder advarslen er modtaget.

Advarsler om hvidvask eller terrorfinansiering

Ved en advarsel om hvidvask eller terrorfinansiering forstås enhver meddelelse, som vedrører en viden eller mistanke om en tidligere, nuværende eller eventuelt kommende overtrædelse af reglerne om hvidvask og terrorfinansiering med forbindelse til virksomheden, kunderne, de ansatte, koncernforbundne selskaber mv.

Fra andre

Ved "andre" forstås, at der efter omstændighederne kan være andre afsendere end de eksplicit nævnte, som sender en advarsel om hvidvask eller terrorfinansiering, hvis indhold har en sådan karakter og alvor, at bestyrelsen skal orienteres herom.

Udenlandske myndigheder

Som udenlandsk myndighed anses enhver institution, som er en del af den offentlige forvaltning i et andet land end Danmark. Dette kan omfatte andre landes tilsyns-, skatte-, politi- og anklagemyndigheder, men begrebet er ikke begrænset til at omfatte disse typer af myndigheder. Også advarsler fra andre landes centralbanker vil være omfattet af rapporteringsforpligtelsen. Advarsler modtaget fra institutioner, som er en del af den offentlige forvaltning i Danmark, sidestilles med advarsler modtaget fra udenlandske myndigheder.

Eksterne revisorer

Eksterne revisorer er personer eller virksomheder, der er godkendt efter §§ 3, 10 eller 11 i revisorloven[13], som udfører revisionsydelser eller lignende ydelser for virksomheden, og som ikke indgår i et ansættelsesforhold med virksomheden.

Konsulenter
Ved konsulenter forstås enhver virksomhed eller person, som udfører tjenesteydelser for virksomheden i form af rådgivning eller lignende, herunder advokater, og som ikke indgår i et ansættelsesforhold med virksomheden. Det er ikke en forudsætning, at der er indgået aftale om udførelse af tjenesteydelser med konsulenten.

Advarsler fra whistleblowere

Ved advarsler fra whistleblowere forstås advarsler om hvidvask eller terrorfinansiering, som modtages gennem den ordning, som følger af hvidvasklovens kapitel 7. Der kan dog også være tale om advarsler fra whistleblowere, som modtages på anden vis.

Forbindelse med og relevans for virksomheden

Virksomheder skal vurdere, om en given advarsel om hvidvask eller terrorfinansiering har en sådan forbindelse med og relevans for virksomheden, kunderne, de ansatte, koncernforbundne selskaber mv., at det medfører, at der skal ske rapportering til virksomhedens øverste ledelsesorgan. Virksomheden bør i den forbindelse holde sig for øje, at rapporteringen til det øverste ledelsesorgan skal ske uden unødigt ophold.

Kravet om rapportering gælder ligeledes for nøglepersoner i virksomheden. Nøglepersoner skal forstås i overensstemmelse med begrebet i lov om finansiel virksomhed. Nøglepersoner er dels ansatte, der i det

[13] Lovbekendtgørelse nr. 1287 af 20. november 2018.

daglige er en del af den faktiske ledelse, dels ansatte, der er ansvarlige for en nøglefunktion i virksomheden, jf. § 64 c, stk. 2, i lov om finansiel virksomhed. Eksempelvis oplister bestemmelsen, at den ansvarlige for compliancefunktionen, den hvidvaskansvarlige og den ansvarlige for den interne revision altid vil blive betragtet som nøglepersoner. Hvis den daglige ledelse modtager en rapportering om en modtaget advarsel fra medarbejdere, skal ledelsen videre rapportere advarslen til virksomhedens øverste ledelsesorgan.

Del 8 – Tavshedspligt og ansvar

30. Ansvarsfrihed

Henvisning til hvidvaskloven: § 37. Henvisning til 4. hvidvaskdirektiv: Artikel 37.

Underretning til Hvidvasksekretariatet
De underretninger og oplysninger, som virksomheder i god tro videregiver til Hvidvasksekretariatet i forbindelse med en underretning, medfører ikke, at en eventuel tavshedspligt overtrædes, og påfører derfor ikke virksomhedens ansatte eller ledelse nogen form for ansvar i den forbindelse.

Den samme ansvarsfrihed gør sig gældende for standsning af transaktioner i forbindelser med underretninger, se afsnit 25.4 om virksomhedens pligt til at undlade at gennemføre transaktioner.
Det er i den forbindelse et krav, at virksomheden er i god tro. Virksomheden kan dermed ikke udnytte bestemmelsen til f.eks. at standse transaktioner, hvis virksomheden er vidende om, at der ikke foreligger et forhold, der er omfattet af underretningspligten.

31. Tavshedspligt

Henvisning til hvidvaskloven: § 38, stk. 1 og 8. Henvisning til 4. hvidvaskdirektiv: Artikel 39.

Virksomheden, herunder virksomhedens ledelse og ansatte, har pligt til at hemmeligholde:

1) at der er sket underretning til Hvidvasksekretariatet,
2) at det overvejes, om der skal gives en underretning,
3) at der er iværksat en undersøgelse eller
4) at der vil blive iværksat en undersøgelse.

