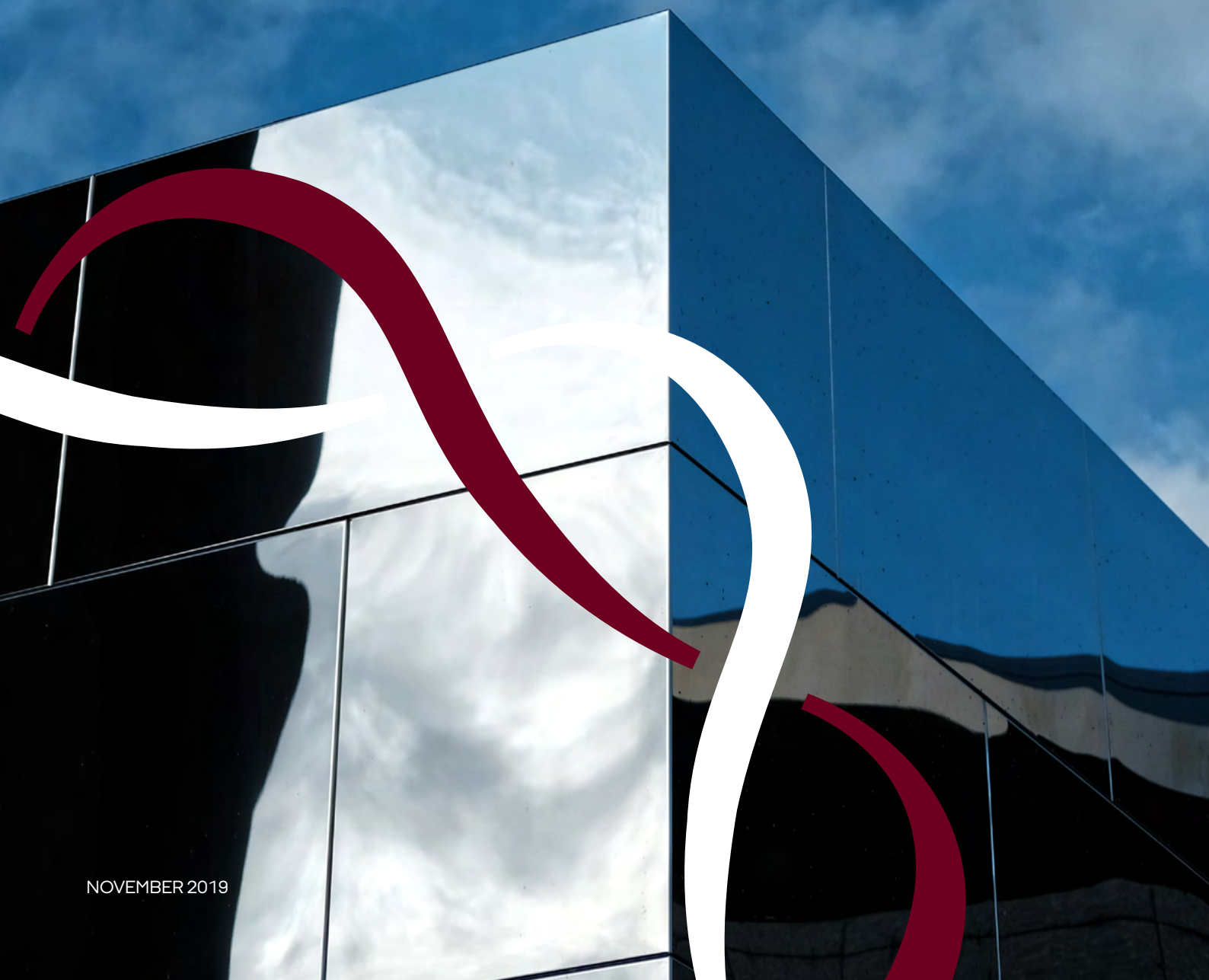
FINANS DANMARK

Afrapportering fra Finans Danmarks Hvidvask Task Force

Finanssektorens indsats mod hvidvask og terrorfinansiering



NOVEMBER 2019

INDHOLD

FORORD

Sager om finansiel kriminalitet i relation til hvidvask og terrorfinansiering har i de senere år præget avisernes forsider og været topindslag i nyhedsudsendelserne. Med god grund. Det har på den baggrund været nødvendigt, at både finansielle virksomheder, myndigheder og samfund tog affære.

På Finans Danmarks årsmøde i 2018 gik den samlede finansielle sektor sammen om at løse en bunden opgave: Vi skal være blandt verdens bedste til at opdage og bekæmpe hvidvask og terrorfinansiering for at muliggøre, at der slås ned på de kræfter, der misbruger pengeinstitutterne til kriminelle formål. De enkelte virksomheder i sektoren arbejder hver dag for at sikre, at vi når den ambition. På ryggen af deres individuelle indsats fik Finans Danmark mandat til at iværksætte en målrettet fælles indsats, som blandt andet inkluderede nedsættelsen af Finans Danmarks Hvidvask Task Force, som består af interne repræsentanter fra sektoren samt fire eksterne eksperter. Hvidvask Task Forcen har nu arbejdet i 11 måneder, og resultatet er denne rapport med tilhørende anbefalinger til sektoren til den fremtidige bekæmpelse af finansiel kriminalitet. Disse anbefalinger skal ses i forlængelse af og som supplement til de initiativer, som pengeinstitutterne allerede har igangsat enkeltvis og sammen, samt de initiativer som er foretaget politisk på Christiansborg og i EU i form af hvidvaskpakker og generel øget regulering. For Hvidvask Task Forcen har det været et centralt omdrejningspunkt at erstatte silotænkning med samarbejde og at knytte samfundsværktøjer til pengeinstitutternes samfundsopgave i relation til hvidvask og terrorfinansiering. Dette vil være afspejlet i anbefalingerne.

Bekæmpelse af hvidvask og terrorfinansiering er et helt centralt tema på den finansielle sektors dagsorden i årene fremover. Med Hvidvask Task Forcens anbefalinger er vi ét skridt videre i kampen mod de finansielle kriminelle. Og med disse konstruktive initiativer, som blandt andet indebærer konkrete anbefalinger til både sektor og myndigheder, herunder nye fælles it-løsninger, en ny fortrolig efterretningsenhed (FEHT), adfærdsprincipper, bedre uddannelse og øget transparens mener vi, at scenen er sat til en endnu stærkere indsats på tværs af sektor, myndigheder og samfund.

Med disse anbefalinger ønsker sektoren at gå foran – og vi ser frem til en fortsat konstruktiv dialog om anbefalingerne til bekæmpelse af hvidvask og terrorfinansiering.

God læselyst.

Linda Nielsen, formand for Hvidvask Task Forcen og
Michael Rasmussen, formand for Finans Danmark.

INDLEDNING

Kommissorium for Hvidvask Task Forcen

I kølvandet på en række sager om hvidvask søsætter Finans Danmark en Task Force, som skal undersøge og komme med anbefalinger til, hvordan indsatsen imod hvidvask og terrorfinansiering fremadrettet styrkes gennem fælles initiativer og løsninger på tværs af den finansielle sektor. Anbefalingerne skal sammen med pengeinstitutternes egne interne initiativer danne grundlag for et tættere samarbejde med myndighederne og sikre en klar, koordineret og konsistent kommunikation med hensyn til udfordringer og løsninger. Den finansielle sektor skal i enhver sammenhæng demonstrere, at den arbejder seriøst og koordineret for at sikre den bedst mulige indsats, som skal højne bevidsthed, kvalitet og effektivitet i enhver del af sektoren.

Fire hovedspor

Task forcens arbejde deles i fire hovedspor, som sætter rammen for arbejdet.

1. Fælles it-løsninger

Hvidvask Task Forcen skal undersøge muligheden for et styrket samarbejde om fælles it-løsninger, der forbedrer kvalitet og effektivitet i bekæmpelsen af hvidvask og terrorfinansiering. Mulighederne for en samlet sektorløsning ved onboarding af kunder – såvel private som erhvervskunder – skal analyseres. Tilsvarende skal ske i forhold til etableringen af det lovpligtige fælles bankkontoregister, hvor der skal bidrages med idéer og løsninger til fælles gavn for samfundet, myndighederne og sektoren. De fælles løsninger skal tage højde for konkurrenceretlig og persondataretlig regulering.

2. Øget samarbejde med myndighederne

Hvidvask Task Forcen skal undersøge mulighederne for et øget samarbejde med myndighederne. Der afholdes allerede på nuværende tidspunkt en række møder med Finanstilsynet, SØIK, PET, Erhvervsministeriet og andre myndigheder, såvel i regi af Finans Danmark som bilateralt mellem de større pengeinstitutter og myndighederne. Det skal vurderes, hvordan samarbejdet med myndighederne bedst kan optimeres, herunder hvilke initiativer der konkret kan igangsættes for at sikre, at sektoren og myndighederne sammen kan yde en effektiv og koordineret indsats i bekæmpelsen af hvidvask og terrorfinansiering. I den forbindelse vil Hvidvask Task Forcen i samarbejde med myndighederne se på mulighederne for inspiration fra udlandet – blandt andet England og Holland – hvor der især for Englands vedkommende er et meget velfungerende samarbejde i JMLIT (Joint Money Laundering Intelligence Taskforce).

3. Selvregulering og etik

Hvidvask Task Forcen skal undersøge rammer, erfaringer og mulighed for brug af selvregulering og etiske guidelines. Erfaringer fra blandt andet Sverige og Holland i forhold til guidelines og branchekodeks vil blive anvendt som inspiration.

4. Certificering

Hvidvask Task Forcen kan også se på mulighederne for at skabe fælles rammer for certificering af medarbejderne i de danske pengeinstitutter i henhold til bekæmpelse af hvidvask.

Hvidvask Task Forcen kan også tage andre temaer op, som den finder relevant[1]. Arbejdet afsluttes i Q4 2019, hvor anbefalingerne tilgår Finans Danmarks bestyrelse. Finans Danmarks Hvidvask Task Force består af en række interne repræsentanter fra pengeinstitutterne samt fire eksterne eksperter. Hvidvask Task Forcen har derudover haft sekretariatsassistance i Finans Danmark.

[1] *Det vil senere fremgå af rapporten, at Hvidvask Task Forcen har ønsket et spor om øget transparens i sektoren. Dette vil udgøre hovedspor 5 i rapporten.*

Medlemmer af Finans Danmarks Hvidvask Task Force

Eksterne eksperter

- Formand: Linda Nielsen, professor, Juridisk Fakultet, Københavns Universitet
- Lars Krull, seniorrådgiver, Aalborg Universitet
- Per Gunslev, statsautoriseret revisor og forhenværende partner, EY
- Anne Birgitte Gammeljord, advokat, Rovsing & Gammeljord

Interne repræsentanter fra sektoren

- Carsten Egeriis, Chief Risk officer, Danske Bank,
- Anders Jensen, koncerndirektør, Nykredit
- Anita Nedergaard, Country AML Responsible, Nordea Denmark
- Bo. A. Christensen, direktør forretningsservice, Jyske Bank
- Lene Lorentzen, hvidvaskansvarlig, Sydbank
- Karin Duerlund, juridisk direktør, Spar Nord
- Anders Balle Rasmussen, områdedirektør, Sparekassen Kronjylland
- George Wenning, juridisk direktør, LOPI

Sekretariat

- Ulrik Nødgaard, administrerende direktør, Finans Danmark
- Kjeld Gosvig-Jensen, juridisk direktør, Finans Danmark
- Stine Luise Goll, kommunikationsdirektør, Finans Danmark
- Jens Kasper Rasmussen, chefkonsulent, Finans Danmark
- Cecilie Sander Bernbom, seniorkonsulent, Finans Danmark
- Camilla Thorning, pressechef, Finans Danmark

PIXI-UDGAVE AF ANBEFALINGERNE

25 konkrete forslag til bekæmpelse af hvidvask og terrorfinansiering - med samfundskontrakten skal der følge samfundsværktøjer

Hvidvask Task Forcen har i sit arbejde de forgangne 11 måneder kortlagt, analyseret og debatteret den finansielle sektors rolle og indsats i relation til bekæmpelse af hvidvask og terrorfinansiering. Arbejdet har været centreret omkring fire spor fastsat i kommissoriet samt et tilvalgt spor (øget transparens) efter ønske fra Hvidvask Task Forcen.

Resultatet af det intensive arbejde er 25 konkrete anbefalinger til pengeinstitutter, Finans Danmark, myndigheder og samfund. Hvidvask Task Forcens udgangspunkt har været, at pengeinstitutterne i styrket grad skal leve op til samfundskontrakten og de forventninger, som samfundet med rette har til, at den finansielle sektor går foran i indsatsen. Det har i den kontekst været afgørende for Hvidvask Task Forcen samtidig at levere anbefalinger til, hvordan den finansielle sektor får de nødvendige redskaber og ressourcer til at løfte opgaven – også fra samfundets side. Populært kan man sige, at med en defineret samfundsopgave bør følge konkrete samfundsværktøjer.

De 25 anbefalinger kommer vidt omkring og forpligter både sektor, brancheorganisation, myndigheder og samfund. Størstedelen af anbefalingerne er løsninger skitseret til implementering i sektoren og i Finans Danmark. Af de mest omfattende anbefalinger kan nævnes: Sektorfælles vision for it-samarbejde 2025, fælles efterretningsenhed for hvidvask - og terrorfinansiering, 6 adfærdsprincipper, uddannelsessamarbejde og erfaringsudveksling, informationsoplysning til samfundet, årlig konference og rapport, som kortlægger omfanget og indsatsen, kontrol af bankbokse, støtte til whistleblowere, dybdegående evaluering af hvidvaskunderretninger, samarbejde med Hvidvasksekretariatet i SØIK, og øget fokus på EU-samarbejdet.

Læs de 25 anbefalinger i kort oprids her:

Hovedspor 1: Fælles it-løsninger

1. Fem konkrete it-projekter på anti-money laundering (AML)

- Task Forcen anbefaler, at der etableres et bredere samarbejde, når det gælder fælles it-løsninger med hensyn til hvidvaskbekæmpelse (AML) – og bredere bekæmpelse af økonomisk kriminalitet
- Task Forcen anbefaler på den baggrund gennemførelsen af fem konkrete it-projekter på AML:

1. KYC (kend din kunde): Ny fælles standard for kundekendskabsprocedurer
2. Pasvalidering: Ny løsning som validerer match mellem CPR- og pasnummer
3. Fælles PEP/RCA-register: Nyt fælles register, som forankres i myndighedsregi
4. Fælles dataregister: Register på de tre ovenstående initiativer
5. Kontoopslagsportal: Portal over hvem der ejer bankkonto eller bankboks

2. Vision om sektorfælles it-samarbejde 2025

- Task Forcen anbefaler, at der hurtigst muligt igangsættes et forprojekt, der kortlægger præcis, hvad det vil kræve at realisere visionen for sektorfælles it-samarbejde 2025. Et langsigtet vidtgående sektorfælles AML/CTF-samarbejde er meget ambitiøst, og der skal i processen løses mange tekniske og regulatoriske udfordringer. Det vil fx kræve en ændret lovgivning, for at pengeinstitutter kan dele kundedata.
- Task Forcen anbefaler, at det på baggrund af kortlægningen undersøges, om det er muligt at oprette en sektorfælles enhed, der strømliner indsamlingen, verifikationen, opbevaringen og delingen af data og dokumenter, som understøtter sektorens AML/CFT-procedurer og processer. Formålet er at bekæmpe og forebygge hvidvask og finansiering af terrorisme ved hjælp af digitale og datadrevne løsninger.
- Task Forcen anbefaler, at visionen for sektorfælles it-samarbejde kobles tæt til anbefalingen om øget samarbejde med myndighederne, herunder "Den Fælles Efterretningsenhed for Hvidvask og Terrorfinansiering" (anbefaling nr. 4).

Hovedspor 2: Øget samarbejde med myndighederne

3. Dilemmaerne skal frem i lyset

- Task Forcen anbefaler, at sektoren og samfundet i fællesskab drøfter dilemmaerne i indsatsen til bekæmpelse af hvidvask og terrorfinansiering ud fra afvejninger baseret på oplysningernes karakter sammenholdt med kriminalitetens karakter og ser på, hvordan man kan optimere det generelle samarbejde, herunder den generelle informationsudveksling, og på mulighederne for at udveksle oplysninger i konkrete sager.

4. Dansk JMLIT: Den Fælles Efterretningsenhed for Hvidvask og Terrorfinansiering (FEHT)

- Task Forcen anbefaler, at "Den Fælles Efterretningsenhed for Hvidvask og Terrorfinansiering" (FEHT) nedsættes med repræsentanter fra pengeinstitutter, politi, FE, PET og Skattestyrelsen.
- Task Forcen anbefaler, at der indføres en særskilt bestemmelse i hvidvaskloven, der inden for rammerne af persondataforordningen og lov om finansiel virksomhed giver hjemmel til, at myndighederne nedsætter FEHT'en, hvor det med behørige sikkerhedsforanstaltninger er tilladt at udveksle fortrolige oplysninger, når det gælder de „store fisk" og sager som har større samfundsmæssig betydning.

5. HvidvaskForum

- Task Forcen anbefaler, at HvidvaskForum gøres til et forum, der ikke kun understøtter videndeling og erfaringsudveksling, men også i lige så høj grad er med til at sikre en reel holistisk tilgang på tværs af myndigheder i form af fx fælles prioritering i tilsynsindsatsen.

6. Datatilsynet

- Task Forcen anbefaler, at Datatilsynet i højere grad inddrages i HvidvaskForum og HvidvaskForum+.

7. Digitaliseringsstyrelsen og Udbetaling Danmark

- Task Forcen anbefaler, at det overvejes, om Digitaliseringsstyrelsen og Udbetaling Danmark skal inddrages i HvidvaskForum og HvidvaskForum+.

8. Kvartalsrapport og feedback på underretninger fra Hvidvasksekretariatet i SØIK

- Task Forcen anbefaler, at Hvidvasksekretariatet ser på måder til i højere grad at kunne give feedback på de underretninger, som sektoren sender til myndighederne.

Hovedspor 3: Uddannelse

9. Casebaseret uddannelse og erfaringsudveksling

- Task Forcen anbefaler, at der for medarbejdere på hvidvaskområdet etableres kurser med erfaringsudveksling, casearbejde og dilemmaer.

10. Halvårlige konferencer med fokus på erfaringsudveksling

- Task Forcen anbefaler, at Finans Danmark afholder halvårlige konferencer med mulighed for erfaringsudveksling på området. På denne måde kan der igangsættes en udvikling, der kan medvirke til øget ensartethed i praksis.

Hovedspor 4: Adfærdsprincipper

11. Seks adfærdsprincipper

- Task Forcen anbefaler 6 adfærdsprincipper til sektoren i arbejdet i relation til bekæmpelse af hvidvask og terrorfinansiering.

12. Fokus på kultur og transparens

- Task Forcen anbefaler at sektoren med adfærdsprincipperne sætter fokus på, at etik altid bør komme før profit, at behovet for at blive kigget i kortene anerkendes, og at der arbejdes målrettet med virskomhedskulturen.

13. Tone fra toppen og ned gennem organisationen

- Task Forcen anbefaler at sektoren med adfærdsprincipperne sætter fokus på at sikre tonen fra toppen, samt at alle led i organisationen betoner vigtigheden af bekæmpelse af hvidvask og terrorfinansiering.

Hovedspor 5: Øget transparens

14. Ledelsesberetning

- Task Forcen anbefaler, at de enkelte pengeinstitutter forpligter sig til i deres ledelsesberetning at redegøre overordnet for, hvordan de arbejder med bekæmpelse af hvidvask og terrorfinansiering, herunder deres hvidvaskpolitik.

15. Dedikeret hjemmeside

- Task Forcen anbefaler, at pengeinstitutterne på deres hjemmeside opretter en dedikeret side, hvor de målrettet og tilgængeligt for den brede offentlighed kan oplyse, hvordan de arbejder med bekæmpelse af hvidvask og terrorfinansiering.

16. Årlig konference

- Task Forcen anbefaler, at Finans Danmark årligt afholder en konference, der tematiserer nogle af de udfordringer og dilemmaer, der er i forhold til finansiel kriminalitet.

17. Årsrapport

- Task Forcen anbefaler, at Finans Danmark årligt udarbejder en rapport, der går mere i detaljen i forhold til sektorens arbejde på området, herunder beskriver udviklingen i antal underretninger, brug af ressourcer, ansatte mv. i sektoren.

18. Informationsoplysning

- Task Forcen anbefaler, at Finans Danmark øger informationsmaterialet til pengeinstitutternes kunder og til samfundet, hvor der nærmere redegøres for, hvad pengeinstitutterne gør på området, og hvilke krav der er i forhold til pengeinstitutterne, herunder i forhold til indhentelse af kundeoplysninger, og hvad de skal bruges til. Dette kan gøres ved informationskampagner, brug af sociale medier, pjecer og direkte brev/mail til pengeinstitutternes kunder.

Yderligere initiativer

19. Støtte til whistleblowere

- Task Forcen anbefaler, at de respektive bestyrelser - udover at sikre whistleblowerordninger i alle banker – overvejer, hvordan whistleblowere kan understøttes, f.eks. ved at bistå med advokatbistand.