Tavshedspligten omfatter kun ovenstående oplysninger. Hvis en virksomhed får mistanke om, at en ansat i en anden virksomhed hvidvasker udbytte fra f.eks. underslæb eller mandatsvig over for virksomheden, er tavshedspligten ikke til hinder for, at den førstnævnte virksomhed kan oplyse den sidstnævnte virksomhed om mistanken om underslæb eller mandatsvig.

Revisorer eller andre, der udfører eller har udført et særligt hverv for virksomheden, har samme pligt til at hemmeligholde ovenstående oplysninger.

Tavshedspligten er tidsubegrænset. Det betyder, at uanset om en underretning ikke medfører, at kunden bliver sigtet for et kriminelt forhold, må virksomheden ikke informere kunden om, at der tidligere er foretaget en underretning vedrørende kunden.

Tavshedspligten er ikke til hinder for, at advokater, revisorer, eksterne bogholdere og skatterådgivere fraråder deres klient at udøve ulovlig virksomhed.

For så vidt angår øvrige virksomheder kan disse fraråde deres kunder at begå strafbare forhold, hvis virksomheden vurderer, at det kan ske, uden at kunden bliver klar over, at underretning er indgivet eller vil blive indgivet.

31.1. Undtagelser til tavshedspligten

Henvisning til hvidvaskloven: § 38, stk. 2-7. Henvisning til 4. hvidvaskdirektiv: Artikel 39. Henvisning til 5. hvidvaskdirektiv: Artikel 1, stk. 1, nr. 24.

Videregivelse til tilsynsmyndigheder og organisationer
Virksomheden kan efter anmodning videregive oplysninger om, at der er givet underretning, eller at dette overvejes, til de myndigheder eller organisationer, der fører tilsyn med overholdelse af hvidvaskloven. Det er her tale om Advokatrådet (Advokatsamfundet), Erhvervsstyrelsen, Spillemyndigheden og Finanstilsynet.

Der er ikke tale om en generel informationspligt til tilsynsmyndigheden eller organisationen, men alene en mulighed for at videregive oplysninger om underretninger på baggrund af en anmodning.

Videregivelse i forbindelse med retshåndhævelsesformål
Videregivelsen af oplysninger om underretninger kan også ske, hvis der er tale om retshåndhævelsesformål. Retshåndhævelsesformål omfatter forebyggelse, efterforskning, opdagelse og retsforfølgning af straffelovsovertrædelser og desuden beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed.

Videregivelse af oplysninger mellem virksomheder i samme koncern
Virksomheder i samme koncern kan videregive oplysninger om følgende:

1) At der givet underretning, eller at dette overvejes.
2) At der er eller vil blive iværksat en undersøgelse.

Undtagelsen til tavshedspligten gælder for virksomheder i samme koncern, der er underlagt Finanstilsynets tilsyn, og andre virksomheder i koncernen der har hjemsted eller er hjemmehørende i et EU- eller EØS-land.

Se afsnit 27.5 om virksomheders pligt til at udveksle oplysninger.

Videregivelse af oplysninger til filialer og majoritetsejede datterselskaber i tredjelande
Virksomheder kan videregive oplysninger til filialer og majoritetsejede datterselskaber beliggende i tredjelande om følgende:

a) At der givet underretning, eller at dette overvejes.
b) At der er eller vil blive iværksat en undersøgelse.

Der er alene adgang til at udveksle oplysninger med sådanne virksomheder, hvis disse fuldt ud overholder koncernens politikker og forretningsgange på hvidvaskområdet, herunder forretningsgange for udveksling af oplysninger i koncernen. Det er et krav, at koncernens politikker og forretningsgange på hvidvaskområdet opfylder kravene i 4. hvidvaskdirektiv. Se afsnit 5.2 om koncernfælles risikovurdering, politikker og forretningsgange.

Se afsnit 27.5 om virksomheders pligt til at udveksle oplysninger.

Videregivelse af oplysninger mellem virksomheder med samme juridiske eller organisatoriske struktur
Advokater, revisorer og revisionsvirksomheder, der er godkendt i henhold til revisorloven, samt virksomheder, der i øvrigt erhvervsmæssigt leverer samme ydelser som de tidligere nævnte virksomhedsgrupper, herunder revisorer, som ikke er godkendt i henhold til revisorloven, skatterådgivere og eksterne bogholdere, kan videregive oplysninger mellem hinanden om følgende:

1) At der givet underretning, eller at dette overvejes.
2) At der er eller vil blive iværksat en undersøgelse.

For at der kan ske udveksling af oplysninger, skal virksomhederne levere deres ydelser inden for samme juridiske enhed eller organisatoriske struktur. Det vil sige, at både den person, der videregiver oplysningerne, og den person, oplysningerne videregives til, skal have fælles ejerskab, fælles ledelse eller fælles kontrol med overholdelse af regler om forebyggelse af hvidvask og finansiering af terrorisme.

Der kan derfor ikke ske udveksling mellem f.eks. to advokater, hvis disse ikke tilhører samme juridiske enhed eller organisatoriske struktur. Kravet om, at personerne udøver deres virksomhed inden for samme juridiske enhed eller organisatoriske struktur, betyder ikke, at personerne skal være arbejdstagere i samme juridiske enhed eller organisatoriske struktur.

Der kan kun ske udveksling af oplysninger mellem ovenstående virksomheder, hvis de har hjemsted eller er hjemmehørende i et EU- eller EØS-land samt i tredjelande, der opfylder kravene i 4. hvidvaskdirektiv.

Videregivelse af oplysninger mellem virksomheder, der ikke er del af samme gruppe eller koncern
Videregivelse af oplysninger mellem virksomheder, der ikke er en del af samme gruppe eller koncern mv., kan ske om følgende:

1) At der givet underretning eller at dette overvejes.
2) At der er eller vil blive iværksat en undersøgelse.

Tre betingelser skal være opfyldt, før der kan ske videregivelse:

1) oplysningerne vedrører samme kunde og samme transaktion,
2) modtageren af oplysningerne er underlagt krav til bekæmpelse af hvidvask og finansiering af terrorisme, der svarer til kravene i 4. hvidvaskdirektiv, og
3) modtageren er underlagt forpligtelser med hensyn til tavshedspligt og beskyttelse af personoplysninger.

Ad 1)
Det er et krav, at kunden er kunde hos både modtageren og afsenderen af oplysningerne, og at oplysningerne vedrører en transaktion, som både involverer modtageren og afsenderen. Kunden skal derfor være en fælles kunde på tidspunktet for videregivelsen af oplysningerne.

Ad 2)
Modtageren af oplysningerne skal være underlagt krav til bekæmpelse af hvidvask og finansiering af terrorisme, der svarer til kravene i 4. hvidvaskdirektiv. Afsenderen skal, inden oplysningerne bliver videregivet, kontrollere, at dette er opfyldt.

Hvis modtageren er etableret i et EU- eller EØS-land, hvor 4. hvidvaskdirektiv er implementeret, vil dette krav være opfyldt. Er modtageren etableret uden for et EU-eller EØS-land, kan oplysninger om, hvorvidt kravene er opfyldt, findes i f.eks. FATF's evalueringsrapporter.

Ad 3)
Modtageren og afsenderen skal være underlagt forpligtelser med hensyn til tavshedspligt og beskyttelse af personoplysninger.

Der kan kun ske udveksling af oplysninger mellem virksomheder, der har hjemsted eller er hjemmehørende i et EU- eller EØS-land samt i tredjelande, der opfylder kravene i 4. hvidvaskdirektiv.

Følgende virksomheder kan ikke benytte undtagelsen til tavshedspligten og videregive oplysninger mellem virksomheder, der ikke er en del af samme gruppe eller koncern mv:

1) udbydere af tjenesteydelser til virksomheder,
2) udbydere af spil,
3) ejendomsmæglere og ejendomsmæglervirksomheder samt virksomheder, der leverer samme ydelser som ejendomsmæglere eller ejendomsmæglervirksomheder.

Del 9 – Pengeoverførsler

32. Pengeoverførselsforordningen

Henvisning til EU-retsakter: Europa-Parlamentets og Rådets forordning (EU) 2015/847 af 20. maj 2015 om oplysninger, der skal medsendes ved pengeoverførsler, og om ophævelse af forordning (EF) nr. 1781/2006.

Henvisning til anden lovgivning: Direktiv 2015/2366 om betalingstjenester i det indre marked og om ændring af direktiv 2002/ 65/EF og 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF af 25. november 2015, artikel 3.

Henvisning til anden relevant vejledning: EBA's endelige retningslinjer af 16. januar 2018: "Fælles retningslinjer i henhold til artikel 25 i forordning (EU) 2015/847 om de foranstaltninger, betalingsformidlere bør træffe med henblik på at konstatere, om oplysninger om betaler eller betalingsmodtager mangler eller er ufuldstændige, og de procedurer, de bør indføre for at håndtere en pengeoverførsel, som mangler de krævede oplysninger".

32.1. Baggrund

Pengeoverførselsforordningens formål er at forebygge, opdage og efterforske hvidvask og finansiering af terrorisme. Forordningen omfatter pengeoverførsler, når mindst én af de involverede betalingsformidlere – dvs. de virksomheder, som udfører pengeoverførslen for en kunde – er etableret i EU.

Pengeoverførselsforordningen fastsætter regler om de oplysninger om betaler og betalingsmodtager, der skal medsendes ved pengeoverførsler, uanset valuta.

Oplysningerne skal følge med pengeoverførslen for, at det er muligt at spore transaktionen tilbage til betaleren eller frem til betalingsmodtageren.

Pengeoverførselsforordningen vedrører som udgangspunkt alle pengeoverførsler, der helt eller delvist gennemføres elektronisk, uanset hvilket meddelelses-, betalings- eller afviklingssystem der benyttes. Pengeoverførsler, hvor en betaling afsendes eller modtages uden for EU, er også omfattet af forordningen.

32.2. Definitioner

Henvisning til pengeoverførselsforordningen: Artikel 3.

I forordningen defineres relevante begreber. Nedenfor følger udvalgte definitioner.

Ved ”betaler” forstås en fysisk eller juridisk person, der er indehaver af en betalingskonto og som tillader en pengeoverførsel fra denne betalingskonto, eller, hvis der ikke er nogen betalingskonto, som udsteder en betalingsordre.

Ved ”betalingsmodtager” forstås en person, som er den tiltænkte modtager af pengeoverførslen.