20. Samarbejde med SØIK

- Task Forcen anbefaler, at sektoren i form af "Den Fælles Efterretningsenhed for Hvidvask og Terrorfinansiering" stiller medarbejdere til rådighed i et udvekslingsforløb med fokus på videndeling for en periode af op til 3 måneder.

21. Evaluering af underretninger til Hvidvasksekretariatet i SØIK

- Task Forcen anbefaler, at sektoren årligt evaluerer

pengeinstitutternes underretninger i samarbejde med Hvidvasksekretariatet i SØIK med det formål at sikre, at de har den rette kvalitet i forhold til at undersøge mistænkelige forhold og at undgå, at sektoren sender unødvendige underretninger.

22. Bankbokse

- Task Forcen anbefaler, at sektoren indsamler et overblik over bankbokse. Baggrunden for at fokusere på bankbokse er, at de kan bruges til at opbevare kriminelt hittegods, narkotika, sorte penge eller andet.
- Task Forcen anbefaler derefter, at sektoren ser nærmere på, hvordan der kan etableres et betryggende niveau af foranstaltninger og processer, når pengeinstitutterne udbyder denne service.
- Task Forcen anbefaler ydermere, at sektoren indgår i en dialog med Finanstilsynet om, hvad vejledningen til sektoren bør være i forhold til effektivt at overvåge bankbokse som led i kravene om kundekendskabsprocedurer og overvågning.

23. Bankforum under HvidvaskForum+

- Task Forcen anbefaler som et supplerende politisk initiativ, at der ud over HvidvaskForum for myndighederne og HvidvaskForum+ for myndigheder og brancheorganisationer – etableres et Bankforum med fokus på pengeinstitutter med deltagelse fra Finans Danmark og repræsentanter fra medlemsvirksomheder. Et sådant forum vil give mulighed for en detaljeret og sektorspecifik videndeling fra begge sider, og samtidig vil det give rum for konkrete drøftelser.

24. EU+

- Task Forcen anbefaler, at Finans Danmark arbejder for, at det i den fremadrettede EU-regulering indsættes som en eksplicit mulighed, at medlemslandene kan etablere et organ lig "Den Fælles Efterretningsenhed for Hvidvask og Terrorfinansiering (FEHT), og at det muliggøres, at disse nationale enheder kan udveksle informationer med hinanden på tværs af grænserne.

25. Vejledning til hvidvaskloven

- Task Forcen anbefaler et fortsat fokus på, at der til hvidvasklovgivningen følger vejledning, der er aktuel, og som særligt underbygger de regelområder, hvor anden lovgivning krydser med hvidvasklovgivningen samt yderligere vejledning om konkrete situationer, hvor der er sparsom vejledning af finde i reglernes forarbejder.

HVIDVASK OG TERRORFINANSIERING
– HVEM, HVAD OG HVOR MEGET?

Hvidvask som begreb bliver brugt i mange sammenhænge og blev tilmed i 2018 kåret som årets ord i Danmark. Terrorfinansiering har ikke fået lige så meget omtale, men er et indsatsområde, der er mindst lige så vigtigt. Men hvad dækker begreberne egentlig over, og hvem er de kriminelle? Afgrænsningen er vigtig for at få en forståelse af, hvor bredspektret en indsats, der er behov for, for at komme hvidvask, terrorfinansiering og dermed finansiel kriminalitet til livs, og hvor stor og ressourcekrævende en opgave det egentlig er.

Hvem er de finansielle kriminelle?

Er det de finansielle kriminelle, der hvidvasker penge gennem pengeinstitutter – eller er det pengeinstituttet, som hvidvasker pengene for de kriminelle? Og er der forskel? Det kan man til tider komme i tvivl om, når man læser den dækning, der har været af fx hvidvakssagerne.

Overordnet er det vigtigt at forstå, at hvidvask og terrorfinansiering kan begås af både det, man populært kan kalde små og store fisk. I forhold til hvidvask er det fx ikke kun professionelle kriminelle som narkokarteller, terrorister og it-svindlere, der forsøger at hvidvaske ulovlige midler. Det kan også være små fisk som den lokale håndværker, der indsætter indtægter fra sort arbejde, eller en pensionist der begår socialt bedrageri, så ældrechecken kan stige. Hvidvask og terrorfinansiering straffes nu efter straffeloven.

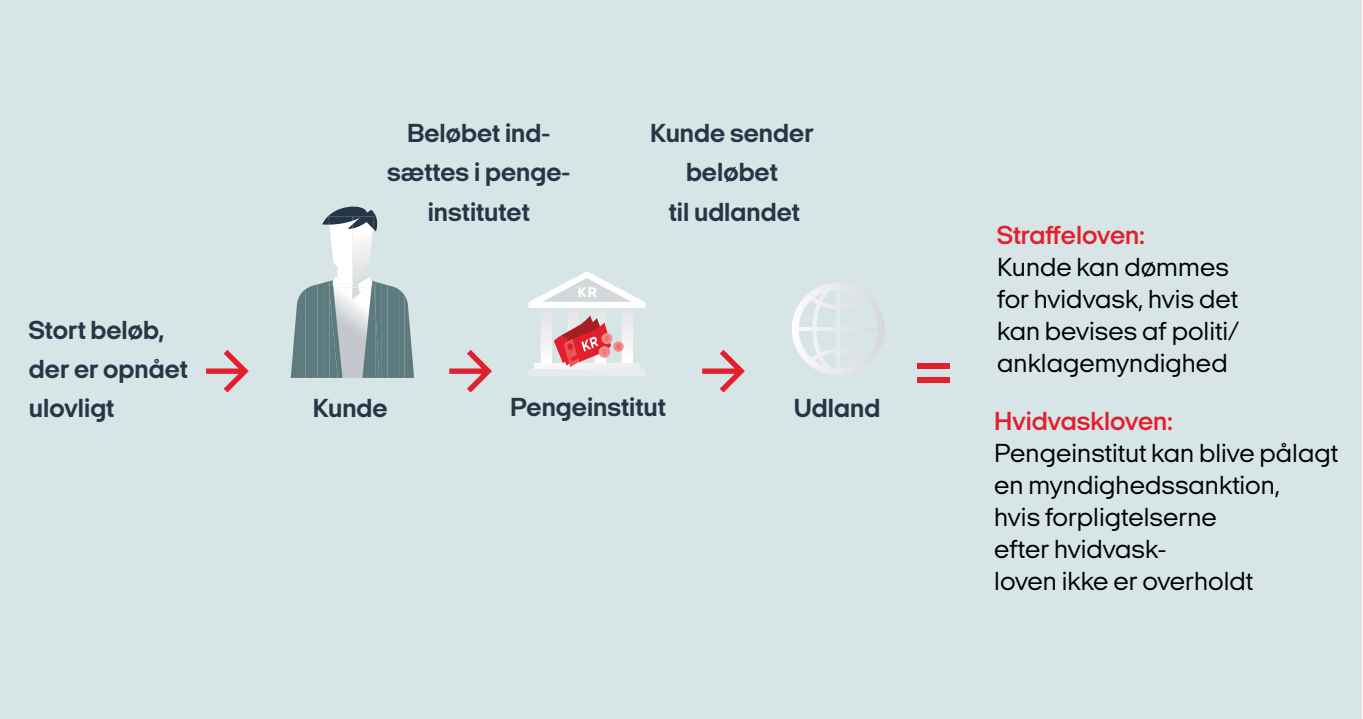
Pengeinstitutternes rolle

Hvad er så pengeinstitutternes rolle? Pengeinstitutterne er en del af samfundets "dørvogtere" (gatekeepers) i den forstand, at de først og fremmest skal søge at spotte og underrette myndighederne om kunder, der ønsker at hvidvaske penge eller bidrage til terrorfinansiering, ligesom de i form af "overvågning og opfølgning" skal undersøge, om kunder forsøger at hvidvaske penge eller foretage terrorfinansiering. Pengeinstitutterne skal kort sagt beskytte indgangen til det finansielle system.

Det er ikke en enkel opgave. For at kunne varetage disse formål er der i hvidvaskloven fastsat en lang række krav til pengeinstitutterne. Disse omfatter regler, der skal sikre, at sektoren har tilstrækkelige foranstaltninger, der forebygger og bekæmper hvidvask og terrorfinansiering. Hvidvaskloven fastslår fx, at pengeinstitutterne skal udarbejde en risikovurdering af deres forretning ud fra input fra myndigheder og egne erfaringer. På den baggrund skal pengeinstitutterne udarbejde politikker og forretningsgange, og bekæmpelsen af hvidvask og terrorfinansiering skal være en del af den løbende kundehåndtering og udførelse af transaktioner mv.

[2]*Kilde: Straffelovens §§ 290 og 290 a og § 114 b*

Figur 1 Case: Sondringen mellem straffeloven og hvidvaskloven



Kilde: Straffelovens §§ 290 og 290 a og § 114 b

Pengeinstituttets opgave er således at opdage den mistænkelige adfærd eller aktivitet, undersøge om mistanken kan afkræftes, og hvis ikke så foretage underretning til Hvidvasksekretariatet hos Statsadvokaten for Særlig Økonomisk og International Kriminalitet (SØIK) og i visse tilfælde standse transaktionen.

En sidste vinkel på pengeinstitutternes rolle er, at hvidvasktransaktioner i den finansielle sektor nogle gange får lov at ske decideret af hensyn til samfundsindsatsen mod finansiel kriminalitet. Det vil være, når myndighederne beder om at lade en kunde fortsætte i pengeinstituttet efter en underretning, fx for at efterforskningen af større sagskomplekser ikke bliver forstyrret og for at få bevismateriale til straffesager mod de kriminelle. Pengeinstitutterne kan også i andre forbindelser bistå myndighederne i deres indsats samt formidle advarsler og anden viden til kunderne, som skærper deres opmærksomhed på at forebygge finansiel kriminalitet og derved forbedre det samlede samfundsforsvar.

Sondring mellem overtrædelser af straffeloven og hvidvaskloven

Hvidvask og terrorfinansiering er strafbelagt i straffeloven. Den person, der er skyldig i hvidvask eller terrorfinansiering, straffes ikke efter hvidvaskloven men efter straffeloven[2]. Det er en vigtig sondring, idet egentlig hvidvask eller terrorfinansiering kræver både en kriminel hensigt og en aktiv handling, som straffes. Hvis et pengeinstitut er klar over, at midler stammer fra kriminalitet eller skal bruges til terror, og alligevel bistår med transaktioner uden at underrette myndighederne, vil pengeinstituttet (og de tilknyttede personer, som har udført handlingerne med samme viden og hensigt) kunne straffes for medvirken efter straffeloven.

I hvidvaskloven er det forpligtelserne til at have et stærkt beredskab, der er i fokus. Loven kriminaliserer ikke forsættet til at begå hvidvask eller terrorfinansiering og heller ikke medvirken hertil, disse forhold er omfattet af straffeloven.

Overtrædelse af hvidvaskloven afhænger heller ikke af, om der faktisk er begået hvidvask eller terrorfinansiering eller ej. Det er en mere skønsbaseret vurdering af, at en omfattet virksomhed, fx et pengeinstitut, ikke har det tilstrækkelige beredskab mod, at pengeinstituttet kan blive brugt til hvidvask eller terrorfinansiering og derfor ikke lever op til sine forpligtelser. Har et pengeinstitut ikke levet op til hvidvasklovens krav om risikovurderinger, overvågninger m.v., har pengeinstituttet derfor ikke hvidvasket penge, men pengeinstituttet kan have skabt et muligt hul for kunder til at bruge pengeinstituttet som et led i kundens egen kriminalitet.

Udfordringen i at hindre de kriminelle i at bruge det finansielle system opstår blandt andet i pengeinstituttets møde med og senere overvågning af sine kunder. Pengeinstitutterne skal afvise en kunde, hvis kundens identitet ikke kan identificeres og kontrolleres. Men det er ikke altid, at en finansiel kriminel kunde starter med at være kriminel. Lidt populært sagt er det en sjældenhed, at kunder ankommer til pengeinstituttet og ligner en virkelig udgave af Andebys Bjørnebande.

Hvis en (finansiel kriminel) kunde ønsker et kundeforhold med produkter, som svarer til den sammenlignelige kunde og desuden er samarbejdsvillig og viser en økonomi og et transaktionsmønster, der kan forventes for den sammenlignelige kunde, er pengeinstituttet typisk ikke i stand til at opfange den kriminelle hensigt hos kunden. På det senere tidspunkt, hvor kundens adfærd synligt fremstår usædvanlig og mistænkelig, vil pengeinstituttet allerede være blevet udnyttet til den kriminelles aktivitet. Uden pengeinstituttet har et ønske om at være det. Tværtimod.

Hvidvask

Hvad dækker hvidvask og terrorfinansiering over? Hvidvaskbegrebet er et bredt begreb, fx dækker det over, når man uberettiget anskaffer sig, modtager eller opbevarer økonomisk udbytte, som man ikke er berettiget til. Hvidvaskbegrebet i hvidvasklovgivningen omfatter også skatteunddragelse, og da der ikke er en nedre grænse for begrebet, omfattes som nævnt også socialt bedrageri og betaling for sort arbejde.

Hvidvask er defineret i hvidvaskloven 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.

4. Omfatter også dispositioner foretaget af den, der har begået den strafbare lovovertrædelse, som udbyttet eller midlerne hidrører fra.

Hvidvask kan blandt andet ske ved, at ulovlige midler anbringes i det finansielle system og sløres ved at foretage transaktioner. På den måde kan midlerne skilles fra den oprindelige kilde og herefter ved efterfølgende anvendelse, kan midlerne ende med at fremstå som lovlige. Dette kunne være ved at indsætte sort tjente penge blandet med legitime "rene" penge på en konto i et pengeinstitut for efterfølgende at sende dem til flere udenlandske konti, eller ved at købe en genstand af større værdi for sorte penge for efterfølgende at sælge genstanden, således at overskuddet herefter fremstår lovligt.

Figur 2 Hvidvask i praksis

	Eksempel A	Eksempel B	Eksempel C
Anbringelse Det ulovlige udbytte anbringes. Det kan f.eks. være i det finansielle system.	Indbetaling af kontanter i et pengeinstitut (evt. blandet med midler fra lovlig virksomhed).	Udførsel af kontanter til udlandet.	Anvendelse af kontanter til køb af højværdivarer, fast ejendom eller aktiver til erhvervsvirksomhed.
Sløring Det ulovlige udbytte adskilles fra dets kilde. Det kan f.eks. ske gennem (finansielle) transaktioner.	Elektronisk overførsel til udlandet (ofte ved brug af selskaber uden reel aktivtet, eller midlerne maskeres som udbytte fra lovlige forretninger).	Indsættelse af kontanter i et pengeinstitut i udlandet.	Salg af de købte varer/aktiver.
Anvendelse Det ulovlige udbytte tilbageføres til gerningsmanden. Det kan f.eks. være tilbageførsel i en form, hvor udbyttet er ændret til midler eller aktiver, der ser ud til at være lovlige.	Tilbageførsel som betaling for (fiktive) lån eller betaling af (fiktive) fakturaer.	Et kompliceret net af overførsler nationalt og internationalt, der gør det næsten umuligt at spore midlernes oprindelige kilde.	Indtægt fra fast ejendom eller virksomhed, der fremstår som lovlig.

Kilde: anklagemyndigheden.dk/da/hvidvask[3].

Formålet med de meget omfattende regler om hvidvask er først og fremmest på globalt plan at medvirke til at bekæmpe meget alvorlig kriminalitet, herunder menneskehandel, narkokriminalitet, terror o.l. (store fisk). Dette er baggrunden for de meget omfattende og strenge regler herom i fx USA og EU. Hvidvask omfatter imidlertid også andre former for finansiel kriminalitet (små fisk).

Straffelovens § 114 b definerer finansiering af terrorisme som den, 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.

Det gælder fx "sort arbejde" hvor der ikke betales den pligtige skat af ydelser. Et andet eksempel er "socialt bedrageri", hvor pengeinstituttet benyttes til at flytte rundt på midler, således at de formelle betingelser for at opnå en social ydelse, knyttet fx til formuens størrelse, synes at være opfyldt, selvom dette er uberettiget ud fra de virkelige forhold.

Hvidvask kan altså ske på mange måder, og med mange formål. Det er vigtigt at fremhæve, at det oftest sker uden brug af kontante midler. De finansielle kriminelle – især de "hårdkogte, store fisk" – udvikler mange og komplicerede metoder til at misbruge både det finansielle system og andre sektorer. Jo mere fintmaskede systemerne bliver – desto mere ihærdige bliver de kriminelle i deres evige jagt på at finde huller. Det er en konstant oprustning og et vanskeligt kapløb, hvor det gælder om på samfundsniveau konstant at udvikle og opdatere bekæmpelsessystemerne hele vejen rundt, når et hul for kriminelt misbrug til hvidvask bliver opdaget.

Terrorfinansiering

Finansiering af terrorisme som begreb er defineret i straffelovens § 114 b.

Finansiering af terrorisme er med andre ord, når man samler ind, yder støtte eller stiller penge til rådighed for personer eller grupperinger, der indgår i terroraktiviteter. Terrorfinansiering kan være svært at opdage, idet det typisk er små betalinger eller overførsler.

Dertil er terrorfinansiering ofte sværere at overvåge og opdage end hvidvask, fordi den "synlige" ulovlige handling nogle gange først sker efter det finansielle systems involvering, og det er derfor personens kriminelle hensigt bag handlingen, der skal opdages.

Pengeinstitutterne kan blive brugt til terrorfinansiering, fx hvis en kunde lovligt modtager reel lønindkomst eller offentlig understøttelse på sin konto, men vedkommende har i sinde at videreformidle beløb til personer, der er involveret i terroraktiviteter. Det kan også være, at en person optager mindre forbrugslån, som umiddelbart fremstår legitime, men pengene benyttes ikke som oplyst og bliver ikke betalt tilbage. Terrorfinansiering kan desuden fremstå som indsamling til et godt og velgørende formål uden for EU, hvor bidragsyderne ikke er vidende om, at pengene i virkeligheden bruges til terroraktiviteter.

Hvor stort er omfanget?

Der findes ikke officielle tal på, hvor store beløb der hvidvaskes for i Danmark, og i hvilken udstrækning terrorfinansiering foregår. Omfanget af disse aktiviteter er således meget vanskeligt at opgøre, hvilket blandt andet fremhæves i SØIKs nationale risikovurdering fra 2018.

I Financial Action Task Forces (FATF) evaluering af Danmark fra 2017 anslås hvidvask i Danmark til 2,8 mia. euro (ca. 21 mia. kr.) årligt. FATF er en mellemstatslig organisation, der har til formål at fremme internationale standarder for bekæmpelsen af hvidvask og terrorfinansiering. Tallet dækker over udbytter fra handel med narkotika, menneskehandel, biltyveri, røverier, våbenhandel, tobaks- og spiritussmugling, skatte- og momssvig og anden økonomisk kriminalitet. Formodningen er, at skatte- og momssvig generer de største udbytter. Ifølge rapporten vurderer de danske myndigheder, at staten årligt mister 0,4 mia. euro (ca. 3 mia. kr.) i indtægter på grund af skattesvig alene. Vurderingen er endvidere, at terrorfinansiering sker særligt til terrorgrupper og netværk i udlandet, men at omfanget er ukendt.

De samfundsmæssige konsekvenser af hvidvask og terrorfinansiering må dog uanset fraværet af konkrete tal for omfanget anses for alvorlige.

I SØIK's nationale risikovurdering fremhæves følgende samfundsskadende konsekvenser af hvidvask[4]:

- Hvidvask af kriminelt udbytte fastholder og bidrager til væksten på de kriminelle markeder på tværs af EU.
- Kriminelle aktørers bestræbelser på at tilsløre udbytte fra strafbare forhold kan medføre svækket tillid til det finansielle system.
- Det kan ligeledes være skadeligt for andre tilknyttede finansielle institutioner, lovgivende myndigheder og almindelige kunder i institutionen.
- Derudover kan det virke krænkende for befolkningens retsfølelse, hvis der er en opfattelse af, at hvidvask forbliver uopdaget eller ustraffet.
- Det er samtidig skadeligt for samfundsøkonomien, når kriminelle aktører hvidvasker udbytte fra kriminalitet. Der er både direkte og indirekte konsekvenser, hvoraf de direkte konsekvenser ses i form af mistede skatter og afgifter. De indirekte konsekvenser kan eksempelvis ses i de tilfælde, hvor der placeres en stor mængde udbytte fra kriminalitet i specifikke typer af varer eller ydelser. Dette kan have negative konsekvenser for markedet, da det vil være konkurrenceforvridende for de personer og virksomheder, som legalt handler varerne og ydelserne. Det samme gør sig gældende for brancher, hvor der en stor grad af "sort" økonomi, eksempelvis visse dele af servicebranchen.

[4] *Kilde: https://bit.ly/2s1eBTC*

Regulering

Som tidligere nævnt, er den centrale regulering i forhold til pengeinstitutternes forpligtelser på området hvidvaskloven. Hvidvaskloven er ikke en dansk opfindelse men er i høj grad udtryk for gennemførelse af EU-regulering på området.

EU's primære regulering på området er de såkaldte hvidvaskdirektiver, der i overvejende grad er baseret på anbefalingerne fra FATF. Dertil kan endvidere fremhæves de sanktionslister, som EU vedtager blandt andet på baggrund af FN's sikkerhedsresolutioner.