Ved ”betalingsformidler” forstås de kategorier af udbydere af betalingstjenester, som er omfattet af artikel 1, stk. 1, i direktiv 2015/2366 om betalingstjenester i det indre marked, fysiske og juridiske personer, der drager fordel af undtagelser i henhold til artikel 32 i direktivet og juridiske personer, der drager fordel af undtagelser i henhold til artikel 9 i Europa-Parlamentets og Rådets direktiv 2009/110/EF (19) om adgang til at optage og udøve virksomhed som udsteder af elektroniske penge og tilsyn med en sådan virksomhed, og som udbyder tjenester i form af pengeoverførsler.

Ved ”mellembetalingsformidler” forstås en betalingsformidler, som hverken er betalers eller betalingsmodtagers betalingsformidler, og som modtager og videresender en pengeoverførsel på vegne af betalers eller betalingsmodtagers betalingsformidler eller på vegne af en anden mellembetalingsformidler.

Ved ”betalingskonto” forstås en betalingskonto som defineret i artikel 4, nr. 12, i direktiv 2015/2366 om betalingstjenester i det indre marked.

Ved ”midler" forstås midler som defineret i artikel 4, nr. 25, i direktiv 2015/2366 om betalingstjenester i det indre marked.

Ved ”pengeoverførsel” forstås en transaktion, der helt eller delvist gennemføres elektronisk på en betalers vegne gennem en betalingsformidler med henblik på at stille midler til rådighed for en betalingsmodtager gennem en betalingsformidler, uanset om betaler og betalingsmodtager er den samme person, og uanset om betalerens og betalingsmodtagerens betalingsformidler er den samme, herunder:

a) En kreditoverførsel som defineret i artikel 2, nr. 1, i forordning (EU) nr. 260/2012 om tekniske og forretningsmæssige krav til kreditoverførsler og direkte debiteringer i euro.

b) En direkte debitering som defineret i artikel 2, nr. 2, i forordning (EU) nr. 260/2012 om tekniske og forretningsmæssige krav til kreditoverførsler og direkte debiteringer i euro.

c) Pengeoverførsler som defineret i artikel 4, nr. 22, i direktiv 2015/2366 om betalingstjenester i det indre marked, uanset om de er indenlandske eller grænseoverskridende

d) En overførsel gennemført ved hjælp af et betalingskort, et elektronisk pengeinstrument eller en mobiltelefon eller andet digitalt udstyr eller IT-udstyr, der anvender teknologi med forud- eller efterbetaling og som har tilsvarende karakteristika om betalingskort mv.

Pengeoverførselsforordningen skelner mellem: betalers betalingsformidler, betalingsmodtagers betalingsformidler og mellembetalingsformidlere. Derudover skelnes der mellem overførsler inden for og uden for EU.

32.3. Indledende overblik over pengeoverførselsforordningen

Udgangspunkt

Udgangspunktet er, at der ved en pengeoverførsel skal medsendes fuldstændige oplysninger om betaler og betalingsmodtager. Der er dog visse undtagelser til oplysningsforpligtelsen.

Undtagelser for betalingsformidlere indenfor EU

Hvis alle betalingsformidlere i relation til en pengeoverførsel er etableret inden for EU, kan der medsendes begrænsede oplysninger om betaler og betalingsmodtager.

Dog kan betalingsmodtagerens betalingsformidler eller mellembetalingsformidleren kræve flere oplysninger i følgende situationer:

1) Hvis pengeoverførslen er over 1.000 euro, kan betalingsmodtagers betalingsformidler eller mellembetalingsformidler kræve fuldstændige oplysninger.
2) Hvis pengeoverførslen er under 1.000 euro, kan betalingsmodtagers betalingsformidler eller mellembetalingsformidler kræve at få oplysninger om som minimum betaler og betalingsmodtagers navn og betalingskontonummer/transaktionsindentifikator.

Undtagelser for betalingsformidlere uden for EU

Hvis en eller flere betalingsformidlere i relation til en pengeoverførsel er etableret uden for EU, gælder der kun en undtagelse, hvis

1) pengeoverførslen er under 1.000 euro, i disse tilfælde kan medsendes begrænsede oplysninger.

Hvis pengeoverførslen derimod er over 1.000 euro, gælder udgangspunktet, og der skal medsendes fuldstændige oplysninger.

Hvad er fuldstændige oplysninger?

1) betalerens navn,
2) betalerens betalingskontonummer (eller transaktionsidentifikator),
3) betalerens adresse, officielle personlige dokumentnummer, kunde-id-nummer eller fødselsdato og –sted,
4) betalingsmodtagerens navn, og
5) betalingsmodtagerens betalingskontonummer (eller transaktionsidentifikator).

Hvad er begrænsede oplysninger?

1) betalerens og betalingsmodtagerens betalingskontonummer, eller
2) en entydig transaktionsidentifikator, hvis de ikke har et betalingskontonummer.

Hvem skal sende oplysningerne?

Betalers betalingsformidler er forpligtet til at kontrollere og medsende de nødvendige oplysninger i forbindelse med en pengeoverførsel for sin kunde.

Hvem skal undersøge, om oplysningerne er tilstrækkelige?

Betalers betalingsformidler skal sikre, at der ikke er mangler i de oplysninger, som medsendes pengeoverførslen.

Betalingsmodtagers betalingsformidler og mellembetalingsformidler skal sikre, at der er medsendt de nødvendige oplysninger med en pengeoverførsel inden en pengeoverførsel kan godkendes.