Det første hvidvaskdirektiv kom i 1991 og indførte forpligtelser for pengeinstitutterne. Direktivet er efterfølgende blevet afløst af ny EU-regulering, og som det seneste skal det 5. hvidvaskdirektiv implementeres inden januar 2020. EU-reguleringen er udtryk for en risikobaseret tilgang til bekæmpelsen af hvidvask og terrorfinansiering. Det betyder, at de omfattede virksomheder og myndigheder skal fokusere indsatsen på de områder, som indebærer den største risiko for hvidvask og terrorfinansiering.

Direktiverne indebærer forpligtelser for virksomhederne, herunder pengeinstitutterne, i forhold til at gennemføre kundekendskabsprocedurer, overvåge transaktioner og underrette myndighederne om mistænkelige aktiviteter. Disse forpligtelser er i Danmark gennemført i den danske hvidvasklov.

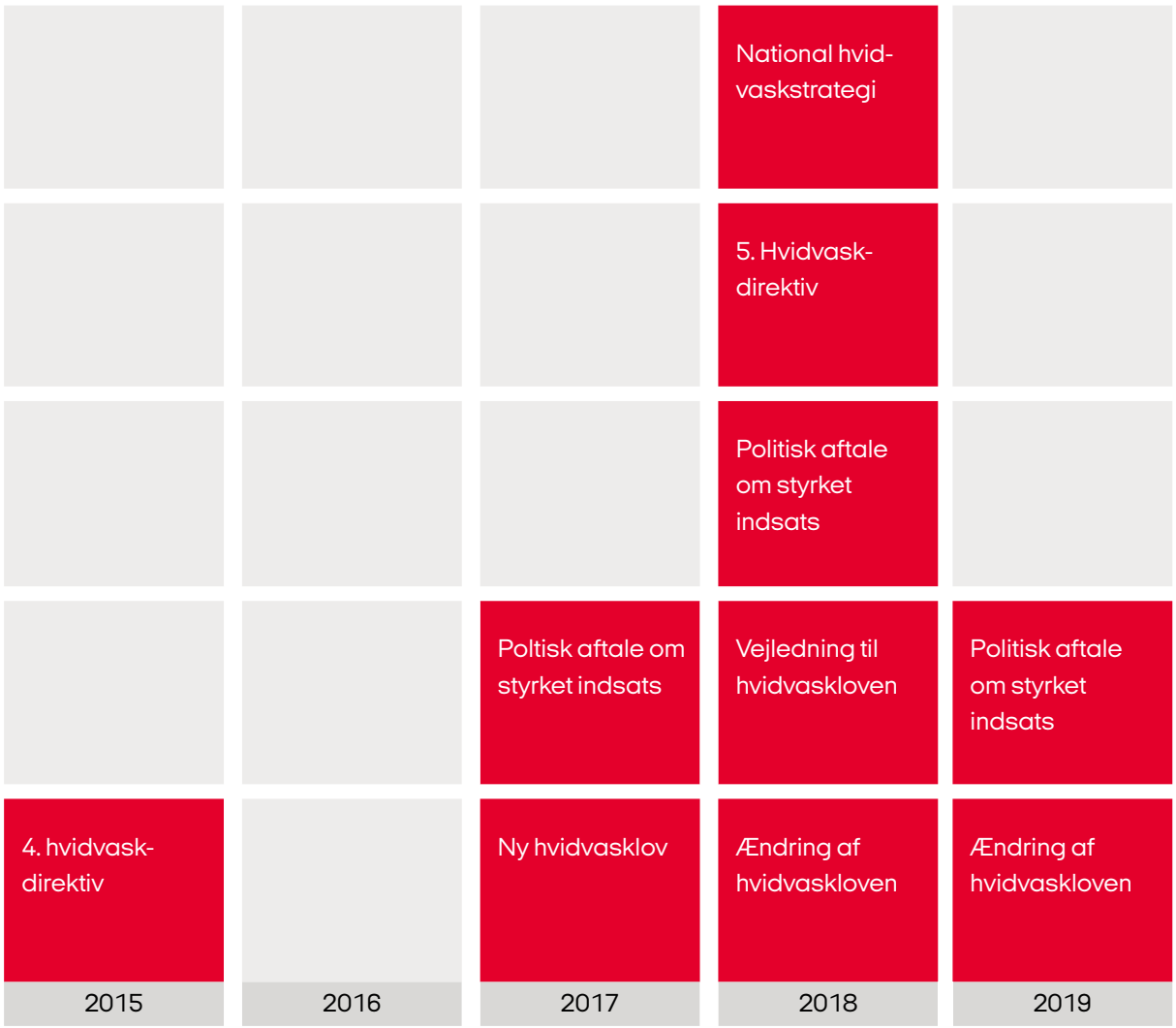
Den danske regulering indeholder dertil også forpligtelser, som ikke kommer direkte fra EU-reguleringen. På baggrund af den seneste tids udvikling og de seneste hvidvasksager, har man fra politisk side haft som ambition, at den danske regulering på området skal være den førende i EU. Der er derfor gennem den seneste tid indgået en række politiske aftaler om nationale initiativer, der er gennemført i både hvidvaskloven og i andre love.

Indholdet af aftalerne er beskrevet nærmere i bilag 2: Tidslinje. På side 17 følger en kronologisk oversigt over udvalgte politiske initiativer. Oversigten er med til at illustrere, at reguleringsintensiteten de seneste par år er steget.

Indhold af politiske aftaler

De politiske aftaler fra 2017-2019 har blandt andet medført indgåelse af en national hvidvaskstrategi, højere bødeniveauer, øgede ressourcer til Finanstilsynet og Hvidvasksekretariatet i SØIK, skærpede fit and proper krav, øget beskyttelse af whistleblowere mv.

Figur 3 Kronologisk oversigt over **udvalgte** politiske initiativer på området



Kilde: Finans Danmark

PENGEINSTITUTTERNES INDSATS I DAG

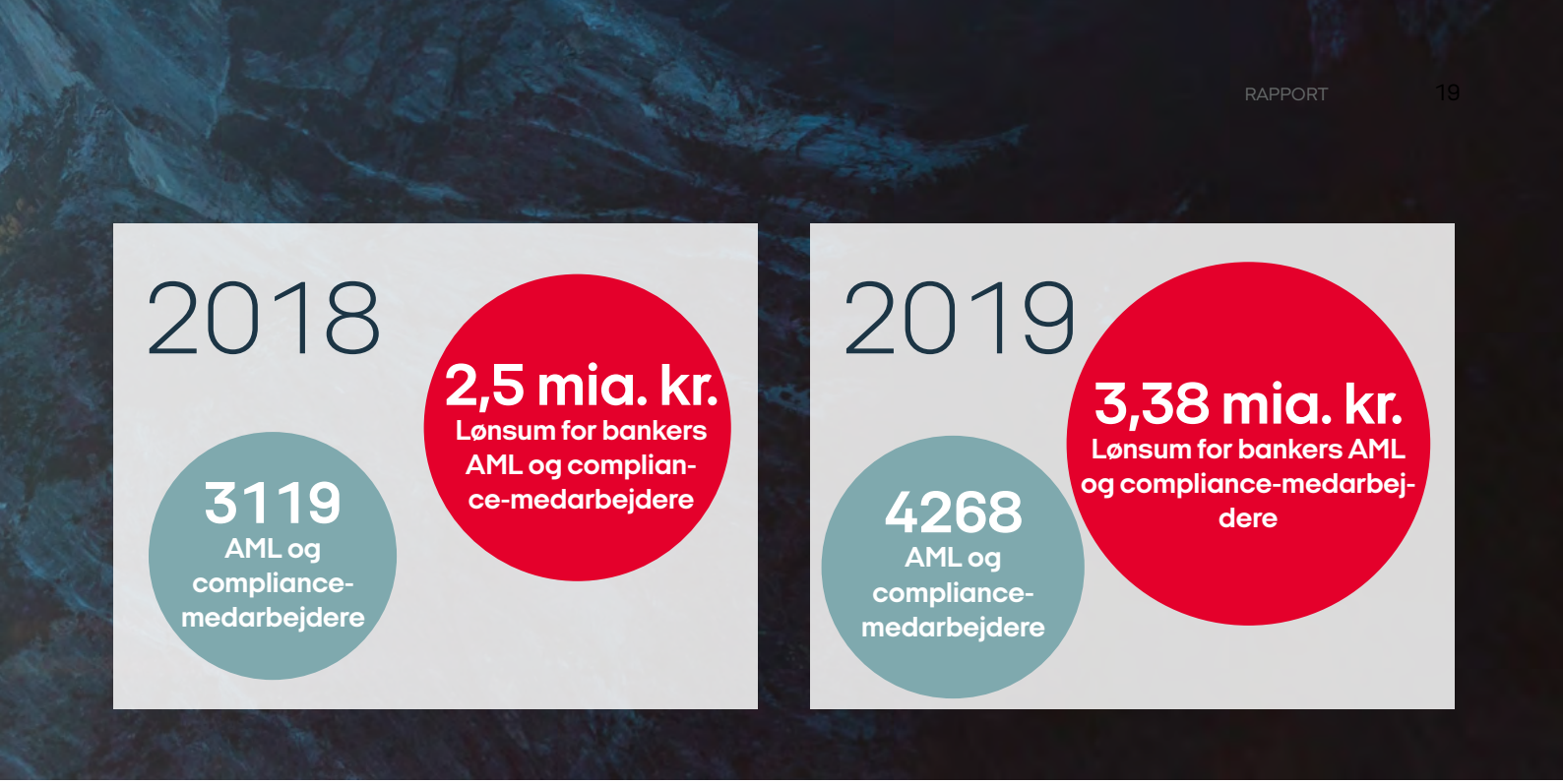
Pengeinstitutterne spiller en central rolle i bekæmpelsen af hvidvask og terrorfinansiering i Danmark. Faktisk er pengeinstitutterne én af de vigtigste medspillere for myndighederne, og er uden sammenligning dem, der foretager flest underretninger til Hvidvasksekretariatet i SØIK om mistænkelige forhold. For at dette kan lade sig gøre, har sektoren over de seneste år investeret massivt i både mandskab og udvikling af it-systemer på området. Antallet af ansatte der har hvidvask og compliance som kerneopgave har pr. november 2019 ramt 4.300. Det svarer til lønudgifter på i alt 3,4 mia. kr. om året. Alene fra 2018-2019 er udgifterne steget med 0,9 mia. kr. Baggrundstæppet for bekæmpelsen af hvidvask og terrorfinansiering udgøres af den meget intensive lovgivning, der er på området. Lovgivningen udspringer fortrinsvis af EU-regulering og indeholder en række forpligtelser for pengeinstitutterne og andre virksomheder som pensionsselskaber, valutavekslingsvirksomheder, advokater, revisorer, forsikringsselskaber mv. Dertil er der i Danmark vedtaget en række skærpelser på området for at gøre den danske lovgivning til en af de strammeste i EU.

Kravene er udtryk for, at man fra lovgivers side har sat pengeinstitutterne og andre aktører i forreste række i forhold til at kunne opdage og indrapportere mistænkelige aktiviteter til myndighederne. Det er forståeligt, da pengeinstitutterne er en så vigtig del af samfundet, at der nødvendigvis skal stilles store krav til pengeinstitutterne på flere fronter, og da netop pengeinstitutterne har mulighed for at opdage hvidvask og terrorfinansiering.

Men lad os gå ned i maskinrummet og se nærmere på, hvad pengeinstitutterne konkret gør for at bekæmpe hvidvask og terrorfinansiering.

Hvidvaskpolitik og risikovurdering

Pengeinstitutternes hvidvaskpolitik og risikovurderingen er de styrende dokumenter, der angiver rammen for det enkelte pengeinstituts hvidvaskindsats. I risikovurderingen vurderer pengeinstituttet de konkrete risikofaktorer, der gør sig gældende i fastlæggelsen af pengeinstituttets risiko for at blive misbrugt til hvidvask og terrorfinansiering, og hvor udgangspunktet tages i pengeinstituttets forretningsmodel. Risikofaktorer er fx kundetyper, produkttyper og tjenesteydelser, geografiske placeringer mv. Risikovurderingens konklusioner er grundlaget for pengeinstituttets beslutninger i forhold til fastlæggelsen af hvidvaskpolitikken og de procedurer, der skal iværksættes i forhold til at begrænse de konstaterede risici.



I hvidvaskpolitikken fastsættes overordnet, hvordan pengeinstituttet forebygger og sikrer sig mod at blive misbrugt til hvidvask og terrorfinansiering. Der skal blandt andet fastlægges retningslinjer for, hvordan pengeinstituttet overvåger sine kunder – både elektronisk og manuelt – hvordan pengeinstituttet underretter, om der er geografiske områder, hvor pengeinstituttet ikke vil operere eller indgå forretningsforbindelser mv. Inden for rammen af hvidvaskpolitikken udarbejder pengeinstituttet procedurer eller forretningsgange, der beskriver de enkelte aktiviteter, som pengeinstituttet foretager for at bekæmpe hvidvask og terrorfinansiering. Forretningsgange kan beskrives som et værktøj for de ansatte, der beskriver rollefordeling, ansvar og hvordan opgaverne skal udføres. Endelig fastlægges der kontroller, der skal sikre, at politik og forretningsgange overholdes. De nævnte dokumenter kan samlet beskrives som den ramme og de procedurer, som pengeinstituttet arbejder på baggrund af i forhold til bekæmpelse af hvidvask og terrorfinansiering. Det er et krav efter hvidvaskloven, at rammen og rutinerne passer til pengeinstituttets konkrete forretningsmodel, kundetyper mv. og de risici, der er forbundet hermed. Der ligger derfor fra pengeinstituttets side et grundigt og omfattende arbejde bag udarbejdelsen af de nævnte dokumenter, der er individuelle fra pengeinstitut til pengeinstitut.

Organisering af bekæmpelsen af hvidvask og terrorfinansiering

At bekæmpelse af hvidvask og terrorfinansiering fylder meget i de enkelte pengeinstitutter, kan også ses på den måde, pengeinstitutterne er organiseret. Som nævnt er der i dag ca. 4300 AML- og compliance-medarbejdere, der har til opgave at overvåge og sikre, at pengeinstitutter ikke misbruges til hvidvask, terrorfinansiering eller anden finansiel kriminalitet. Tallet har været stigende over en længere periode og forventes at stige yderligere i fremtiden. Dertil kommer alle de ansatte i andre jobfunktioner i pengeinstitutterne, der også som led i deres arbejde er involveret i bekæmpelse af hvidvask og terrorfinansiering. Det gælder fx kunderådgiverne.

Indsatsen er dertil ikke bare samlet ét sted, men er derimod forankret flere steder i organisationen for blandt andet at sikre, at der løbende arbejdes med området i overensstemmelse med lovgivningen og pengeinstituttets interne regler. Pengeinstitutternes bekæmpelse af hvidvask og terrorfinansiering er bygget op om det, man kalder de tre forsvarslinjer:

Figur 4 De tre forsvarslinjer

1. Første forsvarslinje udgøres blandt andet af de mange ansatte ude i pengeinstitutternes filialer, der i den daglige kontakt med kunderne undersøger, om der skulle være tegn på hvidvask eller terrorfinansiering. I mange pengeinstitutter er der desuden en central AML-enhed, der tager stilling til de sager, hvor fx rådgiveren eller it-overvågningssystemet har fundet, at der kan være risiko for hvidvask eller terrorfinansiering.
2. Anden forsvarslinje er det, man typisk vil kalde compliance og risikoafdelingerne. Bankernes compliance – og risikoafdeling arbejder med at kontrollere om første forsvarslinje lever op til de krav der fremgår at såvel lovgivning som bankens forretningsgange og procedurer. Dette sker for at sikre en tilstrækkelig håndtering af bankens risici for at blive misbrugt til hvidvask eller terrorfinansiering.
3. Tredje forsvarslinje er typisk en uafhængig afdeling, i form af intern revision, der har til opgave at kontrollere, at bankens forsvarsværker er tilstrækkelige. De tjekker med andre ord, om første og anden forsvarslinje arbejder med bekæmpelse af hvidvask eller terrorfinansiering og efterlever de af banken udstukne rammer for indsatsen.

Kilde: https://secure.finansforbundet.dk/da/nyheder-aktuelt/Sider/Bankerneshvidvaskomraadevokser.aspx

Ansvaret for bekæmpelse af hvidvask og terrorfinansiering skal være forankret i pengeinstituttets direktion. Der er derfor et direktionsmedlem, der er ansvarlig for at sikre, at virksomheden gennemfører og overholder kravene i hvidvaskloven ved effektive politikker, procedurer og kontroller.

Pengeinstitutterne skal dertil efter hvidvaskloven udpege en hvidvaskansvarlig, der skal godkende virksomhedens politikker, procedurer og kontroller på hvidvaskområdet[5].

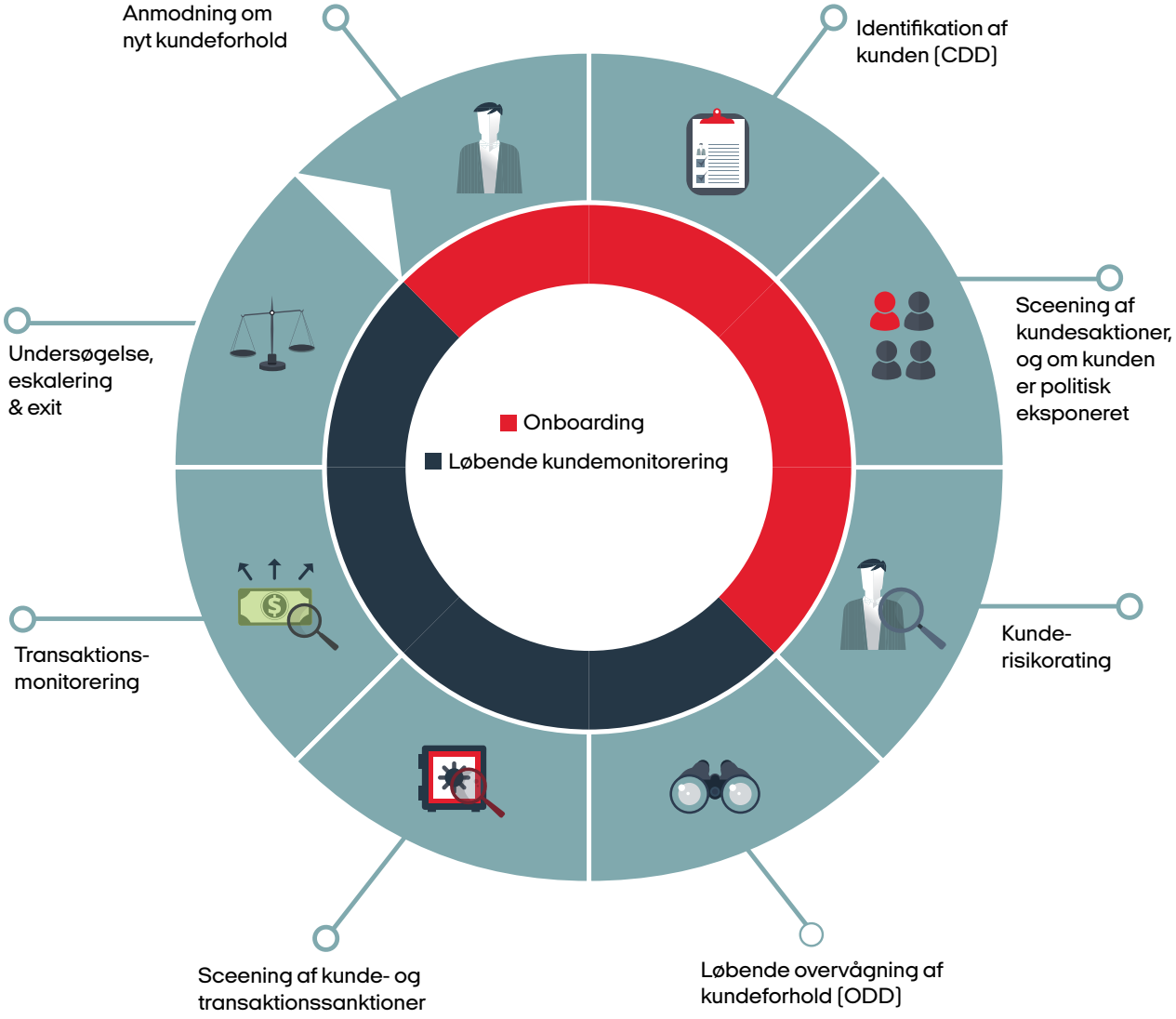
Det er desuden den hvidvaskansvarlige, der skal godkende korrespondentforbindelser, dvs. forbindelser med andre pengeinstitutter og kundeforhold til politisk eksponerede personer og deres nærtstående og nære samarbejdspartnere.

Opsummerende bruges der altså bag den almindelige kundekontakt mange ressourcer i pengeinstitutterne på at få etableret den mest hensigtsmæssige organisation og de mest hensigtsmæssige sagsgange for at sikre et så effektivt værn som muligt mod, at pengeinstitutterne bliver misbrugt til hvidvask eller terrorfinansiering.

AML i kundeforholdet

Bekæmpelse af hvidvask og terrorfinansiering er dybt integreret i pengeinstitutternes kundeforhold. De forskellige trin i, hvordan pengeinstitutterne håndterer risici for hvidvask og terrorfinansiering er overordnet skitseret i nedenstående figur.

Figur 5 AML i kundeforholdet



Kilde: Finans Danmark

[5] *Filialer af udenlandske pengeinstitutter skal ikke udpege en hvidvaskansvarlig, jf. hvidvasklovens § 7, stk. 2.*

Kend din kunde

I pengeinstituttets kontakt med kunderne er det helt grundlæggende princip "kend din kunde". Efter hvidvaskloven skal pengeinstitutterne have et godt kendskab til alle deres kunder. Det skal være med til at forebygge misbrug af det finansielle system ved at gøre pengeinstitutterne i stand til at reagere, hvis en kunde foretager sig noget usædvanligt.

I praksis betyder det, at pengeinstitutterne skal vide, hvem deres kunder er, og hvilket forretningsomfang kunderne vil have med det enkelte pengeinstitut. Pengeinstituttet skal kende kundens navn og CPR-nr. og indsamle dokumentation herfor, fx ved kopi af kundens pas og sygesikringskort. Når der kommer en ny potentiel kunde, foretager pengeinstituttet derfor en screening af kunden og spørger ind til identiteten af vedkommende, indhenter dokumentation for kundens oplysninger og spørger ind til med hvilket formål og omfang kunden ønsker at bruge pengeinstituttet. Er det fx for at optage et lån, have en lønkonto eller for at kunne overføre betalinger til udlandet. Disse informationer er centrale for, at pengeinstituttet kan udføre en risikovurdering af den nye potentielle kunde og på den baggrund afgøre, om det er en kunde, man ønsker at have i pengeinstituttet. Risikovurderingen gør også pengeinstituttet i stand til på baggrund af sin hvidvaskpolitik, kontroller og forretningsgange at fastlægge, hvilke kontroltiltag man skal træffe for at kunne imødegå den risiko, som en kunde konkret udgør. Alt efter hvilket risikoniveau kunden har, vil pengeinstituttet gentage kundekendskabsprocedurerne med forskelligt interval, fx årligt for kunder med øget risiko.

Når mængden af spørgsmål og krav om dokumentation, som pengeinstituttet stiller over for nye kunder, kan virke overvældende, skal det ses i sammenhæng med, at et indgående kendskab til kunden er nødvendigt for, at pengeinstituttet effektivt kan overvåge pengeinstituttets kundeforhold og identificere sager, hvor der er tegn på hvidvask eller terrorfinansiering. Den risikovurdering, som pengeinstituttet foretager af den enkelte kunde, er derfor på mange måder lige så indgående som den kreditvurdering, pengeinstituttet foretager af kunden. Selvom risikoen for et enkelt kundeforhold er lav, er det nødvendigt at afdække en række oplysninger for at have en god sikkerhed for, at vurderingen er rigtig. Processen kan sammenlignes med sikkerhedskontrollen i en lufthavn – alle skal igennem, selvom risikoen ved den enkelte passager er lille.

Det er et lovkrav, at pengeinstituttet skal kende og kontrollere en kundes navn og CPR-nr. og for en erhvervskunde navn og CVR-nr. Dette kan ikke fraviges. Foruden dette skal pengeinstituttet ud fra en risikovurdering sikre sig, at pengeinstituttet henter andre relevante oplysninger for at opnå et tilstrækkeligt kendskab til sin kunde. Det er derfor det enkelte pengeinstitut, som i forhold til pengeinstituttets egen risikovurdering vurderer, hvad der er relevant at spørge om og indhente dokumentation for.

Når kundeforholdet er etableret, overvåger pengeinstituttet løbende dette, herunder om kundens adfærd passer til det billede, kunden har givet pengeinstituttet ved sine oplysninger. Hvis kundens adfærd ændrer sig – fx hvis kunden begynder at foretage transaktioner af en størrelse eller et omfang, som afviger fra det oplyste – kan det betyde, at pengeinstituttet udvider overvågningen eller stiller yderligere spørgsmål. Pengeinstituttet vil fx også, hvis en kunde modtager et atypisk beløb på sin konto, spørge ind til, hvor beløbet stammer fra. Pengeinstituttet skal også løbende opdatere oplysningerne.

Overvågning af usædvanlige forhold

Et pengeinstitut kan blive opmærksom på usædvanlige forhold, der kan give anledning til en mistanke, på forskellige måder.

Et vigtigt aktiv, pengeinstitutterne har i bekæmpelsen af hvidvask og terrorfinansiering, er personalet. Medarbejdere i pengeinstitutter er rigtigt gode til at bruge deres sunde fornuft og spørge ind til forhold, som de ikke forstår i deres kontakt med kunderne. Det kan fx være et par, der i forbindelse med godkendelse af et boliglån oplyser, at de foruden deres lønindkomst har en "indtægt ved siden af", hvilket kan tyde på sort arbejde. De ansatte i pengeinstitutterne understøttes i deres arbejde af de uddannelsesforløb, som pengeinstitutterne efter loven skal tilbyde. Der er krav om, at ledelsen og de ansatte, der beskæftiger sig med områder, hvor der kan være en risiko for misbrug, skal gennemføre disse uddannelsesforløb.

Der foretages ca. 1,3 mio. transaktioner og ca. 850.000 transaktioner dagligt i henholdsvis straks- og intradag-clearingen i Danmark. Værdien af de samlede transaktioner (sum-, intradag- og straksclearing) er dagligt ca. 41,1 mia. kr., hvoraf de ca. 1,2 mia. kr. stammer fra straksclearingen, der foregår inden for få sekunder uden involvering af en rådgiver i pengeinsti-

Eksempler på oplysninger og dokumentation, som en privat- eller erhvervskunde typisk bliver bedt om at oplyse og fremvise:

- Navn.
- CPR-nr. eller CVR-nr.
- Adresse.
- Pas, kørekort, sundhedskort eller fødselsattest.
- Kundens formål med kundeforholdet til pengeinstituttet.
- Kundens forventninger til omfanget af kundeforholdet med pengeinstituttet.
- Oplysninger og/eller dokumentation for oprindelsen af kundens midler.
- Kundens indtægt, fx lønsedler, pension, offentlige ydelser mv.
- Erhvervskundens forretningsmæssige formål.
- Oplysninger og/eller dokumentation for erhvervskundens forretningsmæssige ejer- og kontrolstruktur og reelle ejere. Erhvervskundens tegningsregler eller ejeraftaler.

Hvidvasksekretariatet i SØIK videresender underretninger til relevante myndigheder. Det kan være PET, når det gælder terrormistanke, det almindelige politi, når det gælder forbrydelser i øvrigt, Skattestyrelsen, når det gælder skattesvig og Udbetaling Danmark, når det gælder socialt bedrageri (De fleste underretninger videresendes til PET eller det lokale politi. Skattestyrelsen modtager underretninger om skattesvig. Udbetaling Danmark modtager et meget begrænset antal underretninger om socialt bedrageri).

tuttet. Pengeinstitutternes overvågning af usædvanlige forhold er derfor i høj grad afhængig af en automatiseret digital overvågning. Pengeinstitutterne har de seneste år investeret massivt i it-systemer, der i højere grad gør det muligt for pengeinstitutterne at identificere usædvanlige transaktioner. It-systemerne muliggør, at atypiske transaktioner bliver "fanget". Det kan være en transaktion, der størrelsesmæssigt er atypisk for den pågældende kunde, og transaktionen vil herefter blive taget ud til manuel kontrol af pengeinstituttets personale. I langt de fleste tilfælde vil der være tale om falsk alarm, men i nogle tilfælde er der en mistanke, der ikke kan afkræftes.

Underretning til myndighederne

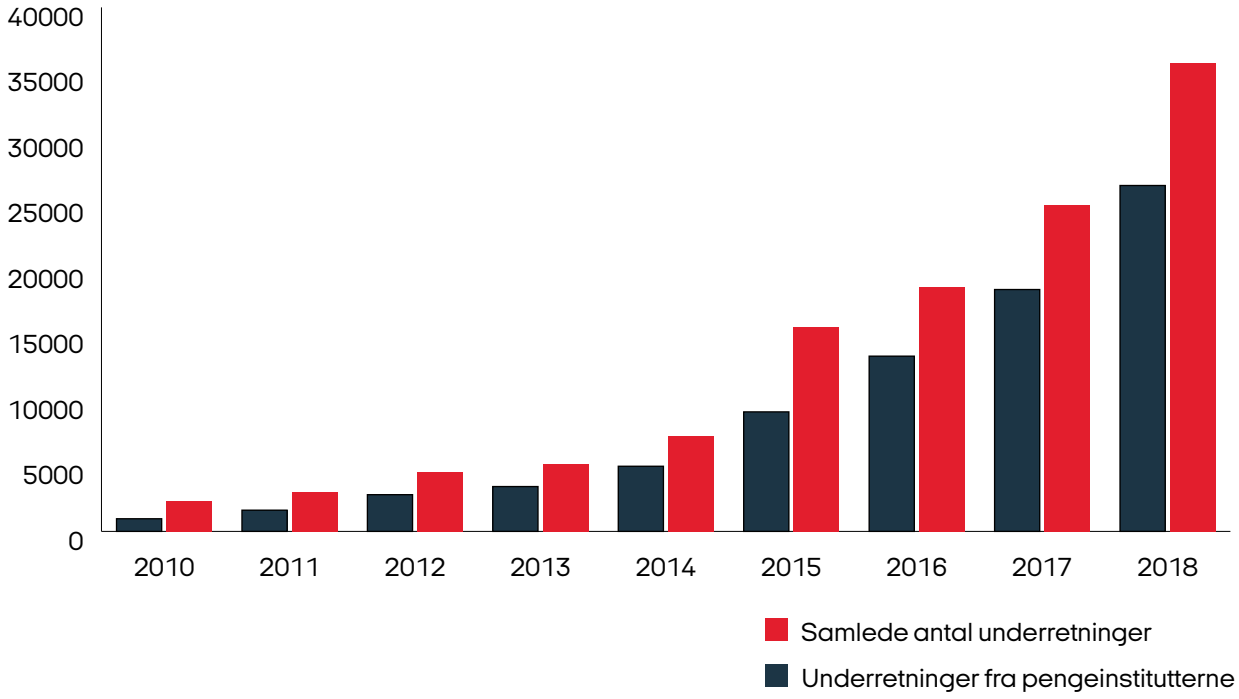
Hvis en transaktion eller adfærd fremstår usædvanlig, og pengeinstituttet ikke kan afkræfte, at dette giver anledning til mistanke om hvidvask og terrorfinansiering, skal pengeinstituttet underrette myndighederne. Underretningen går til Hvidvasksekretariatet i SØIK, der screener underretningen og videreformidler de underretninger, der vedrører andre myndigheder, fx PET eller det lokale politi, Skattestyrelsen eller eventuelt Udbetaling Danmark.

Pengeinstitutterne har kontinuerligt underrettet flere mistænkelige forhold gennem de seneste år. I 2018 foretog pengeinstitutterne godt 26.000 underretninger ud af i alt godt 35.000 underretninger. Det var en stigning på 43 pct. i forhold til 2017 og hele 189 pct. i forhold til de 9.124, der blev sendt af sted i 2015.

Pengeinstitutterne står således for langt hovedparten af de underretninger, der går til myndighederne. Det er en tendens, der forventes at fortsætte i 2019. Pengeinstitutterne har således for de to første kvartaler i 2019 foretaget over 17.000 underretninger ud af et samlet antal underretninger på ca. 24.000, hvilket giver en forventning om, at årets samlede antal underretninger vil ende omkring 35.000 – 40.000.

Et spørgsmål, der kan rejses er, om alle underretninger kan bruges af myndighederne. Generelt er det tilbagemeldingen fra SØIK, at langt hovedparten af de under-

Figur 6 Udvikling i antal underretninger til Hvidvasksekretariatet i SØIK



Kilde: Graf baseret på tal fra SØIK.

retninger, som sektoren kommer med, er både kvalificerede og screenet, så de tilsammen udgør et godt fundament for myndighederne at arbejde videre med. Der er ingen indikation af, at pengeinstitutternes underretninger skulle være for mange eller for ukvalificerede. Tværtimod er der kommet tilkendegivelser fra myndighederne, som indikerer, at der i alene omkring 5 pct. af alle underretninger kan rejses tvivl om berettigelsen af underretningen. Et yderligere element i denne diskussion er, at anvendeligheden af en underretning ikke skal afgøres af pengeinstituttet, men derimod af myndighederne, netop fordi pengeinstituttet har en ubetinget forpligtelse til at underrette i tilfælde af mistænkelig adfærd.

Hvidvasksekretariatet i SØIK benytter ofte underretningerne til at samle puslespil af viden, der samlet kan benyttes til større sager. Selvom hver enkelt underretning ikke fører til konkrete resultater, vil den således ofte være yderst nyttig som brik i et puslespil.

I Hvidvasksekretariatets opgørelse over underretninger og videregivelser fremhæves, at der er videregivet 75 pct. flere underretninger i 2018 end i 2017, hvoraf størstedelen, hvorfra der er videregivet oplysninger, er videregivet til Skatteforvaltningen. I 2018 blev der videregivet oplysninger til Skatteforvaltningen fra 5.536 underretninger[6]. Skattestyrelsen oplyser, at de undersøgelser og kontroller, der er udført på baggrund af disse oplysninger, har resulteret i et væsenligt nettoprovenu for staten.

Finans Danmark

Finans Danmark understøtter alle initiativer, som med succes kan være med til at bekæmpe finansiel kriminalitet. Derfor har Finans Danmark aktivt og konstruktivt spillet ind - og været med i de sammenhænge, det har været muligt undervejs i forskellige fora og forhandlinger.

Eksternt har det blandt andet betydet, at Finans Danmark har været i dialog med samtlige partier på Chri-

[6] *Kilde: https://anklagemyndigheden.dk/sites/default/files/inline-files/Underretninger%20og%20videregivelser%202018.pdf*

stiansborg i forhold til udfordringer og løsninger, det samme i forhold til embedsværket og Finanstilsynet. Finans Danmark har haft sæde i KL's råd om kriterierne til fremtidige kontrakter med pengeinstitutterne. Finans Danmark deltager i Finanstilsynets Hvidvaskforum+ og har generelt intensiveret samarbejdet med Skat, politi, PET m.fl. Finans Danmark har stillet sig til rådighed for Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance (TAX3), der fokuserer på skattely og hvidvask i EU, samarbejde med EBA, som er den Den Europæiske Banktilsynsmyndighed, og som kontaktpersoner fra den danske finansielle sektor for FATF.

Internt har Finans Danmark nedsat Hvidvask Task Forcen, som består af eksterne eksperter og interne fra pengeinstitutterne. Der er iværksat et styrket samarbejde med myndighederne, hvor der holdes kvartalsvise møder mellem pengeinstitutterne og SØIK og Finanstilsynet. Her får Finans Danmarks medlemmer mulighed for at indgå i dialog med de relevante myndigheder om udviklingen på området. I forbindelse med implementering af hvidvaskdirektiverne har der ligeledes været en god kontakt med myndighederne.

Finans Danmark har derudover nedsat en permanent hvidvaskarbejdsgruppe, som har til opgave at facilitere sparring på lovgivningen og best practice.

Dertil kommer alle de interne initiativer i pengeinstitutterne, hvor de selvstændigt og uafhængigt af hinanden har oprustet på compliance, iværksat dialogkampagner med kunderne og sendt markant flere underretninger til Hvidvasksekretariatet i SØIK.

UDFORDRINGER VED BEKÆMPELSE AF HVIDVASK OG TERROR-FINANSIERING

Selvom sektoren og myndighederne gør alt, hvad de kan for at bekæmpe hvidvask og terrorfinansiering, må man også erkende, at truslen fra hvidvask og terrorfinansiering ikke kan nedbringes helt. Men hvorfor er det så svært at bekæmpe misbruget af det finansielle system til hvidvask og terrorfinansiering?

Det er svært at komme med en enkel forklaring på dette. De professionelle kriminelle er dygtige og intelligente. De følger med tiden, og de udvikler metoder i takt med nye systemer og teknologier, de møder, når de involverer det finansielle system. Kriminalitet kræver ikke nødvendigvis fysisk kontakt, men kan fx ske ved køb og salg af stjålen information som koder og data. Hvis man ser på organiseret kriminalitet, er det også tydeligt, at de kriminelle er hurtige til at finde nye veje til at misbruge det finansielle system til finansiel kriminalitet. Det betyder uvægerligt, at både myndigheder og pengeinstitutter mange gange vil være et skridt bagefter i forhold til de nyeste metoder, som de kriminelle bruger.

Som fremhævet i SØIK's nationale risikovurdering involverer "processen med at hvidvaske udbytte fra alvorlig og organiseret kriminalitet (...) forskellige og ofte komplekse metoder, der kombinerer elementer fra den legale og illegale økonomi. Sammenblandingen af illegale og legale transaktioner sker blandt andet gennem pengeinstitutter, vekselkontorer, spiludbydere, betalingsinstitutter, pengeoverførselsvirksomheder og forskellige virksomhedskonstruktioner."

Bekæmpelse af hvidvask og terrorfinansiering er med andre ord et meget komplekst område med mange forskellige aktører. Historisk har Danmark været præget af at være et samfund, der er meget tillidsbaseret. Danmark ligger bedst placeret på listen over lande med korruption[7], og samfundet har ikke været vant til at opleve bestikkelse og korruption som et samfundsproblem.

Hvidvaskbegrebet og hvidvaskloven rummer desuden alt fra hvidvask via internationale komplicerede konstruktioner ved brug af skuffeselskaber og strømænd til fx skattesnyd, socialt bedrageri og it-relateret kriminalitet. Opgaven kræver derfor mange ressourcer og mange forskellige typer tiltag. Der er mange aktører på området, politiske tiltag, EU-tiltag og lovgivning, der generelt også skal passe ind med andre regler og retsområder, som ikke er til for at bekæmpe økonomisk kriminalitet.

Det værn, som den finansielle sektor skal stå på mål for, har grundlag i hvidvasklovgivningen. Lovgivningen stiller de grundlæggende rammer for organisering, forretningsmæssige politikker, lavpraktiske forretningsgange mv. Der stilles krav til kundekendskab både i form af identitet og forståelse af, hvilke ydelser og service kunden ønsker og hvorfor.

[7] *Kilde: https://www.transparency.org/cpi2018*

DILEMMAER

På trods af det stigende fokus og de tiltag, der løbende vedtages på området, er der stadig nogle iboende dilemmaer, som sektoren møder i praktikken i arbejdet som dørvogteren, der skal forebygge og bekæmpe hvidvask og terrorfinansiering.

It-løsninger

Pengeinstitutter i Danmark har forskellige it-systemer. Danske Bank og Nordea har egne it-systemer, og for de øvrige pengeinstitutter er det datacentraler, der varetager en stor del af it-opgaverne. Datacentralen BEC anvendes af 22 pengeinstitutter, Bankdata anvendes af 9 pengeinstitutter, og SDC anvendes af en række små og mellemstore pengeinstitutter i Danmark, Sverige, Norge, Finland og Færøerne. Endelig er der JN Data, der ejes af de tre datacentraler samt Jyske Bank og Nykredit.

It-systemerne er naturligt opstået og ændret over tid. Der er derfor en vis grad af "lag på lag-løsninger", der har søgt at tage højde for behov for tilpasninger, ændringer og nye tiltag.

I hvidvasklovgivningen er der krav, der fordrer, at pengeinstitutterne har nogle effektive it-løsninger. Eksempelvis skal alle kunder identificeres og kontrolleres, og oplysningerne skal opdateres løbende. Ved det store antal kunder, som pengeinstitutterne har, er it-løsninger nødvendige. Det samme gælder kravene om overvågning af transaktioner, screening af kunder mod sanktionslister, screening af, hvilke kunder der er PEP'er eller nærtstående til en PEP mv.

Idet bekæmpelse af hvidvask og terrorfinansiering ikke er et konkurrenceparameter men en fælles samfundsopgave, er det et oplagt samarbejdsområde, når der udarbejdes it-løsninger. Ved i større grad at samtænke it-løsninger fremover vil sektorens samlede indsats mod hvidvask og terrorfinansiering kunne effektiviseres. Det vil gavne it-systemerne, så de lettere kan følge den teknologiske udvikling, og samlet set vil det gavne effektiviteten af hvidvaskarbejdet og være effektivt på længere sigt.

Myndighedssamarbejde – modsatrettede hensyn

Hvidvaskloven har det overordnede formål at forebygge og bekæmpe hvidvask og terrorfinansiering, og loven bærer derfor et bredt og meget vigtigt samfundshensyn. Lovens legitime hensyn krydser eller udfordres

dog på nogle punkter af andre lovreglers formål og hensyn, herunder blandt andet databeskyttelsesregler, forbrugerretlige regler, regler om god skik, regler om tavshedspligt mv. Det rejser en række dilemmaer, hvor den finansielle sektor kan stå i situationer, hvor der er to modsatrettede hensyn, der hver især er vigtige, men som i den konkrete situation ikke begge kan efterleves.

Hvidvaskloven er det man med en juridisk term kalder for lex specialis lovgivning, hvilket betyder, at loven som udgangspunkt vil gå forud for anden eventuel modsatrettet generel lovgivning. Det betyder, at det er vigtigt med en klar forståelse af rækkevidden af hvidvasklovens regler, for at man kan være betrygget i, at hvidvasklovens regel og hensyn konkret går forud for en anden regel med et andet hensyn. Det er derfor en helt afgørende opgave for myndighederne, der varetager sådan modsatrettet lovgivning, at de sikrer en overensstemmende fortolkning af reglerne, så der er en klar forståelse i de situationer, hvor lovgivningen krydser, og hvor ét vigtigt hensyn må vige for et andet.