32.4. Undtagelser i forordningen

Henvisning til pengeoverførselsforordningen: Artikel 2.

Det følger af pengeoverførselsforordningen artikel 2, der vedrører forordningens anvendelsesområde, at visse tjenester ikke er omfattet. For en udtømmende liste over undtagelser, se pengeoverførselsforordningen.

Direktiv 2015/2366 anfører i artikel 3, litra a, -m og o, de tjenester, som pengeoverførselsforordningen ikke finder anvendelse på, herunder er bl.a. oplistet:

1) Betalingstransaktioner, der udelukkende foretages kontant direkte fra betaleren til betalingsmodtageren uden noget mellemled.
2) Betalingstransaktioner fra betaleren til betalingsmodtageren gennem en handelsagent, som ved aftale har tilladelse til at forhandle eller afslutte salg eller køb af varer eller tjenesteydelser på vegne af enten kun betaleren eller kun betalingsmodtageren mv.

Tilsvarende finder pengeoverførselsforordningen ikke anvendelse på pengeoverførsler, der foretages ved hjælp af et betalingskort, et elektronisk pengeinstrument, en mobiltelefon eller lignende, hvis:

1) dette kort, instrument eller udstyr udelukkende anvendes til at betale for varer eller tjenesteydelser,
2) nummeret på dette kort, instrument eller udstyr medsendes ved alle overførsler i forbindelse med transaktionen.

Det betyder omvendt, at hvis et sådant kort, instrument eller lignende derimod kan benyttes til overførsler, der kan foretages "person til person", er sådanne transaktioner med kort, instrumenter og lignende omfattet af pengeoverførselsforordningen.

Hvis virksomheden gør brug af undtagelserne i litra a og b, bør virksomheden derfor have procedurer, der kan fastslå, at en pengeoverførsel ikke er en person-til-person overførsel, men i stedet er en pengeoverførsel, der sker som en betaling for varer eller tjenesteydelser.

Indenlandske pengeoverførsler til en betalingsmodtagers betalingskonto i forbindelse med køb af varer og tjenesteydelser er ikke omfattet af pengeoverførselsforordningen, hvis:

1) modtagerens betalingsformidler er omfattet af hvidvaskloven,
2) denne via entydigt referencenummer kan finde frem til den juridiske eller fysiske person, som leverer varer eller tjenesteydelser, og
3) beløbet ikke overstiger et beløb, der modsvarer værdien af 1.000 euro.

32.5. Betalers betalingsformidlers forpligtelser

Henvisning til pengeoverførselsforordningen: Artikel 4 og 10.

Betalers betalingsformidler skal altid sikre, at der ved en pengeoverførsel medsendes oplysninger om betaler og betalingsmodtager.

Betalers betalingsformidler bør derfor have politikker og forretningsgange der i forhold til betalingsformidlerens forretningsmodel effektivt kan sikre, at betalingsformidleren efterlever pengeoverførselsforordningens krav.

Betalers betalingsformidler skal sikre, at følgende oplysninger om betaleren medsendes:

1) Betalerens navn.
2) Betalerens betalingskontonummer.
3) Betalerens adresse, officielle personlige dokumentnummer, kunde-id-nummer eller fødselsdato og –sted.

Betalers betalingsformidler skal sikre, at følgende oplysninger om betalingsmodtager medsendes:

1) Betalingsmodtagerens navn.
2) Betalingsmodtagerens betalingskontonummer.

Hvis betaleren eller betalingsmodtageren ikke har en betalingskonto, skal betalers betalingsformidler i stedet medsende en entydig transaktionsidentifikator, som gør det muligt at spore pengeoverførslen.

Ved en "entydig transaktionsidentifikator" forstås en kombination af bogstaver, tal eller symboler, fastlagt af betalingsformidleren i overensstemmelse med protokollerne for de betalings-, afviklings- og meddelelsessystemer, der anvendes til at foretage pengeoverførslen.

Kontrol af oplysninger om betaler
Betalers betalingsformidler skal kontrollere de oplysninger om betaler, der skal medsendes, før pengeoverførslen må gennemføres. Kontrollen skal ske ved brug af dokumenter, data eller oplysninger fra en pålidelig og uafhængig kilde.

Betalerens identitet kan kontrolleres på samme måde, som kontrol gennemføres i henhold til hvidvasklovens §§ 10 og 11, der beskriver de kundekendskabsprocedurer, som virksomheder skal gennemføre ved nye kunder og ved etablerede kunder. Se del 3 om kundekendskabsprocedurer.

Det betyder, at betalers betalingsformidlers forretningsgange skal sikre, at de nødvendige oplysninger om betaler bliver kontrolleret og følger med pengeoverførslen fra betaler til betalingsmodtager.

Hvis der indgår en mellembetalingsformidler i pengeoverførslen, skal mellembetalingsformidleren sikre, at de modtagne oplysninger om betaleren og om betalingsmodtageren bliver opbevaret sammen med overførslen.

32.5.1. Pengeoverførsler indenfor EU

Henvisning til pengeoverførselsforordningen: Artikel 5.

Hvis alle betalingsformidlere, der er involveret i betalingskæden, er etableret inden for EU, kan en pengeoverførsel ledsages af begrænsede oplysninger om betaler og betalingsmodtager.