Eksempler på praktiske dilemmaer, der kan opstå:

En privatpersons ret til en konto

En privatperson har ret til en såkaldt basal betalingskonto[8]. På en basal betalingskonto kan man sætte penge ind, hæve kontanter, overføre penge samt få tilknyttet et betalingskort og anvende betalingsservice. Med en basal betalingskonto får man også adgang til en netbankløsning, og kontoen kan bruges som NemKonto. De serviceydelser, der er tilknyttet en basal betalingskonto, kan man også gøre brug af inden for EU-/EØS-landene.

Denne regel om ret til en basal betalingsskonto kan stå i modsætning til hvidvaskloven. Hvidvaskloven stiller krav om, at et pengeinstitut ikke må indgå et kundeforhold, hvis kundekendskabsproceduren ikke kan gennemføres[9]. Imidlertid er der taget stilling til, at hvidvasklovens krav om kundekendskab har forrang. Det illustrerer den balancegang, der er mellem hensynet til borgerens basale rettighed set i forhold til det brede samfundshensyn i pengeinstituttets dørvogterrolle, som skal skærme samfundet mod hvidvask og terrorfinansiering.

---

[8] *Kilde: Lov om betalingskonti § 11, stk. 1.*
[9] *Kilde: Hvidvasklovens § 14, stk. 5.*

En kundes krav på en begrundelse ved afvisning eller opsigelse

Afvisning eller opsigelse af et kundeforhold forudsætter en saglig begrundelse[10], men på den anden side er der et krav i hvidvaskloven om tavshedspligt, når pengeinstituttet mistænker en kunde og derfor underretter Hvidvasksekretariatet i SØIK[11].

Kravet om saglig begrundelse ved opsigelse følger blandt andet af regler om god skik for finansielle virksomheder. Endvidere gælder der et krav om begrundelse, når kunden er et betalingsinstitut i lov om betalinger.

Et konkret eksempel findes i lov om betalinger[12] , som sætter et krav i forhold til betalingsinstitutter, når de er kunder i et pengeinstitut. Et betalingsinstitut er en virksomhed, der udbyder betalingstjenester. En betalingstjeneste kan fx være pengeoverførsel, mobil betaling eller betaling via internettet. Det kan også være indsættelse på og hævning fra en konto. Efter lov om betalinger skal "Pengeinstitutter [...] give betalingsinstitutter adgang til deres betalingskontotjenester på objektive, ikkediskriminerende og proportionale vilkår". Hvis et pengeinstitut giver et betalingsinstitut afslag, skal pengeinstituttet: "underrette Konkurrence- og Forbrugerstyrelsen og behørigt begrunde årsagerne til afslaget".

Hensynet i lov om betalinger kan give udfordringer, hvis eksempelvis et pengeinstitut ikke ønsker at indgå et kundeforhold med et betalingsinstitut på grund af en konkret mistanke om hvidvask. Pengeinstituttet vil afvise betalingsinstituttet som kunde i henhold til hvidvaskloven og underrette Hvidvasksekretariatet i SØIK om den konkrete mistanke. Samtidig skal pengeinstituttet dog i udgangspunktet behørigt begrunde afvisningen af betalingsinstituttet og indberette det til Konkurrence- og Forbrugerstyrelsen. Det kan pengeinstituttet ikke, for pengeinstituttets mistanke om betalingsinstituttet er underlagt tavshedspligt.

Hvidvasklovens regler om afvisning eller afvikling af et kundeforhold

Som følge af regler om god skik, privatpersoners ret til en basal indlånskonto og betalingsskonto og kunders generelle ret til en saglig begrundelse er hvidvasklovens regler om afvisning eller afvikling af et kundeforhold vigtige at fremhæve.

Hvidvaskloven stiller et krav om, at en kunde – privat- eller erhvervskunde – afvises eller afvikles, hvis hvidvasklovens krav om kundekendskab ikke kan gennemføres.

Det er dog først relevant, når pengeinstituttet har udtømt alle muligheder for at opfylde lovens krav om kundekendskab[13].

Dernæst følger det også i tilfælde, hvor oplysninger indhentet om en kunde ikke er tilstrækkelige eller ikke kan ajourføres, at pengeinstituttet skal imødegå den eventuelle risiko og overveje, om kundeforholdet skal afvikles[14].

Ifølge hvidvaskloven vil der derfor være situationer, hvor en kunde ikke kan blive kunde eller må opsiges. Det er pengeinstituttet, der skal vurdere, hvornår der er ret/pligt til at afvise kunden, når pengeinstituttet først har gjort alle forsøg på at få de nødvendige oplysninger om kunden. Pengeinstituttet skal altså her foretage en i situationen svær vurdering, som også må tage højde for de rettigheder, en kunde har. Det praktiske problem her er ikke modsatrettede regler, men tvivl om præcis hvornår de aktiveres – pengeinstituttet er overladt til selv at vurdere, præcis hvad der er passende foranstaltninger, men risikerer, at myndigheder senere finder, at den valgte forkert.

---

[10] *Kilde: Lov om finansiel virksomhed § 43, lov om betalinger § 63, stk. 2, god skik-bekendtgørelsens § 6, stk. 5 og § 15.*
[11] *Kilde: Hvidvasklovens § 38.*
[12] *Kilde: Lov om betalinger § 63, stk. 2.*
[13] *Kilde: Hvidvasklovens § 14, stk. 5.*
[14] *Kilde: Hvidvasklovens § 15*

Når mistanken står alene

Et særligt svært dilemma opstår i de situationer, hvor pengeinstituttet for at beskytte sit omdømme ikke ønsker et kundeforhold på grund af en mistanke, men ikke har et juridisk grundlag til at opsige eller afvise kunden. Eksempelvis vil kunden gerne udlevere de adspurgte identitetsoplysninger, kunden har papirer, der dokumenterer kundens formue, kunden forklarer et legitimt formål med brugen af pengeinstituttet, kunden er samarbejdsvillig mv. Hvis pengeinstituttets trods dette har en mistanke om hvidvask eller terrorfinansiering i relation til kunden, kan pengeinstituttet da afvise kunden?

Dilemmaet kan også opstå på en anden måde, hvis pengeinstituttet til at begynde med ikke har en mistanke, og kunden ikke opfører sig til gene for pengeinstituttet, ikke misligholder sine engagementer mv., men pengeinstituttet senere får mistanke og foretager en underretning til Hvidvasksekretariatet i SØIK. I denne situation er pengeinstituttets eneste opsigelsesgrund denne mistanke. Hvis mistanken ikke er af en art, så det er påkrævet at afslutte kundeforholdet, kan pengeinstituttet alligevel vælge at opsige kunden og herefter, hvis pengeinstituttet opsiger kunden for ikke potentielt at kunne blive misbrugt til hvidvaskaktiviteter, hvorledes skal pengeinstituttet begrunde opsigelsen over for kunden, når pengeinstituttet har tavshedspligt om mistanken?

På den ene side, skal pengeinstitutterne værne om hensynet til kunden, men samtidig skal pengeinstituttet effektivt forebygge og bekæmpe hvidvask og terrorfinansiering. Ofte vil en mistanke opstå, fordi pengeinstituttets overvågningssystemer giver en alarm i forhold til et kundeforhold. Pengeinstituttet vil undersøge alarmen og vurdere, om forholdet skal underrettes til Hvidvasksekretariatet i SØIK, og om der er andre foranstaltninger, der skal iværksættes. Med teknologiske systemer, der bygger alarmer på scenarier, der kan indikere forskellige risici, er der risiko for såkaldte "false positives". Ofte kan disse frasorteres, når grundlaget for alarmen undersøges. Der er dog en risiko for, at der afgives en underretning om en kunde, og kunden måske i yderste tilfælde opsiges af pengeinstituttet på grund af false positives, hvor pengeinstituttet vurderer eller ikke konkret kan afkræfte, at der er en alvorlig mistanke og risiko forbundet med kundeforholdet.

Dette er en risiko, der følger, når samfundshensynet til at bekæmpe hvidvask og terrorfinansiering skal løftes. Pengeinstituttet skal være loyal over for sin rolle som dørvogter og undgå hvidvask og terrorfinansiering via pengeinstituttet. Det kan som beskrevet medføre, at en kunde afvises på grund af et fejlskøn. Hvis kundekendskabsproceduren skal være grundig og rimelig, må dette mulige fejlskøn accepteres.

En privatpersons ret til sletning af personoplysninger

Af databeskyttelseslovgivningen følger en ret til sletning af personoplysninger[15] og et princip om dataminimering, således at der kun indsamles relevante oplysninger begrænset til, hvad der er nødvendigt[16]. Dette hensyn kan umiddelbart synes at blive udfordret af hvidvasklovens meget entydige krav om indsamling af oplysninger til kundekendskabsproceduren og opbevaring af identitets- og kontroloplysninger om personer frem til 5 år efter endt kundeforhold[17].

Eksempelvis ønsker en kunde at få slettet de personoplysninger, som pengeinstituttet har på kunden i forbindelse med, at kunden flytter til udlandet og søger en ny pengeinstitutforbindelse. Kunden har været kunde i pengeinstituttet i 25 år, og pengeinstituttet har derfor mange oplysninger om kunden, herunder blandt andet kopi af pas og samtlige transaktionsoversigter. Pengeinstituttet må ikke slette de oplysninger, som kunden ønsker, idet pengeinstituttet er forpligtet til at gemme disse i alle 25 år og i de følgende 5 år efter, at kunden har forladt pengeinstituttet.

Der er således ikke et praktisk dilemma i reglerne, men i forhold til at imødekomme hensynet til kundens ønsker. Politisk er dette udtryk for en afvejning af de modsatrettede hensyn mellem på den ene side at gemme data for eventuel brug i bekæmpelsen af hvidvask og terrorfinansiering og på den anden side hensynet til privatlivets fred for de berørte personer.

Behov for erhvervskonti

Virksomheder har brug for erhvervskonti for at drive forretning og kunne udbetale løn, afregne moms mv. Pengeinstitutterne har derfor en afgørende rolle i forhold til at understøtte erhvervslivet og skabe adgang for virksomheder.

Pengeinstitutterne kan dog kun stille konti til rådighed til erhvervskunder, hvis de kan opnå et tilstrækkeligt kundekendskab. Pengeinstitutterne skal blandt andet kende og indsamle dokumentation for erhvervskundens CVR-nr., forretningsformål, organisation, ejerskab mv. for at kunne indgå et kundeforhold.

Pengeinstitutterne skal derfor først forstå og dokumentere erhvervskunders individuelle formål, ledelsessammensætning, ejerskab, som kan være udenlandske borgere med udenlandske identifikationsdokumenter mv. Pengeinstituttet står altså over for en afvejning af hensynet til at bidrage til samfundet og understøtte erhvervslivet i forhold til at føle sig tilstrækkeligt betrygget i at kende kunden.

Pengeinstitutternes kontrol af identifikationsoplysninger vanskeliggøres af, at der ikke i alle offentlige tilgængelige registre foregår en kontrol af oplysningerne. Dette giver i dag udfordringer i forhold til stråmandskonstruktioner.

Tavshedspligt/tipping-off og undersøgelsespligt ved usædvanlige og komplekse forhold

Hvidvaskloven fastsætter en pligt for pengeinstitutterne til at undersøge usædvanlige og komplekse forhold nærmere. Samtidig anbefaler FATF, at enhver finansiel virksomhed, herunder ledelse og medarbejdere, skal være forpligtet til ikke at afsløre – "tipping off" – at en mistænkelig transaktion eller relateret information indgives til Hvidvasksekretariatet i SØIK. Derfor følger der en tavshedspligt i hvidvaskloven, så en virksomhed ikke kommer til at afsløre over for en kunde, at virksomheden har opdaget kundens mistænkelige og ulovlige handlinger eller adfærd. Tavshedspligten omfatter også alle de usædvanlige forhold, hvor der viser sig en tilstrækkelig forklaring, så mistanke kan afvises.

Selve afvisningen eller opsigelsen af en kunde kan i sig selv også risikere at give kunden indikationer om, at kunden mistænkes. I nogle tilfælde må et pengeinstitut derfor efter underretning til Hvidvasksekretariatet i SØIK bevare et kundeforhold for ikke at ødelægge efterforskningen, selvom kunden tydeligvis fortsætter sin mistænkelige adfærd.

Imidlertid fremgår det af Finanstilsynets vejledning, at

[15] *Kilde: Databeskyttelsesforordningens artikel 17*
[16] *Kilde: Databeskyttelsesforordningens artikel 5, c.*
[17] *Kilde: Hvidvasklovens § 30.*

hvis pengeinstituttet vurderer, at spørgsmål til kunden vil give kunden viden om undersøgelsen/mistanken eller i øvrigt finder det uhensigtsmæssigt at kontakte kunden, kan dette undlades, og underretning til Hvidvasksekretariatet i SØIK skal ske med det samme. Det fremgår også, at kundens reaktion kan underbygge en mistanke.

I andre tilfælde kan en kunde dog alligevel fatte mistanke, fx fordi pengeinstituttet spørger ind til de forhold, som giver pengeinstituttet anledning til at undersøge kunden. Det kan eksempelvis være, at pengeinstituttet spørger kunden, hvorfor kunden er begyndt at foretage transaktioner til et land, som kunden ikke tidligere har overført eller modtaget midler fra, eller hvorfor kunden er begyndt at indsætte større kontante beløb på sin konto. Har kunden kriminelle hensigter, vil kunden måske hurtigt finde et andet pengeinstitut og forsøge at fortsætte sine aktiviteter der. Da pengeinstitutterne i dag ikke kan udveksle oplysninger om kunder ved skift af pengeinstitut, er det ikke muligt for pengeinstitutterne at modvirke en sådan trafik.

Udveksling af oplysninger

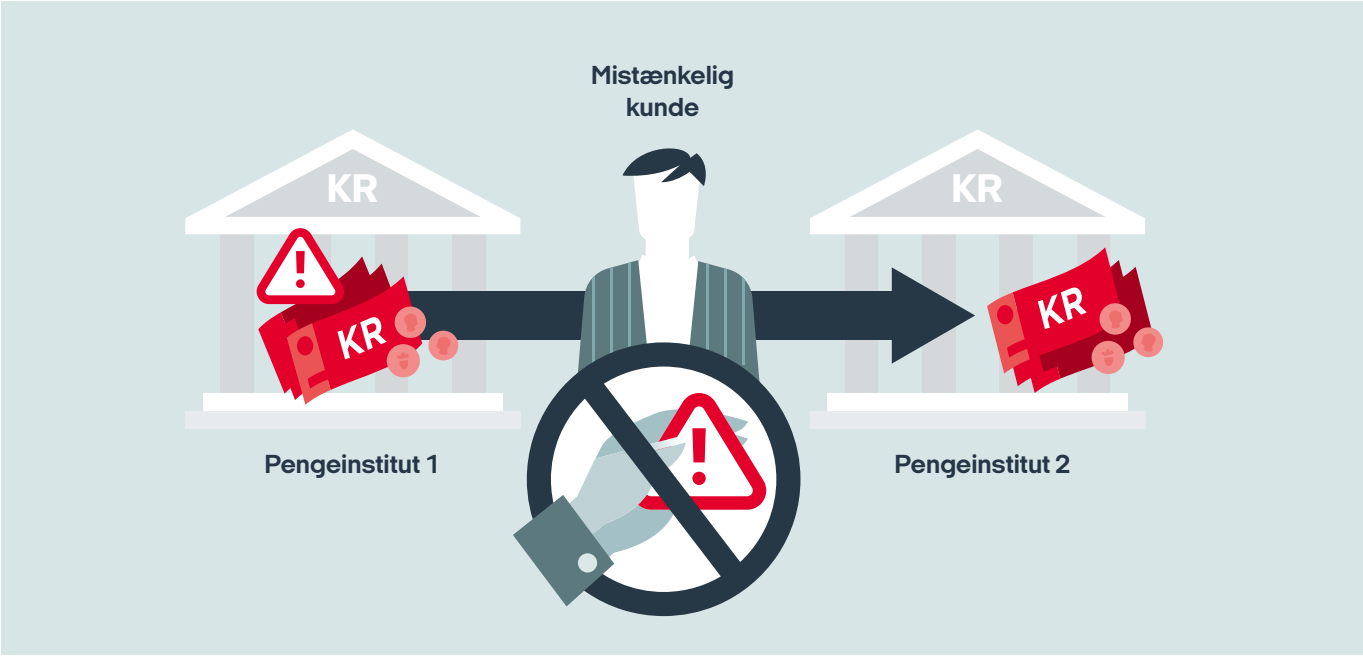
Sektoren har sammen med Finanstilsynet, SØIK og Hvidvasksekretariatet i SØIK, PET og Skattestyrelsen intensiveret samarbejdet. Finans Danmark har etableret et forum, hvor myndighederne har sat sig sammen med pengeinstitutterne for med jævne mellemrum at drøfte, hvorledes bekæmpelsen af hvidvask og terrorfinansiering bedst kan håndteres. Hvidvasksekretariatet giver her blandt andet feedback på pengeinstitutternes underretninger.

Der er dog fortsat et stykke vej, før informationsudvekslingen er effektiv. Hvis et pengeinstitut afviser en potentiel kunde på grund af en stærk mistanke om fx hvidvask, vil pengeinstituttet foretage en underretning til Hvidvasksekretariatet i SØIK. Men som den nuværende lovgivning er sat sammen, er der ikke mulighed for, at andre pengeinstitutter kan blive advaret om denne kunde.

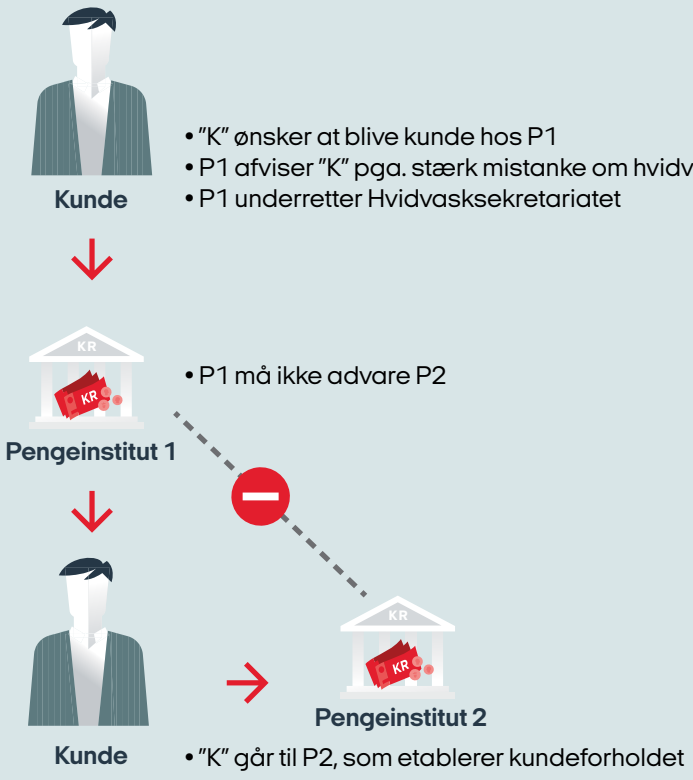
Sagt med andre ord, hvis et pengeinstitut afviser en kunde på grund af hvidvask, og kunden derefter kontakter "naboinstituttet", har pengeinstituttet ikke mulighed for at advare naboinstituttet om, at kunden sandsynligvis er involveret i hvidvask eller terrorfinansiering. Det gør systemet mindre effektivt, se figur 7, 8 og 9 nedenfor.

Det er på den anden side igen en svær balancegang, da kunder har en grundlæggende og berettiget ret til, at pengeinstitutterne behandler deres oplysninger fortroligt. Som det vil blive belyst senere i rapporten, er der derfor behov for at finde en løsning, der tilgodeser både hensynet til den enkelte kunde og hensynet til at have en effektiv bekæmpelse af hvidvask og terrorfinansiering.