En sådan pengeoverførsel skal som minimum ledsages af:
1) betalerens og betalingsmodtagerens betalingskontonummer, eller
2) en entydig transaktionsidentifikator, hvis de ikke har en betalingskonto.

På trods af muligheden for, at en pengeoverførsel kan ledsages af begrænsede oplysninger, kan betalingsmodtagerens betalingsformidler dog anmode om supplerende oplysninger. Hvilke supplerende oplysninger, som betalingsmodtagerens betalingsformidler kan anmode om, afgøres ud fra, om pengeoverførslen er på et beløb, der overstiger 1.000 euro.

Betalingsformidlere og mellembetalingsformidlere bør have politikker og forretningsgange til at vurdere, om en pengeoverførsel på under 1.000 euro hænger sammen med andre pengeoverførsler, dvs. om de er indbyrdes forbundne og tilsammen overstiger grænsen på 1.000 euro.

Pengeoverførsler kan f.eks. hænge sammen, hvis de henholdsvis fra og til den samme betalingskonto, eller hvis de sendes inden for en kort periode.

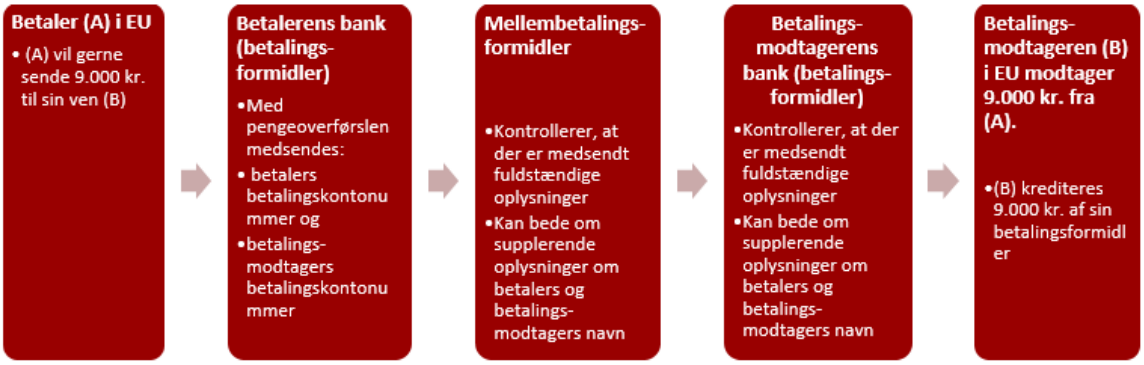
Pengeoverførsel over 1.000 euro
Betalingsmodtagerens betalingsformidler kan kræve, at de fuldstændige oplysninger om betaler eller betalingsmodtager stilles til rådighed inden for en frist på 3 arbejdsdage, hvis pengeoverførslen er på et beløb over 1.000 euro. Se afsnit 32.5 om forpligtelser for betalers betalingsformidler.

Pengeoverførsel under 1.000 euro
Hvis pengeoverførslen er på et beløb under 1.000 euro, kan betalingsmodtagers betalingsformidler indenfor en frist på 3 arbejdsdage kræve, at betalers og betalingsmodtagers navn og betalingskontonummer/transaktionsidentifikator, som minimum stilles til rådighed.

I de tilfælde, hvor pengeoverførslen er under 1.000 euro, har betalers betalingsformidler som udgangspunkt ikke pligt til at kontrollere oplysningerne om betaler.

Betalers betalingsformidler skal dog altid kontrollere oplysningerne, hvis
1) betalerens betalingsformidler har modtaget midlerne, der skal overføres, i kontanter eller i anonyme elektroniske penge, eller
2) betalerens betalingsformidler har en rimelig begrundet mistanke om hvidvask og/eller finansiering af terrorisme.

Eksempel: *processen for en pengeoverførsel, hvor betalingsformidlerne er banker, og hvor betalingsmodtagers betalingsformidler er etableret i EU.*



32.5.2. Pengeoverførsler udenfor EU

Henvisning til pengeoverførselsforordningen: Artikel 6.

For pengeoverførsler til betalingsformidlere, der er etableret uden for EU, skal betalers betalingsformidler altid medsende fuldstændige oplysninger om betaler og betalingsmodtager.

Pengeoverførsler under 1.000 euro
Kravet om, at der skal medsendes fuldstændige oplysninger gælder dog ikke, hvis pengeoverførslen ikke overstiger 1.000 euro.

En sådan pengeoverførsel skal i stedet som minimum ledsages af begrænsede oplysninger:

1) Betaleren og betalingsmodtagerens navn.
2) Betalerens og betalingsmodtagerens betalingskontonummer eller en entydig transaktionsidentifikator, hvis de ikke har en betalingskonto.

I de tilfælde, hvor pengeoverførslen er under 1.000 euro, har betalers betalingsformidler som udgangspunkt ikke pligt til at kontrollere oplysningerne om betaler.

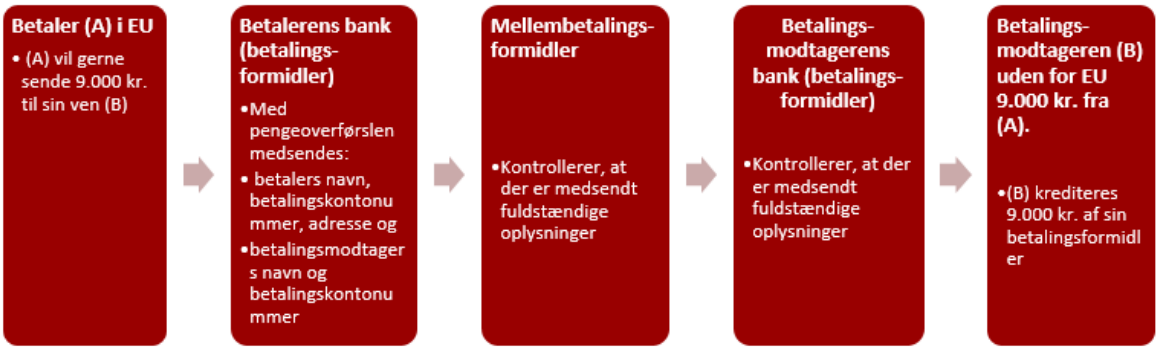
Dog skal betalers betalingsformidler altid kontrollere oplysningerne, hvis

- betalerens betalingsformidler har modtaget midlerne, der skal overføres, i kontanter eller i anonyme elektroniske penge, eller
- betalerens betalingsformidler har en rimeligt begrundet mistanke om hvidvask og/eller finansiering af terrorisme.

Batchfiloverførsel
Hvis en enkelt betaler gennemfører en batchfiloverførsel til en betalingsmodtager uden for EU, finder kravet om at medsende fuldstændige oplysninger om betaler og betalingsmodtager ikke anvendelse på

hver enkelt overførsel i batchoverførslen. I stedet er det afgørende, at batchfilen samlet indeholder de fuldstændige oplysninger og at oplysningerne om betaler er blevet kontrolleret.

Eksempel: *processen for en pengeoverførsel, hvor betalingsformidlerne er banker, og hvor betalingsmodtagers betalingsformidler er etableret uden for EU.*



32.6. Betalingsmodtagers betalingsformidlers forpligtelser

Henvisning til pengeoverførselsforordningen: Artikel 7, 8, 9 og 10.

Betalingsmodtagers betalingsformidler skal konstatere, om der mangler oplysninger om betaler eller betalingsmodtager.

Betalingsmodtagers betalingsformidler er derfor forpligtet til at have effektive forretningsgange, der kan bruges til at konstatere om de oplysninger, der er medsendt, i det system, der anvendes, er udfyldt med tegn eller input i overensstemmelse med det anvendte system. Betalingsformidlerens forretningsgange bør derfor også kunne forhindre eller standse en gennemførelse af en pengeoverførsel, hvis der ikke i forbindelse med pengeoverførslen er anvendt tegn eller input i overensstemmelse med systemet, eller hvis oplysningerne er meningsløse, f.eks. hvis tegnene er tilfældige tegn som ”ABCDEFG”, eller hvis navnet ikke er angivet, men der f.eks. i stedet kun står ”kunde”.

Effektive forretningsgange forudsætter ikke, at der sker en manuel gennemgang. Betalingsformidleren kan eksempelvis have et system, hvori der er angivet en liste med tegn eller ord, der er meningsløse, og som derfor skal medføre, at en overførsel ikke gennemføres eller standses, hvis der medfølger sådanne oplysninger.

Derudover bør betalingsmodtagers betalingsformidler have forretningsgange, der sikrer, at der gennemføres efterfølgende overvågning eller realtidsovervågning, der kan bruges til at konstatere, om der mangler oplysninger om betaler eller betalingsmodtager, f.eks. om der er opgivet betaler og betalingsmodtagers betalingskontonummer eller en entydig transaktionsidentifikator.

Forretningsgangene for overvågningen skal være proportionale i forhold til betalingsformidlerens forretningsmodel og de risici for hvidvask og finansiering af terrorisme, som forretningsmodellen er eksponeret for.

Betalingsformidleren kan også foretage regelmæssige stikprøver af pengeoverførsler, der er blevet gennemført, for at vurdere, om forretningsgangene er effektive.

Ved en direkte debiteringsopkrævning
Det er som udgangspunkt betalers betalingsmodtager, der skal medsende de nødvendige oplysninger med en pengeoverførsel, men hvis pengeoverførslen sker som en direkte debitering, er det betalingsmodtagerens betalingsformidler, der bør sende de nødvendige oplysninger om betaler og betalingsmodtager til betalerens betalingsformidler som en del af den direkte debiteringsopkrævning.

Pengeoverførsler over 1.000 euro
Ved pengeoverførsler på over 1.000 euro skal betalingsmodtagers betalingsformidler, uanset om pengeoverførslen modtages som en eller flere sammenhængende overførsler, altid kontrollere, om de medsendte oplysninger om betalingsmodtageren er korrekte, før betalingsmodtageren krediteres midlerne eller får dem stillet til rådighed. Kontrollen skal foretages på grundlag af uafhængige og pålidelige dokumenter. Bemærk, at kontrollen af betalingsmodtagerens oplysninger allerede bør være foretaget i forbindelse med betalingsformidlerens gennemførelse af kundekendskabsprocedurer på betalingsmodtageren. Se del 3 om kundekendskabsprocedurer.