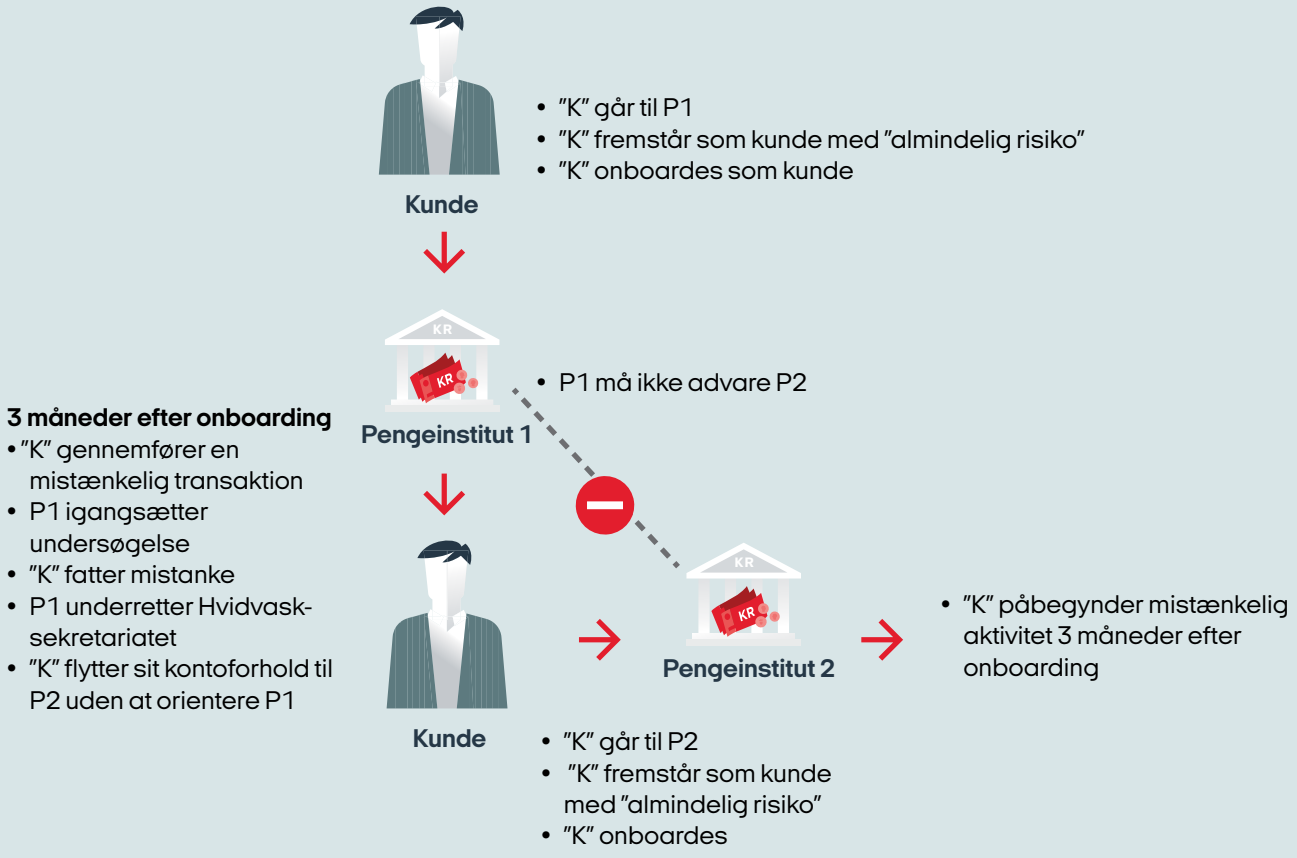
Figur 7 Ingen adgang til at advare andre pengeinstitutter

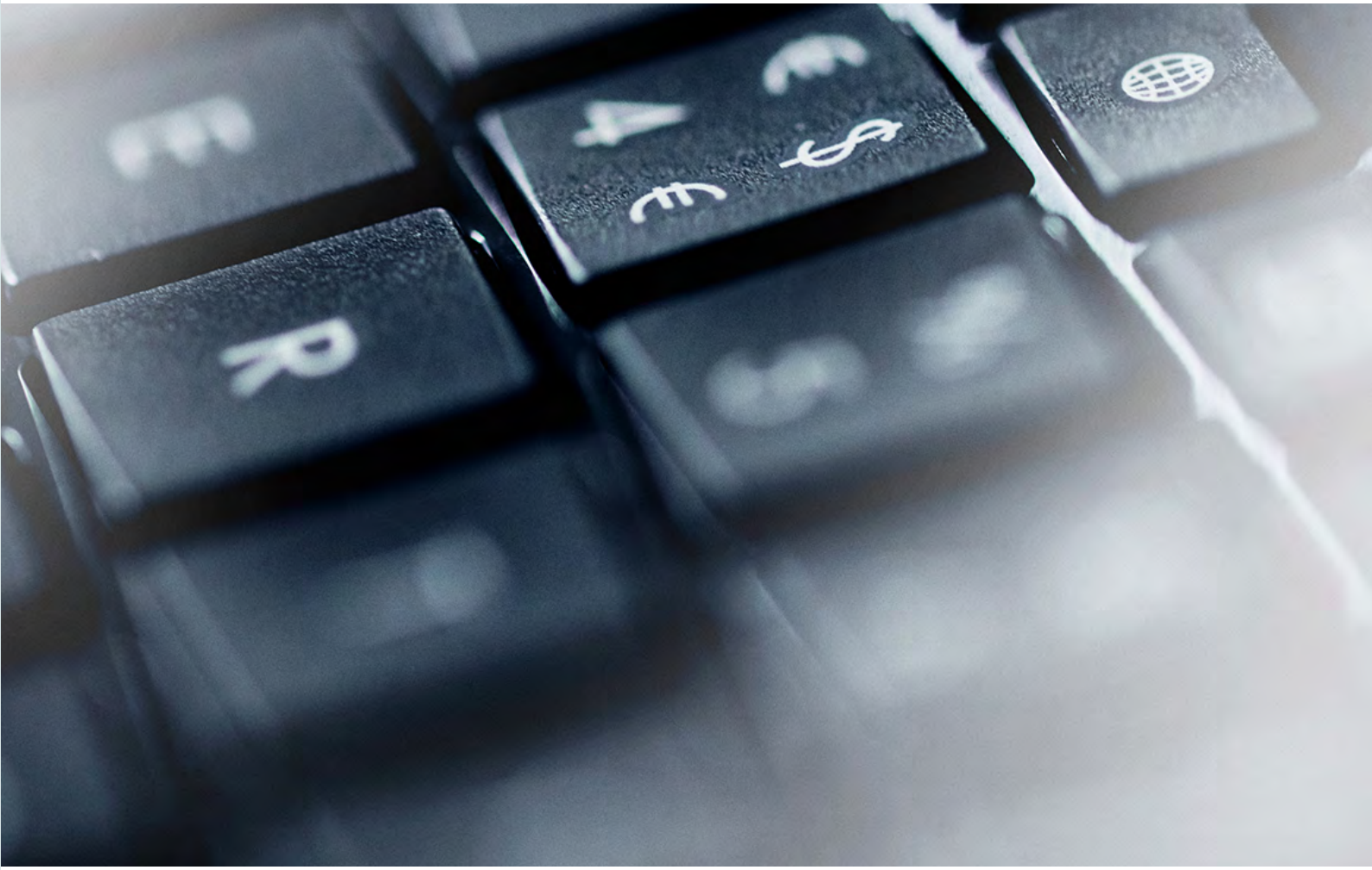


Figur 8 Barrierer i forhold til tavshedspligten



Figur 9 Barrierer i forhold til tavshedspligten udvidet





Andre situationer der kan skabe mistanke

Kampen mod hvidvask og terrorfinansiering via det finansielle system, som det er skildret ovenfor, skaber situationer med en svær balancegang. At reagere på mistanke kan komme samfundet til gode, men det kan også lægge kunden til last, hvis det viser sig, at der ikke er hold i mistanken. Pengeinstitutterne er ofte fanget mellem mange hensyn, og det skaber dagligt dilemmaer i bekæmpelsen af hvidvask og terrorfinansiering.

Yderligere situationer der kan skabe mistanke:

- En kunde indsætter et større beløb på sin konto, kunden fortæller, at det er en gevinst fra et kasino.
- En kunde ønsker en konto og udleverer de nødvendige oplysninger til pengeinstituttet, men kunden vil ikke eller kan ikke dokumentere, hvorledes kunden har tjent eller opnået midlerne. Kunden mener, at det er private oplysninger.
- En kunde får en basal indlånskonto til løn, men der foregår nogle usædvanlige transaktioner på kontoen, kunden rejser derefter ud af landet, hvorefter pengeinstituttet ikke kan få kontakt til kunden.
- En person har via borger.dk valgt en tredjemands NemKonto, som sin NemKonto, idet der ikke er et krav om, at man skal eje sin NemKonto. Der er nu forskel på, hvem der ejer kontoen, og hvem der får fx udbetalt offentlige ydelser på konto. Dette kan bevirke, at pengeinstituttet ikke kender den person, der bruger kontoen, fordi pengeinstituttet har indgået kundeforhold til den person, der rent faktisk ejer NemKontoen.
- Der foretages en mængde transaktioner imellem erhvervsvirksomheder, hvor forbindelsen ikke forekommer logisk.
- Omsætningen på virksomhedens konto er uforholdsmæssig stor i forhold til virksomhedens omsætning af varer eller tjenesteydelser.
- Et oprettet selskab henstår uden synderlig aktivitet og alene med få kontobevægelser

HVIDVASK TASK FORCENS ANBEFALINGER

Hvidvask Task Forcens arbejde har været delt i fem hovedspor, som har sat rammen for arbejdet de seneste 11 måneder:

1. Fælles it-løsninger
2. Øget samarbejde med myndighederne
3. Uddannelse
4. Selvregulering i form af adfærdsprincipper
5. Øget transparens

På baggrund af en kortlægning af status, en analyse af behov og en vurdering af mulige initiativer har Hvidvask Task Forcen udarbejdet en række anbefalinger til de fem hovedspor. Dertil kommer et afsnit om yderligere sektorinitiativer. Tilsammen udgør anbefalingerne et katalog af 25 konkrete anbefalinger.

Da bekæmpelse af hvidvask og terrorfinansiering er et samfundsansvar, fremhæves endelig nogle ønsker til politiske initiativer med det formål at optimere indsatsen. Målet er ved hjælp af samarbejde mellem sektoren, myndighederne og det politiske niveau at blive en af frontløberne i relation til bekæmpelse af hvidvask og terrorfinansiering på samme måde, som Danmark er i front, når det gælder fx antikorruption.

HOVEDSPOR 1:

FÆLLES IT-LØSNINGER

Et centralt tema er udbygning af fælles it-løsninger. På samme måde som det offentlige har pengeinstitutterne været både effektive og hurtige til at anvende digitale løsninger. Fælles løsninger på tværs af sektoren har desuden været en del af pengeinstitutternes DNA på andre områder.

Forebyggelse og bekæmpelse af hvidvask og terrorfinansiering er gennem de senere år kommet til at fylde mere i pengeinstitutternes arbejde. Også på dette område anvendes it-løsninger i vid udstrækning sammen med en meget markant anvendelse af menneskelige ressourcer. It-løsningerne på dette område har haft en tendens til at være siloprægede, hvor de tre datacentraler BEC, Bankdata og SDC samt Danske Bank og Nordea hver udarbejdede deres egen løsning på udfordringerne i forhold til hvidvask og terrorfinansiering. Det gælder "kend din kunde" (KYC, eller som det nu kaldes CDD), det gælder overvågning af transaktioner, det gælder underretninger til SØIK's Hvidvasksekretariat mv. Tiden er imidlertid kommet til at analysere mulighederne for at udbygge de fælles it-løsninger på hvidvaskområdet. Dette område bør ikke være genstand for konkurrence mellem pengeinstitutterne indbyrdes, men bør være et område hvor man arbejder sammen for at opfylde samfundskontrakten om forebyggelse og bekæmpelse af økonomisk kriminalitet i bred forstand, herunder hvidvask og terrorfinansiering. Samme synspunkt gør sig for så vidt gældende med hensyn til overholdelse af gældende lovgivning.

Kun gennem samarbejde og effektive it-løsninger kan vi vinde samfundets og pengeinstitutternes fælles kamp

Set fra et overordnet perspektiv vil der være en række fordele ved at etablere langt flere fælles it-løsninger for pengeinstitutterne, når det gælder forebyggelse og bekæmpelse af hvidvask. Det vil være omkostningsbesparende, det vil gøre det lettere og mere effektivt at samarbejde om bekæmpelse af hvidvask og terrorfinansiering, og det vil forbedre muligheden for at være avanceret, så man bedre kan bekæmpe økonomisk kriminalitet og "matche" de kriminelle.

Samtidig skal de fælles it-løsninger tage højde for, at der ikke nødvendigvis altid er tale om "one size fits all" på alle planer, men at pengeinstitutterne har forskellige størrelser, forskellige forretningsmodeller, forskellige kunder osv. Kunsten er derfor at sætte pengeinstitutternes mangfoldighed på formler og standarder, når det gælder AML-arbejdet, men samtidig i et vist omfang tage hensyn til deres forskellighed. Dette kræver, at de fælles it-systemer kan moduleres til forskellige pengeinstitutter med forskellige behov. Det fremtidige hvidvasksamarbejde forudsætter dog, at man har en standardiseret måde at anskue hvidvaskarbejdet ud fra, så der er en "fælles bund" for kampen mod hvidvask, hvor alle pengeinstitutter har en minimumsstandard, og hvor standardiserede løsninger benyttes i videst muligt omfang. Det vil også give en vis gardering mod, at finansielle kriminelle søger mod "det svageste led".

En standardisering vil også gøre det langt mere enkelt at samarbejde med myndighederne, hvilket vil være helt nødvendigt i fremtiden.

Det er vigtigt, at pengeinstitutterne allerede nu ruster sig til indførelsen af nye teknologiske løsninger på området. Anvendelse af lærende algoritmer, machine learning og kunstig intelligens (AI) forventes at blive en helt central del af AML-arbejdet og compliance inden for en overskuelig tidsramme, og som med så meget andet, gælder det om at være forberedt til at tage løsningerne ind, når de kommer. Det forudsætter, at man allerede nu sørger for at have tilstrækkelige, relevante og valide data med gode processer og fornøden dokumentation, sådan at det vil være muligt herudfra at iværksætte de lærende processer, som de nye teknologier kan muliggøre.

Hvidvask Task Forcens anbefalinger med hensyn til flere fælles it-løsninger falder i tre lag:

1. En minimumsløsning med 5 konkrete it-projekter, der kan medvirke til at øge effektiviteten.
2. En udbygning af sektorfælles AML-systemer.
3. En vision om sektorfælles it-samarbejde 2025.

Den finansielle sektor i Danmark har lang tradition for at samarbejde om opgaver, som ikke er konkurrencerelaterede. Samarbejder ses både på tværs af den samlede sektor, mellem grupper af pengeinstitutter, som har fælles behov, og som fælles løsninger i offentligt/privat samarbejde. Nedenfor følger eksempler på sådanne samarbejder. Listen er ikke udtømmende.

Fælles løsninger for hele sektoren

- De danske systemer til clearing og afvikling af detailbetalinger: sumclearingen, intradagclearingen (fra 2013) og straksclearingen (fra 2014).
- Dankortet, etableret 1983.
- Betalingsservice, operationelt fra 1974 under navnet PBS (Pengeinstitutternes BetalingsService).
- VP Securities (oprindeligt Værdipapircentralen), ejes af banker, realkreditinstitutter, børsmæglere, Nationalbanken og udstedere, etableret 1980.
- e-engagement – automatisering af bankskift siden 2015.
- NFCERT – Nordic Financial CERT (Computer Emergency Rescue Team) til deling af viden om cybertrusler. NFCERT er oprindeligt startet som en norsk finansiel CERT, men omfatter nu alle nordiske lande, og i Danmark, Island og Norge er de fleste banker medlemmer.

Fælles løsninger for grupper af pengeinstitutter

- De tre fællesejede datacentraler, SDC, BEC og Bankdata, som er grundlagt i henholdsvis 1963, 1965 og 1966.
- BOKIS (Betalings- Og KortIndkøbsSamarbejdet) Selskabets formål er at drive virksomhed med formidling af licenser til udstedelse af betalingskort og betalingsløsninger samt erhvervelse og levering af tjenester i denne forbindelse for Lokale Pengeinstitutters (LOPI) og Landsdækkende Bankers (LDB) medlemmer.

Fælles løsninger i offentligt/privat regi

- NemKonto, operationel i 2005. NemKonto er den konto, som alle offentlige myndigheder og en lang række private aktører bruger, når de skal udbetale penge til danske borgere.
- Digital Tinglysning – digitalisering af den tidligere papirbaserede tinglysningsproces, operationel fra 2009.
- NemID, operationel i 2010.
- NemID Nøgleapp., siden lanceringen i 2018 har næsten 2,6 mio. brugere downloadet app'en.
- MitID, der skal afløse NemID i 2021/2022.

Fælles løsninger i pipelinen

- Nordic KYC Utility, selvstændig virksomhed ejet af de seks største nordiske banker med det formål at udvikle ensartede on-boarding processer (KYC) for store erhvervskunder, forventes operationel medio 2020.
- P27, fælles nordisk clearing i DKK, SEK, NOK og EUR (Island er ikke med i projektet). Ejerkredsen bag P27 består af de seks største nordiske banker. Forventes operationel fra medio 2021.

Fem fælles it-projekter om hvidvask, der igangsættes nu – som minimumsløsning

e-nettet, som er finanssektorens digitaliseringsvirksomhed, er i sommeren 2019 af Finans Danmarks bestyrelse blevet bedt om at undersøge mulighederne for fælles it-løsninger inden for bekæmpelse af hvidvask og terrorfinansiering og komme med forslag til konkrete initiativer.

Hvidvask Task Forcen foreslår på den baggrund, at der snarest etableres 5 konkrete projekter - centreret om kend din kunde-princippet (KYC) og gennemført i regi af e-nettet.

1. KYC (kend din kunde) – Fælles standard for kundekendskabsprocedurer

Dette er en af grundstenene i at styrke samarbejdet på tværs af sektoren, da fælles definitioner af eksempelvis formål, omfang og risikovurdering af kundeforhold herved ensrettes, og kvaliteten højnes.

2. Pasvalidering

Der findes i dag en række udbydere af pasaflæsninger på markedet. Disse vurderer dog udelukkende, om passet er ægte eller uægte. e-nettet vil supplere de eksisterende løsninger med en løsning, der validerer, om der er et match mellem personens CPR-nummer og pasnummer, og om det er validt. Ved at udvikle en fælles sektorløsning vil det være muligt at validere, om pas og person er den samme ved opslag i Rigspolitiets pasregister.

3. PEP/RCA-register

Udbyderne på markedet af screening af PEP (politisk eksponerede personer) og sanktionslister er relativt mange, de har dog alle den udfordring, at screening af PEP'ers nærtstående og nære samarbejdspartnere (RCA'er) ikke fungerer effektivt, og derved er ekstra ressourcekrævende. Det er Hvidvask Task Forcens opfattelse, at løsning af dette problem, som er fælles for pengeinstitutterne, bør ske fælles, da det er uhensigtsmæssigt, at hvert enkelt pengeinstitut skal starte forfra på at finde disse oplysninger. Det er samtidig opfattelsen, at dette bør forankres i myndighedsregi, da det er yderst vanskeligt for pengeinstitutterne at opnå de relevante oplysninger, som er meget vanskeligt tilgængelige og højst usikre, og da netop et register over politisk eksponerede personer samt deres nærtstående og nære samarbejdspartnere synes nærliggende som myndighedsopgave.

4. Fælles dataregister

Hvidvask Task Forcen foreslår indførelse af et fælles register, der sammensætter data fra de ovenstående tre projekter. Det vil betyde, at sektoren samlet står stærkere specielt i forhold til at identificere de personer, der forsøger at udføre finansiel kriminalitet i ét pengeinstitut, og herefter forsøger at gøre det samme, blot i et anden pengeinstitut.

5. Kontoopslagsportal

Med gennemførelsen af EU's 5. hvidvaskdirektiv skal der etableres en it-løsning, der gør det muligt for efterforskningsmyndigheder som PET og SØIK hurtigt at kunne få oplysninger om, hvem der ejer en bankkonto eller bankboks. Oplysningerne er vigtige som led i efterforskningen for at kunne afdække, hvem der fx er involveret i en række mistænkelige transaktioner. Myndighederne kan allerede nu få adgang til disse oplysninger. Det kræver dog en dommerkendelse (en såkaldt editionskendelse), og man kan ikke tilgå oplysningerne samlet et sted. Sektoren ser det som en vigtig opgave at hjælpe myndighederne med at fremskaffe de nødvendige oplysninger. Kontoopslagsregistret rummer et stort potentiale i forhold til at muliggøre, at myndighederne kan få adgang til de relevante oplysninger tids nok til, at de kan nå at beslaglægge de kriminelles midler, inden de når at flytte dem. Sektoren har derfor besluttet i regi af Finans Danmark at stå for udviklingen af løsningen i samarbejde med myndighederne og at afholde udgifterne hertil.

Tendensen er i dag, at der i takt med kriminalitetens globaliserede og digitaliserede karakter i højere grad end tidligere samles oplysninger med det formål at bekæmpe cyberkriminalitet, anden form for grænseoverskridende kriminalitet, herunder hvidvask og terrorfinansiering og andre forhold, hvor kriminalitet kan bekæmpes mere enkelt og effektivt ved datadeling.

Det ses i England, hvor der i højere grad sker datadeling, og der er netop i Sverige igangsat en betænkning om datadeling, som forventes at føre til et lovforberedende arbejde. Betænkningen skal se på, om "Finansinspektionens" kapacitet, informationsdeling mellem pengeinstitutter og myndigheder samt myndighedernes samarbejde og ansvarsfordeling mod hvidvask er hensigtsmæssigt udformet.

Projekter til udbyggede sektorfælles AML-systemer

Mere udbyggede fælles it-løsninger og implementering tager mere tid. De vil kræve en markant indsats, massive investeringer, grundlæggende enighed om omfanget osv. Ikke desto mindre er der næppe tvivl om, at fælles it-løsninger vil være en fordel for branchen og branchens renommé, ligesom det netop vil være en investering, der må forventes at tjene sig hjem.