Pengeoverførsler på ikke over 1.000 euro:
Betalingsmodtagerens betalingsformidler er som udgangspunkt ikke forpligtet til at kontrollere oplysningerne om betalingsmodtageren i henhold til pengeoverførselsforordningen, hvis pengeoverførslen eller flere sammenhængende pengeoverførsler ikke overstiger et beløb på 1.000 euro. Se afsnit 32.5.1 vedrørende en beskrivelse af, hvornår pengeoverførsler er sammenhængende.

Betalingsmodtagers betalingsformidler har dog altid pligt til at kontrollere oplysningerne, hvis:
1) betalerens betalingsformidler har modtaget midlerne, der skal overføres, i kontanter eller i anonyme elektroniske penge, eller
2) betalerens betalingsformidler har en rimelig begrundet mistanke om hvidvask og/eller finansiering af terrorisme.

Manglende eller ufuldstændige oplysninger
Betalingsmodtagerens betalingsformidler skal have risikobaserede forretningsgange til at fastslå, hvorvidt en pengeoverførsel, hvor der mangler oplysninger eller hvor der er medsendt ufuldstændige oplysninger, skal afvises, suspenderes, eller om der skal træffes andre foranstaltninger.

I tilfælde, hvor betalingsmodtagerens betalingsformidler bliver bekendt med, at en pengeoverførsel mangler oplysninger, eller hvor oplysningerne er ufuldstændige, skal betalingsformidleren afvise overførslen eller bede om de manglende oplysninger.

Hvis en betalers betalingsformidler gentagne gange ikke sender de nødvendige oplysninger eller sender ufuldstændige oplysninger med en pengeoverførsel, skal betalingsmodtagers betalingsformidler træffe foranstaltninger i form af udsendelse af advarsler og fastsættelse af frister for at modtage oplysninger og herefter tage stilling til, om fremtidige pengeoverførsler fra den pågældende betalingsformidler skal begrænses eller afvises.

Betalingsmodtagerens betalingsformidler indberetter undladelsen og de trufne foranstaltninger til den relevante tilsynsmyndighed, som fører tilsyn med den pågældende virksomheds overholdelse af hvidvaskloven.

32.7. Mellembetalingsformidlers forpligtelser

Henvisning til pengeoverførselsforordningen: Artikel 10, 11, 12 og 13.

Mellembetalingsformidler skal sikre, at samtlige oplysninger, der medsendes en pengeoverførsel, opbevares sammen med overførslen.

Mellembetalingsformidler skal, ligesom betalingsmodtagers betalingsformidler, have effektive forretningsgange til:

1) at konstatere, om de oplysninger, der medsendt i det system, der anvendes, er udfyldt med tegn eller input i overensstemmelse med det anvendte system,
2) at sikre, at de modtagne oplysninger, der er medsendt, opbevares sammen med overførslen, og
3) at sikre, at der gennemføres efterfølgende overvågning eller realtidsovervågning, der kan bruges til at konstatere, om der mangler oplysninger om betaler eller betalingsmodtager.

Se afsnit 32.6 om betalingsmodtagers betalingsformidler.

Der gælder de samme regler for mellembetalingsformidler ved pengeoverførsler, hvor betaler eller betalingsmodtagers betalingsformidler er etableret uden for EU og for batchfiloverførsler, se afsnit 32.5.2.

Bilag 1

Eksempel på en proces til udarbejdelse af en risikovurdering

Eksemplet er ikke bindende. Det er derfor frit for virksomheder og personer, som er omfattet af hvidvaskloven, hvordan de udarbejder en risikovurdering.

Nedenstående eksempel viser trin, som en virksomhed eller person (i det følgende *virksomhed*) kan følge i udarbejdelsen af virksomhedens risikovurdering. Det er dog vigtigt, at den enkelte virksomhed selv dokumenterer, hvordan den har vurderet sine risici, og at virksomheden selv beslutter, hvilke tiltag, der skal iværksættes som følge af risikovurderingen.

1) Indsamling af intern og ekstern data til vurdering af de forskellige risikofaktorområder
    a) Virksomheden skal dokumentere/begrunde sine vurderinger i interne oplysninger og i eksterne relevante risikovurderinger, rapporter, vejledninger mv.
2) Identificer de iboende risici i virksomhedens forretningsmodel
    a) Hvilke risici er der for, at virksomheden kan misbruges til hvidvask og finansiering af terrorisme i forhold til blandt andet følgende risikofaktorer:
        i. kunder
        ii. produkter, tjenesteydelser og transaktioner
        iii. leveringskanaler
        iv. lande og geografiske områder
3) Vurder størrelsen og karakteren af de iboende risici – eksempelvis ved at vægte dem ud fra en fastsat skala
    a) Dette kan f.eks. ske ved at foretage en vurdering af sandsynligheden for misbrug og konsekvensen af misbrug placeret i en skala, der vægter, om den konkrete risiko er begrænset, mellem eller høj i forhold til sandsynlighed og konsekvens.
    b) Vægtningen kan ske individuelt for hver risikofaktor, så virksomheden kan se, hvor risiciene er størst.
4) Resultat af risiciene i virksomhedens risikofaktorer
    a) Virksomheden kan konkludere på risikoniveauet for hver af de under punkt 2 oplistede risikofaktorer, f.eks. ved at udregne en score for hver risikofaktor.