Det er både fra politisk side og fra branchens side ønsket, at Danmark positionerer sig og markerer sig som fremsynet og aktiv på hvidvaskområdet. Hvis kræfterne slås sammen, kan der opnås massive effektiviseringer samt økonomiske besparelser, idet fælles investeringer vil muliggøre mere effektiv bekæmpelse af hvidvask og terrorfinansiering, end hvis man investerer hver for sig og i forskelligt tempo.

På den baggrund foreslår Hvidvask Task Forcen, at der etableres et bredere samarbejde, når det gælder fælles it-løsninger med hensyn til hvidvaskbekæmpelse (AML) – og måske bredere bekæmpelse af økonomisk kriminalitet. Da dette vil være en proces, der kan kræve massive investeringer, knastørre kompetencer og en betydelig arbejdsindsats, anbefales det, at sektoren nu fastlægger de konkrete visioner for brug af fælles it-løsninger.

Vision for sektorfælles AML-samarbejde 2025

Dette er sket med en fælles vision for sektorfælles AML i erkendelse af, at der ikke bør være tale om et konkurrenceparameter, men om en fælles vision med flere fælles it-løsninger og øget samarbejde på området. Herved har man også bedre mulighed for at holde trit med de kriminelles fantasifuldhed med hensyn til nye metoder til hvidvask og terrorfinansiering. I forhold til at forpligte sig til et fælles AML-system har alle medlemmer af Finans Danmark tilkendegivet, at de via samarbejdet vil bidrage med viden i det omfang, projektet har behov for det. De vil bidrage med data efter de specifikationer, der aftales i sektoren, og som er nødvendige, for at løsningerne er værdiskabende for sektoren samlet set. e-nettet er i forlængelse af ovenstående blevet anmodet af Finans Danmark om at udarbejde et forslag til en langsigtet vision for det sektorfælles AML-samarbejde 2025.
Den overordnede vision er at bekæmpe og forebygge hvidvask og terrorfinansiering ved hjælp af digitale og datadrevne løsninger baseret på samarbejde mellem den finansielle og offentlige sektor. Visionen har som underliggende mål, at tilliden til den finansielle sektor bliver højere, at den daglige interaktion med pengeinstitutterne bliver nemmere for kunderne, at samarbejdet med den offentlige sektor styrkes, at omkostningerne for pengeinstitutterne bliver reduceret, og at Danmark herved kan blive et foregangsland inden for sektorfælles samarbejde.


METRO

Figur 10 AML / CFT Vision 2025

VISIONEN FOR DET SEKTORFÆLLES AML/CFT PROGRAM

Den langsigtede vision vil sætte retningen for de sektorfælles løsninger de kommende år.

GENNEM VISIONEN VIL VI:

01

Genetablere samfundskontrakten herunder højne tilliden til den finansielle sektor i forhold til at tage ansvar i kampen mod hvidvask og finansiering af terrorisme.

- Sikre en høj standard indenfor etik og ansvarlighed i bekæmpelse af hvidvask og finansiering af terrorisme i fællesskab.
- En sektorfælles indsats vil være et stærkt signal, om at sektoren er ambitiøs og vil ændre tilgangen i kampen mod hvidvask og finansiering af terrorisme. Dette vil forbedre sektorens image og styrke samfundskontrakten.

02

Gøre den daglige interaktion med pengeinstitutterne nemmere for borgere og virksomheder, samtidig med at det bliver sværere at begå hvidvask og finansiere terrorisme, da sektoren har de samme høje standarder.

- Gennem digitalisering og standardisering vil sektoren blive i stand til at dele viden i realtid, hvilket vil gøre det lettere for kunden at dele sine data og informationer med pengeinstituttet.
- Ydermere , vil de centraliserede services løfte den sektorfælles barre for sikkerhed og compliance, og derved gøre det sværere for kriminelle at finde "svage led", de kan udnytte.

AML VISION 2025

At bekæmpe og forebygge hvidvask og finansiering af terrorisme ved hjælp af digitale-og datadrevne løsninger baseret på samarbejde mellem den finansielle og offentlige sektor

03

Være foregangsland indenfor sektorfælles samarbejde og anvendelse af teknologi, hvilket vil være til gavn for både den finansielle sektor, og for det danske samarbejde.

- Samarbejde giver muligheder for at indføre nye teknologier billigere og hurtigere i hele sektoren.
- Anvendelse af nye og smartere teknologier såsom biometri, robotter, kunstig intelligens og avancerede arbejdsprocesværktøjer via en central service, vil forbedre mulighederne for at behandle store mængder data billigere og hurtigere, samtidigt med at indsatsen mod hvidvask og terrorfinansiering bliver mere effektfuld.

04

Styrke samarbejde med den offentlige sektor, hvilket vil effektivesere rapportering og efterforskning af mistænkelig adfærd og kan understøtte en genetablering af samfundskontrakten.

- At løse samfundsopgaver, kræver samfundsredskaber. Det styrkede samarbejde mellem myndigheder og den finansielle sektor skal understøtte udviklingen af de nødvendige løsninger.
- Regulering af lovgivning og samarbejde omkring krav til IT-løsninger vil kunne understøtte standardisering, og udveksling af data i realtid mellem myndigheder og den finansielle sektor.

05

Reducere omkostninger for de danske pengeinstitutter gennem digitalisering, stanardisering og stordriftsfordele.

- Et styrket sektorfælles samarbejde vil bane vejen for digitalisering og automatisering af hele AML/CFT økosystemet via centraliserede services. Dette vil eliminere de manuelle processer og reducere omkostningerne væsentlig i forhold til i dag.

I forhold til udmøntningen af visionen peges der konkret på etablering af en sektorfælles enhed, der skal ses som "en fællesejet serviceenhed, der strømliner indsamlingen, verifikationen, opbevaringen og delingen af data og dokumenter, der skal understøtte sektorens AML/ CFT-procedurer og processer. På sigt kan flere processer og procedurer centraliseres i enheden".

Figur 11 En sektorfælles utility

EN SEKTORFÆLLES UTILITY ER LØSNINGEN TIL AT OPNÅ VISIONEN

Det er en udvikling med mange trin undervejs og investeringerne i fremtidens løsninger skal ske nu

HVORDAN HÆNGER VISIONEN SAMMEN MED EN UTILITY?

- Den finansielle sektor skal gentænke måden hvidvask og finansiering af terrorisme bekæmpes på. Med et stigende pres for forandring fra både de interne og eksterne drivkræfter, kombineret med en større vilje til at tage et ansvar, er tiden inde til at ændre status quo.

- Behovet for forandring, kombineret med et komplekst sammenkoblet AML/CFT økosystem, gør en sektorfælles utility til den eneste langsigtede løsning, der kan imødekomme kravene, mitigere problemerne og tilbyde løsninger, der understøtter alle processerne i økosystemet.

- Ydermere, vil en fælles centraliseret utility tilbyde digitale og datadrevne løsninger, som vil højne standardiseringen og automatiseringen indenfor AML/CFT på tværs af sektoren.

- Det er vigtigt at understrege, at det at bygge en sektorfælles utilty ikke kan gøres ved et helt lineært og foruddefineret road map. At opnå visionen, kræver at alle i sektoren forpligter sig til retningen og engagerer sig i en løsning der kan gavne alle.

REJSEN FOR AT OPNÅ VISIONEN

Trin 1

Design af fundamentet for en fælles centraliseret utility

- Dette trin bygger på minimumsløsningen og indebærer en fælles platform med "simple" services.
- Formålet er at forbedre processer gennem digitalisering og standardisering, hvilket er fundamentet for en fælles platform.

Trin 2

Udvikling af en fælles centraliseret utility

- I trin 1 er formålet at standardisere og digitalisere processer, og i trin 2 skal alle processerne forbindes til hinanden i en fælles utility.
- Utilitien vil også gøre det muligt at indsamle og validere generiske KYC data, som herefter kan deles på tværs af sektoren mod samtykke.
- Derudover vil rapportering, vedrørende mistænkelig adfærd angående hvidvask og finansiering af terrorisme, også blive centraliseret.

Trin 3

Implementering af en fælles centraliseret utility

- I trin 3 er alle forudsætninger for at kunne udvikle en fuldt centraliseret utility på plads, hvilket inkluderer alle elementer i AML/CFT økosystemet.
- Centralisering, digitalisering og automatisering af alle AML/CFT processer vil højne sektorens evne til at bekæmpe og forebygge hvidvask og finansiering af terrorisme samtidig med at omkostningerne reduceres.
- En sektorfælles transaktions-monitoreringsservice vil være etableret og gøre det nemmere at kunne identificere kriminelles mønstre

Involvering af interessenter med særlig fokus på den offentlige sektor

Lovændringer

Digitalisering og automatisering

Opbygning af struktur og fundament for en utility

Kommunikation

Der er allerede eksempler på etablering af sektorfælles utilities (enheder). I Nordic KYC Utility er de seks største nordiske pengeinstitutter gået sammen om at etablere en selvstændig juridisk enhed, der kan stå for indsamlingen, valideringen og deling af generisk KYC-data for de største virksomheder i Norden. Samarbejdet skal gøre det enklere for kunder at samarbejde med pengeinstitutterne om at levere de oplysninger, som skal bruges til at identificere det usædvanlige og mistænkelige og reducere omkostningerne for sektoren i deres arbejde med at indsamle og validere data for store erhvervskunder.

Antallet af underretninger er de seneste år bare steget og steget, og det må forventes, at denne udvikling ikke stopper lige med det samme. Dette understreger også vigtigheden af, at man generelt bliver bedre til at arbejde sammen om at finde effektive og besparende løsninger. Det er derfor vigtigt, at arbejdet med etablering af en effektiv fælles it-understøttelse og centraliserede processer kræver et øget samarbejde med den offentlige sektor både i forbindelse med skabelsen og anvendelsen af nye løsninger og med hensyn til behov for justeret lovgivning. Det videre arbejde med it-løsninger vil derfor være tæt koblet med Hvidvask Task Forcens andet spor om øget samarbejde med myndighederne.

Den foreslåede sektorfælles utility kan være en fællesejet serviceenhed, der for eksempel kunne strømline indsamling, verifikation, opbevaring og deling af data, i det omfang, det er foreneligt med kravene til pengeinstitutternes individuelle håndtering og derved understøtte sektorens processer for bekæmpelse af hvidvask og terrorfinansiering. Processen i utilityens arbejde kan ses i tre trin. Et trin, der danner grundlag for minimumsløsninger, og som kan påbegynde det forberedende arbejde og derved skabe et fundament for visionen. Det næste trin, der skaber udviklingen, forbinder processerne og igangsætter de ideer, der udbygger minimumsløsninger og skaber nye it-løsninger. Dette omfatter blandt andet indsamling og validering af generiske kundekendskabsdata. Det sidste trin bygger på implementeringen af en fuldt centraliseret utility, der indeholder og varetager alle de fælles digitaliserede og automatiserede løsninger, som analysearbejdet har vist muligt, blandt andet en sektorfælles transaktionsmonitorering.

Hvidvask Task Forcens anbefaling om et langsigtet vidtgående sektorfælles AML/CTF-samarbejde er meget ambitiøs, og der skal i processen løses mange tekniske og regulatoriske udfordringer. Det vil fx kræve en ændret lovgivning, for at pengeinstitutterne kan dele kundedata. Hvidvask Task Forcen anbefaler derfor, at der hurtigst muligt igangsættes et forprojekt, der kortlægger præcis, hvad det vil kræve at realisere visionen.

Persondataforordningen

- Videregivelse af personoplysninger om et bestemt kundeforhold vil være behandling af persondata i persondataforordningens forstand og er dermed underlagt restriktioner. Behandlingen af oplysningerne vil normalt kræve samtykke, og den pågældende person vil have en række rettigheder i form af indsigtsret med mere.

- Persondataforordningen indeholder dog en række undtagelser, og behandling uden samtykke vil blandt andet kunne ske, hvis det er en opgave i samfundets interesse. Derudover er der mulighed for nationalt at fastsætte hjemmel til, at der kan undtages fra rettighederne i persondataforordningen. Dette kan fx ske i som led i myndighedernes kriminalitetsbekæmpelse.

HOVEDSPOR 2:

ØGET SAMARBEJDE MED MYNDIGHEDERNE

Det er Hvidvask Task Forcens opfattelse, at det har stor betydning for en effektiv bekæmpelse af hvidvask og terrorfinansiering, at der ofres stor energi fra både sektor og myndigheders side for i samarbejde at skabe så intelligente og finmaskede it-systemer som muligt, med tilsvarende mulige brede fælles rammer.
Samarbejdet mellem den finansielle sektor og myndighederne er således grundlæggende og meget afgørende for, med hvor stor succes man kan bekæmpe hvidvask, terrorfinansiering og anden finansiel kriminalitet.

Samfundsansvaret og samfundskontrakten bør føre til et hovedprincip om, at der stilles de samme værktøjer til rådighed for pengeinstitutter, når de arbejder med antihvidvask og terrorfinansiering, som myndighederne tildeles. Altså: Med samfundskontrakt bør følge samfundsværktøjer. Dette ligger til grund for en del af de forslag, der stilles nedenfor.

Gennem de seneste år er samarbejdet om de generelle forhold for bekæmpelse af hvidvask og terrorfinansiering blevet væsentligt udbygget og forbedret. Det gælder både hvad angår samarbejdet myndighederne imellem og samarbejdet mellem myndigheder og de private aktører. Det bør dog løbende være en prioritet at se på måder, hvormed samarbejdet kan forbedres yderligere.

Hvorfor er udbygget samarbejde mellem myndigheder og pengeinstitutter vigtigt – og vanskeligt

Mange af de myndigheder, der er involveret i arbejdet med forebyggelse og bekæmpelse af hvidvask og terrorfinansiering har hver deres egne karakteristika og deres egne it-systemer.

Nogle relevante data ligger hos Hvidvasksekretariatet i SØIK, nogle hos PET, nogle hos Finanstilsynet, nogle hos Erhvervsstyrelsen, nogle hos Skattestyrelsen, nogle hos Digitaliseringsstyrelsen, nogle hos politiet, nogle hos Udbetaling Danmark osv. Når dette sammenholdes med, at mange relevante oplysninger ligger hos pengeinstitutterne, er det tydeligt, at en udbygget brug af eksisterende data kan forbedre arbejdet med at forebygge og bekæmpe hvidvask og terrorfinansiering.

Der er derfor god grund til at udbygge samarbejdet

mellem myndighederne og pengeinstitutterne. Dette kræver først og fremmest mere viden om, hvilke hvidvaskrelevante data der ligger hvor. Denne viden vil være relevant både for myndighederne og for pengeinstitutterne. Herudover kræver udbygget samarbejde, at der sker en vis datadeling. Dette er et følsomt område, og det er vigtigt, at der tages behørigt hensyn til beskyttelse af personoplysninger og til myndigheders og pengeinstitutters tavshedspligt. Der er på dette område både for pengeinstitutterne og for det offentlige en vanskelig og sensitiv grænsedragning mellem beskyttelse af personoplysninger og det samfundsmæssige ønske om kriminalitetsbekæmpelse.

Det generelle dilemma må imidlertid ikke skygge for berettigede konkrete løsninger, hvor man ser på, hvilke slags oplysninger, der er tale om, hvor vigtigt det er at dele dem for at forbedre kriminalitetsbekæmpelsen, og hvordan man bedst muligt kan sikre den nødvendige beskyttelse af kunderne og deres persondata.

Når det gælder kriminalitetens karakter, har det betydning, om der er tale om store fisk eller små fisk. Hvis der er tale om terrorfinansiering eller hvidvask med underliggende meget alvorlig kriminalitet, fx menneskehandel, narkoimperier eller lignende må de fleste forventes at anerkende datadeling for at fange dem. Det samme gælder formentlig anden form for alvorlig kriminalitet, fx korruption. Altså: De store fisk berettiger til den store datadeling.

Ved de små fisk er dilemmaet af en anden karakter. Når vi taler sort arbejde eller socialt bedrageri vil datadeling i videre omfang klart kunne forbedre hvidvaskindsatsen. Om det skal ske, er først og fremmest et politisk valg.

Pengeinstitutterne har en næsten umulig opgave med at balancere på dette vanskelige område, og politisk klarhed vil være ønskelig. Der er således brug for politiske og måske samfundsmæssige drøftelser af, hvor grænserne skal sættes i denne sammenhæng. Bedre bekæmpelse af sort arbejde og socialt bedrageri kan spare samfundsmæssige omkostninger ved manglende skattebetaling og uberettigede ydelser. Hvor langt man ønsker, at det offentlige og pengeinstitutterne skal gå i denne retning, kræver politiske drøftelser med betoning af de iboende dilemmaer og graden af ihærdighed for at opdage sort arbejde og socialt bedrageri, således at de politiske signaler er klare.

Når det gælder beskyttelsen af kunderne og deres persondata, vil det spille ind, hvilke data der er tale om. Da der fortrinsvis er tale om økonomiske oplysninger, vil de normalt ikke kunne karakteriseres som særligt personfølsomme oplysninger. Konsekvenserne af at blive afvist som kunde kan imidlertid være voldsomme.

En alvorlig konsekvens kan være, hvis man afvises som kunde som følge af mistanke om terrorfinansiering eller alvorlig hvidvask. Selvom pengeinstitutterne foretager grundige undersøgelser, har de ikke mulighed for tilbundsgående undersøgelser. De skal derimod underrette Hvidvasksekretariatet hos SØIK, som foretager disse mere tilbundsgående undersøgelser. Det kan derfor ikke udelukkes, at pengeinstitutterne helt berettiget afviser en kunde ud fra deres muligheder for undersøgelse af mulig hvidvask, men at afvisningen viser sig uberettiget ud fra de mere grundige efterforskningsmæssige skridt. Sådanne "falsk positive" tilfælde er alvorlige for kunden. Det gælder, selvom der er tavshedspligt, og selvom der ikke sker domfældelse, men "blot" afvisning for en sædvane (fx afgivelse af kreditoplysninger) eller vurderes berettiget efter en konkret vurdering. Det vil være en konkret vurdering, hvornår det vil være berettiget at videregive oplysninger til brug for pengeinstitutternes indsats mod hvidvask, terrorfinansiering eller anden form for kriminalitet.

Lov om finansiel virksomhed (FIL)

- FIL § 117, stk. 1, fastlægger en tavshedspligt for pengeinstitutter og deres ansatte, De må ikke uberettiget videregive eller udnytte fortrolige oplysninger, de modtager, herunder alle oplysninger om konkrete kundeforhold.
- En berettiget videregivelse eller udnyttelse kræver en klar lovhjemmel, kundens samtykke, være udtryk

som kunde eller underretning af SØIK. Dette dilemma er allerede til stede nu og vil forstærkes i det omfang, der udveksles flere oplysninger.

Hvidvask Task Forcen anbefaler i forlængelse heraf, at man drøfter disse dilemmaer og ud fra en afvejning af oplysningernes karakter sammenholdt med kriminalitetens karakter ser på, hvordan man kan optimere det generelle samarbejde, herunder den generelle informationsudveksling, og på mulighederne for at udveksle oplysninger i konkrete sager. Særligt sidstnævnte er meget begrænset i dag, hvilket gør indsatsen mod hvidvask og terrorfinansiering langt mindre effektiv, end den kunne være.

Igangsatte samarbejdsfora

Hvidvask Task Forcen finder det velgørende, at der er nedsat en række samarbejdsfora, som kan medvirke til at forbedre informationer om den underliggende kriminalitet, erfaringsudveksling og samordning.

Figuren på side 50 giver et overblik over de fora, som Hvidvask Task Forcen har set på i forhold til myndighedssamarbejdet. Anbefalingerne til de enkelte fora vil blive gennemgået nedenfor i afsnittet.

Anbefalinger til det generelle samarbejde

I Danmark er der allerede nedsat eller planlagt en række fora til informationsudveksling, især om den underliggende kriminalitet, som ligger til grund for forsøg på hvidvask og terrorfinansiering. Regeringens strategi til bekæmpelse af hvidvask og terrorfinansiering fra september 2018 opererer med HvidvaskForum (for myndigheder) og Hvidvaskforum+ (for myndigheder og de forskellige relevante private sektorer). Formålet med Hvidvaskforum+ er at sikre udveksling mellem myndigheder og den private sektor af oplysninger om den generelle udvikling på AML-området. Hvidvasksekretariatets kvartalsrapporter om udviklingen på hvidvaskområdet er i den henseende også et vigtigt instrument.

Fra Finans Danmarks side har man dertil iværksat et forstærket samarbejde med myndighederne med omdrejningspunkt i afholdelse af kvartalsvise møder, hvor sektoren og relevante myndigheder kan have en dialog om overordnede trends og udviklingstendenser på området.

Som fremhævet tidligere i rapporten er der mange aktører (både private og offentlige) og flere forskellige lovgivninger i spil, når det gælder bekæmpelse af hvidvask og terrorfinansiering. Dette skaber en udfordring i forhold til at sikre en sammenhængende og koordineret tilgang hos de enkelte aktører og i de enkelte regelsæt.

For Hvidvask Task Forcen er det derfor en central pointe, at øget koordination og samarbejde mellem de relevante myndigheder på området er afgørende for en effektiv myndighedsindsats. Regeringens strategi på området og HvidvaskForum er begge vigtige skridt i den henseende.

Hvidvask Task Forcen vil i forlængelse heraf anbefale, at Hvidvaskforum gøres til et forum, der ikke kun understøtter videndeling og erfaringsudveksling, men også i lige så høj grad er med til at sikre en reel holistisk tilgang på tværs af myndigheder i form af fx fælles prioritering i tilsynsindsatsen.

Hvidvaskloven (HVL)

- Af HVL § 38 følger en særlig tavshedspligt for pengeinstitutterne, som har pligt til at hemmeligholde:
- 1) at der er sket underretning til Hvidvasksekretariatet i SØIK, 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.
- Pengeinstitutterne må dog gerne videregive oplysninger til andre virksomheder omfattet af hvidvaskloven om: 1) at der givet underretning, eller at dette overvejes, og 2) at der er eller vil blive iværksat en undersøgelse. Dette forudsætter dog, at 1) oplysningerne vedrører samme kunde og samme transaktion, 2) modtageren af oplysningerne er underlagt krav til bekæmpelse af hvidvask og terrorfinansiering, og 3) modtageren er underlagt tavshedspligt og pligt til at beskytte personoplysninger.
- Det betyder i praksis, at adgangen til at udveksle oplysninger mellem pengeinstitutter er begrænset til kun at gælde tilfælde, hvor der er tale om samme kunde og samme transaktion.

HvidvaskForum

- HvidvaskForum er lovfæstet i hvidvasklovens § 74 og består af en række af de myndigheder, der er involveret i bekæmpelse af hvidvask og terrorfinansiering. HvidvaskForum har blandt andet til formål:

  - at sikre et effektivt og konstruktivt samarbejde mellem myndighederne i bekæmpelsen af hvidvask og terrorfinansiering
  - at sikre koordinering og informationsudveksling mellem myndighederne.

- Gennem HvidvaskForum skal myndighedernes indsats styrkes. Desuden skal gennemførelsen af nationale og internationale forpligtelser understøttes, og effektiviteten af iværksatte foranstaltninger vurderes[18].

HvidvaskForum+

- HvidvaskForum+ er nedsat som led i den nationale strategi til bekæmpelse af hvidvask og terrorfinansiering 2018-2021. Forummet arrangeres af Finanstilsynet, hvor private aktører løbende kan drøfte problemstillinger og erfaringer med myndighederne, der deltager i HvidvaskForum. Finans Danmark deltager i HvidvaskForum+[19]

Fora på hvidvaskområdet

Kun for myndigheder	Både for myndigheder og den private sektor
HvidvaskForum - Tværgående myndighedssamarbejde.	**HvidvaskForum +** - Generel informationsudveksling om overordnede trends. - Finanstilsynet sidder for bordenden.
Operativt myndighedsforum - Tværgående myndighedssamarbejde.	**Bankforum** - Generel informationsudveksling mellem myndigheder og Finans Danmarks medlemmer. - Finanstilsynet sidder for bordenden.
	FEHT - Operationalt samarbejde mellem myndigheder og udvalgte medlemmer fra bankerne om konkrete sager. - Fortroligt forum hvor myndighederne sidder for bordenden.

De grå fora er allerede nedsat, mens de turkis er fora, der skal overvejes.

[18] *Kilde: National strategi til bekæmpelse af hvidvask og terrorfinansiering 2018-2021*
[19] *Kilde: National strategi til bekæmpelse af hvidvask og terrorfinansiering 2018-2021*

Hvidvaskforum+ inviterer relevante myndigheder på hvidvaskområdet og brancheorganisationer for de af hvidvaskloven omfattede virksomheder. På møderne i Hvidvaskforum+ er der mulighed for videndeling på et generelt niveau, der ikke omfatter deling af personfølsomme oplysninger eller konkrete sager.

Hvidvask Task Forcen ser etableringen af HvidvaskForum+ som et vigtigt tiltag, der kan understøtte videndeling og udveksling af best practices på tværs af sektorer. Det er dog vigtigt at have for øje, at der er tale om en bred deltagerkreds med hver deres udgangspunkt og eksponering for hvidvask og terrorfinansiering. Der vil derfor stadig være behov for sektorspecifikke fora, hvor den enkelte sektor sammen med myndighederne kan gå i dybden med de udfordringer, der gør sig gældende inden for den specifikke sektor.

Task Forcen anbefaler endvidere, at Datatilsynet i højere grad inddrages i HvidvaskForum og HvidvaskForum+. Mange af de udfordringer og ikke mindst muligheder, der er i forhold til at forbedre indsatsen, har også en persondataretlig vinkel. Desuden anbefales, at Digitaliseringsstyrelsen og måske Udbetaling Danmark inddrages.

Bankforum

I forlængelse heraf anbefaler Hvidvask Task Forcen, at der på det finansielle område etableres et bankforum, hvor myndigheder og sektoren har mulighed for at gå i dybden med udviklingstendenserne inden for sektoren. Dette vil kunne nyttiggøre de informationer, der findes hos myndighederne og effektivisere pengeinstitutternes arbejde med forebyggelse og bekæmpelse af hvidvask og terrorfinansiering. Et sådant OPP-samarbejde (Offentligt og Privat Partnerskab) vil kunne medvirke til en betydelig effektivisering af indsatsen mod hvidvask og terrorfinansiering.

I Bankforum vil der fx kunne arbejdes mere indgående med underretningerne fra pengeinstitutterne til Hvidvasksekretariatet, således at der sker en vis standardisering og kvalificering, som spiller konstruktivt ind i Hvidvasksekretariatets analysearbejde og samarbejde med fx politiet og skattemyndighederne mv. Der vil tillige kunne arbejdes med uddannelsesmæssige spørgsmål. Endvidere vil der kunne ske en erfaringsudveksling med hensyn til risikoen for "falsk positive" og problemer med begrundelsespligter, risikoen for "tipping off" af de kriminelle samt muligheder og udfordringer ved eventuel yderligere datadeling. Der vil ved konkrete drøftelser mellem deltagerne kunne lettes på de dilemmaer, som pengeinstitutterne møder (som skildret i rapportens afsnit "Dilemmaer"). Man vil kunne sikre en mere ensartet praksis og sikre, at den rigtige balance findes og følges der, hvor lovgivningen krydser eller skaber tvivl om mistanke. I dette forum vil der også kunne være mulighed for, at hvidvasklovens samspil med databeskyttelseslovgivningen kan drøftes med deltagelse fra Datatilsynet og Justitsministeriet.

Kvartalsrapport og feedback på underretninger fra Hvidvasksekretariatet i SØIK

Hvidvasksekretariatet udarbejder kvartalsrapporter over udviklingen i underretninger samt særlige fokusområder. Rapporterne er et værdifuldt redskab for pengeinstitutterne i deres tilrettelæggelse af deres indsats.

Task Forcen anbefaler dog, at Hvidvasksekretariatet ser på måder til i højere grad at kunne give feedback på de underretninger, som sektoren sender til myndighederne. Efter lovgivningen er der mulighed for, at Hvidvasksekretariatet kan give feedback på de konkrete underretninger. En mulighed, som Hvidvask Task Forcen gerne ser, at Hvidvasksekretariatet i højere grad benytter sig af. Med over 30.000 underretninger årligt (et tal, der ser ud til at stige de kommende år), vil det selvsagt dog også være et spørgsmål om ressourcer. Som alternativ vil Hvidvask Task Forcen derfor anbefale, at Hvidvasksekretariatet ser på måder til at udbygge kvartalsrapporterne.

Anbefalinger til øget samarbejde i konkrete sager

Mulighederne for at udveksle oplysninger og erfaringer om konkrete sager er meget begrænsede i dag, hvilket gør indsatsen på området mindre effektiv. Både fra FATF og fra Europa-Kommissionen opfordres der til en effektivisering af bekæmpelsen af hvidvask og terrorfinansiering, blandt andet ved at koordinere og udveksle oplysninger om konkrete sager og om de kriminelle, der udnytter det finansielle system.

I den forbindelse har Hvidvask Task Forcen ladet sig inspirere af det samarbejde der foregår mellem de engelske myndigheder og den finansielle sektor.

Danske forhold

I Danmark er der som nævnt allerede nedsat eller planlagt en række fora til informationsudveksling. En operativ arbejdsgruppe lig den britiske JMLIT er dog ikke etableret i Danmark. Af den nationale risikostrategi fremgår det, at det skal overvejes, om der er behov for at nedsætte en stående arbejdsgruppe, hvor konkrete efterforskningssager kan drøftes med udvalgte private aktører. I det politiske samarbejde i forligskredsen er det både i efteråret 2018 og atter i marts 2019, forudsat at rammerne for et samarbejde i bekæmpelsen af hvidvask og terrorfinansiering skal forbedres.

Efter Hvidvask Task Forcens vurdering er der behov for at kunne udveksle oplysninger i konkrete sager for effektivt at kunne bekæmpe hvidvask og terrorfinansiering. En stående fortrolig arbejdsgruppe vil kunne være en måde at facilitere dette på, herunder håndtere nogle af de rejste bekymringer ved en øget udveksling af information.

Et forslag til en dansk udgave blev præsenteret på Hvidvask Task Forcens konference 28. august 2019. Ideen blev godt modtaget af de tilstedeværende politikere – dog med betoning af vigtigheden af persondatabeskyttelse. I et senere møde med Datatilsynet er tilkendegivet, at der ikke umiddelbart synes at være persondataretlige problemer i relation til en sådan løsning.

Dansk JMLIT: Den Fælles Efterretningsenhed for Hvidvask og Terrorfinansiering

Det er derfor Task Forcens opfattelse, at der bør etableres en operativ enhed. En enhed som Hvidvask Task Forcen foreslår navngivet "Den fælles Efterretningsenhed for Hvidvask og Terrorfinansiering".
I lighed med den engelske JMLIT er det Hvidvask Task Forcens opfattelse, at den fælles efterretningsenhed skal etableres i regi af det offentlige med relevante deltagere fra SØIK, Hvidvasksekretariatet, Politiet, Skattestyrelsen, PET, eventuelt FE og repræsentanter fra den finansielle sektor. Fra sektorens side skal der udvælges repræsentanter fra en række institutter. Repræsentationen bør her modsvare sammensætningen af Finans Danmarks medlemskreds. En model vil her kunne være, at sammensætningen som udgangspunkt svarer til sammensætningen i Finans Danmarks juridiske udvalg, og at LOPI udpeger repræsentanter fra de små institutter.

Med det formål at tilgodese ønsket om persondatabeskyttelse bør møderne i arbejdsgruppen være fortrolige, og deltagerne skal være sikkerhedsgodkendt. Dette er en forudsætning for, at der kan udveksles klassificerede oplysninger. Begrænsningen af udvekslingen af fortrolige oplysninger til at foregå i et fortroligt forum, hvor deltagerne er underlagt tavshedspligt, vil kunne skabe grobund for at lempe den ellers relativt restriktive

Regeringen vil oprette et operativt myndighedsforum med deltagelse af SØIK, Hvidvasksekretariatet, PET, Rigspolitiet, Finanstilsynet, Erhvervsstyrelsen, Skattestyrelsen og Spillemyndigheden for at styrke det tværgående myndighedssamarbejde om bekæmpelse af hvidvask og terrorfinansiering. Der er tale om en operativ myndighedsgruppe, hvor myndighederne kan lægge viden på bordet om personer eller overførsler, de har mistanke til.

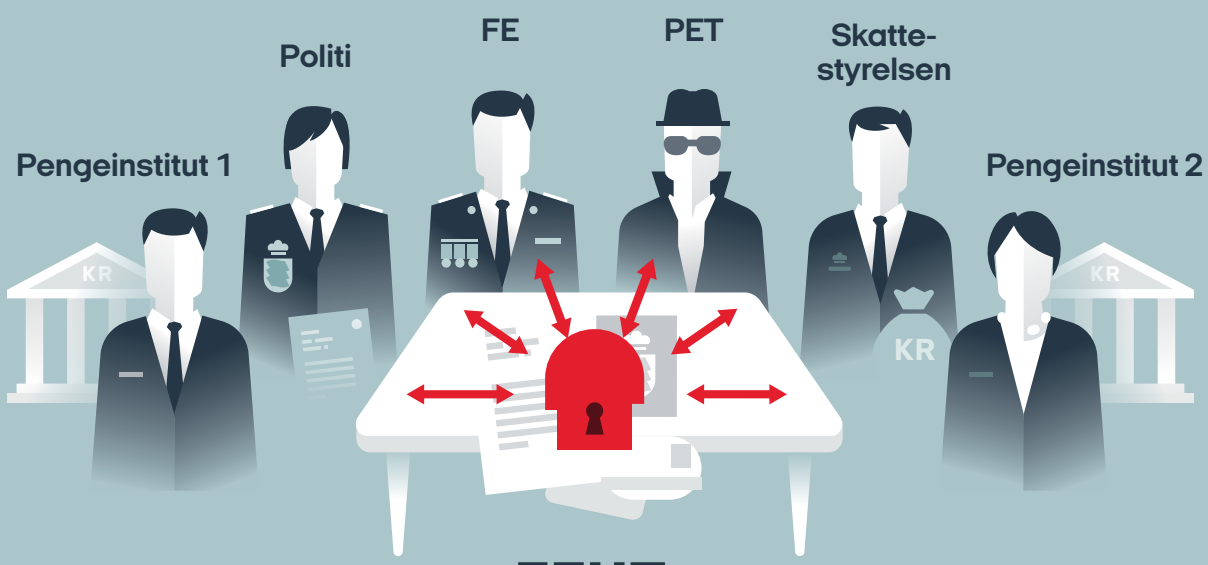
lovgivning på området. Der skal tilsvarende være krav til dokumentationen, da der ikke må herske tvivl om, hvad der behandles i det fortrolige forum.

Udfordringen i at konvertere den britiske JMLIT-model og særligt operationsgruppen til Danmark består primært i den relativt begrænsede adgang, som dansk lovgivning sætter for at udveksle oplysninger inden for den finansielle sektor. Det gælder især lov om finansiel virksomhed og hvidvaskloven. Det er derfor vigtigt, at der skabes en klar lovhjemmel for at have et forum med samme type informationsudveksling som den engelske JMLIT.

JMLIT (Joint Money Laundering Intelligence Taskforce)

I England foregår samarbejdet mellem myndigheder og den finansielle sektor i et Offentlig Privat Partnerskab (OPP) mellem de engelske myndigheder og den finansielle sektor. Målet er – gennem et effektivt samarbejde – at forebygge og bekæmpe hvidvask, terrorfinansiering og økonomisk kriminalitet. Der er fokus på samarbejde om udveksling af informationer og analyser, hvor omdrejningspunktet er hvidvask, terrorfinansiering og økonomisk kriminalitet. Samarbejdet foregår på både strategisk og taktisk niveau.

- Dels i en "Ekspert arbejdsgruppe", hvor der udveksles viden og ekspertise for at forbedre forståelsen af baggrunden og metoderne for samt truslerne ved hvidvask og terrorfinansiering. Dette anvendes til udvikling af typologier for "alarmer" og "red flags" med henblik på at finde mitigerende foranstaltninger for at forebygge kriminelles udnyttelse af det finansielle system.
- Dels i en "Operativ arbejdsgruppe", hvor repræsentanter fra myndighederne og den finansielle sektor mødes hver uge i et fortroligt forum for at udveksle og drøfte efterretninger i konkrete sager.
- Hjemlen til udvekslingen af oplysninger i den operative arbejdsgruppe er givet i en særskilt lov (Section 7 of the Crime and Courts Act 2013) og rammerne for JMLIT'en er detaljeret reguleret i en overenskomst, der er indgået imellem myndighederne og den finansielle sektor.
- Lignende ordninger er eller er ved at blive indført andre steder i EU, herunder Holland, Irland og Tyskland. Endvidere er JMLIT'en blevet fremhævet som et best practice eksempel af blandt andre FATF.



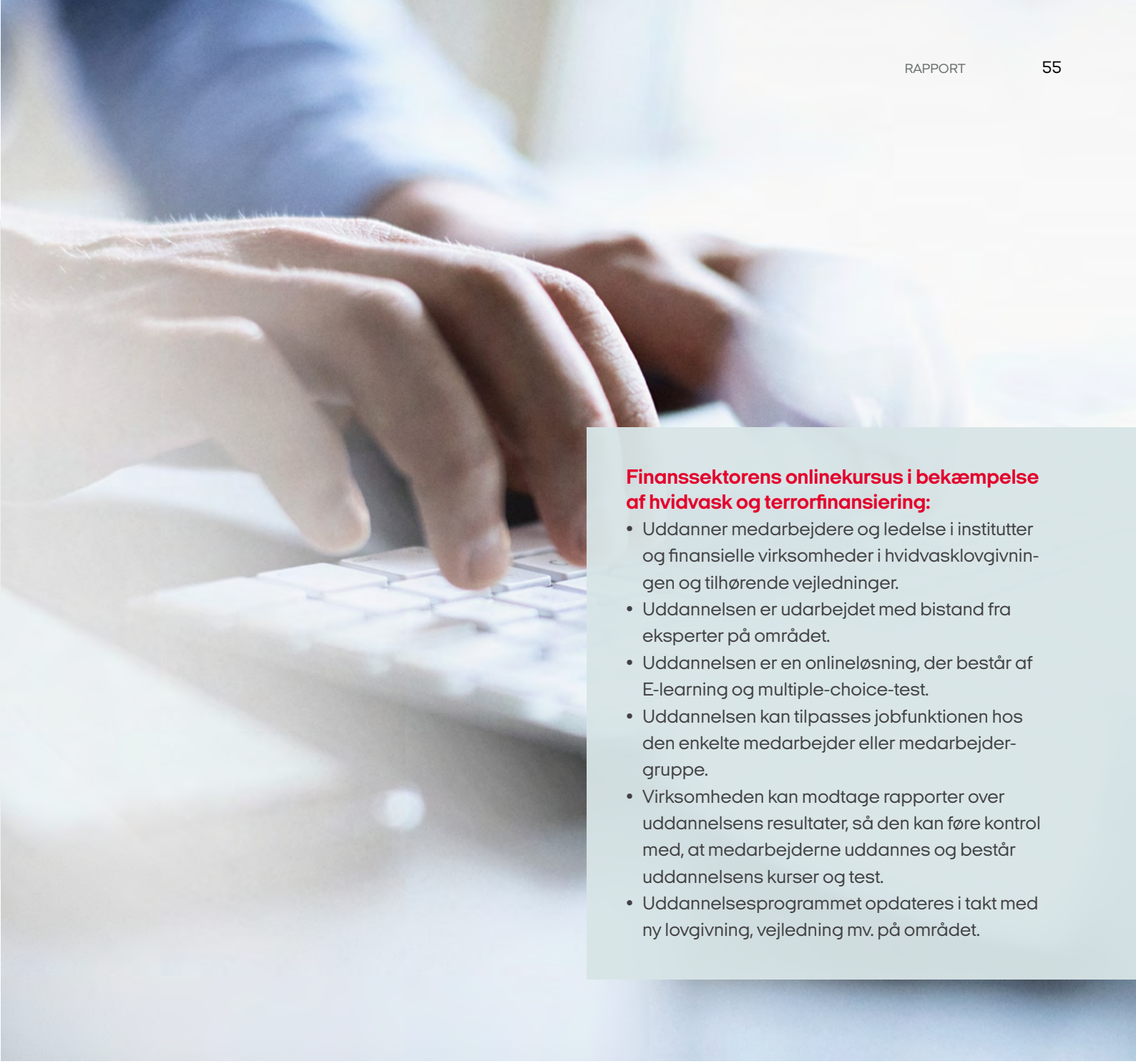
FEHT

Den Fælles Efterretningsenhed
for Hvidvask og Terrorfinansiering

Løsningsmodel – forslag til lovændring

Hvidvask Task Forcen anbefaler, at der indføres en særskilt bestemmelse i hvidvaskloven, der inden for rammerne af persondataforordningen og lov om finansiel virksomhed giver hjemmel til, at myndighederne nedsætter en arbejdsgruppe, hvor det er tilladt at udveksle fortrolige oplysninger. Systemet synes at virke godt i England, ligesom løsningen er anbefalet af den globale organisation FATF og har givet anledning til interesse i en række andre lande, herunder Tyskland. Der bør derfor også i en dansk kontekst kunne etableres passende foranstaltninger til at sikre persondatabeskyttelse, fortrolighed og dokumentationskrav i lyset af, at der især sigtes til "de store fisk" i den øvre ende af hvidvaskskalaen.

En indførelse af en dansk FEHT vil være udtryk for det angivne hovedsynspunkt om, at pengeinstitutternes vigtige samfundsopgave i relation til forebyggelse og bekæmpelse af hvidvask og terrorfinansiering, bør medføre, at pengeinstitutterne også tillægges mulighed for videndeling på linje med de myndigheder, der varetager samme slags opgaver. Med samfundsopgaven bør følge værktøjer, der svarer hertil.



Finanssektorens onlinekursus i bekæmpelse af hvidvask og terrorfinansiering:

- Uddanner medarbejdere og ledelse i institutter og finansielle virksomheder i hvidvasklovgivningen og tilhørende vejledninger.
- Uddannelsen er udarbejdet med bistand fra eksperter på området.
- Uddannelsen er en onlineløsning, der består af E-learning og multiple-choice-test.
- Uddannelsen kan tilpasses jobfunktionen hos den enkelte medarbejder eller medarbejdergruppe.
- Virksomheden kan modtage rapporter over uddannelsens resultater, så den kan føre kontrol med, at medarbejderne uddannes og består uddannelsens kurser og test.
- Uddannelsesprogrammet opdateres i takt med ny lovgivning, vejledning mv. på området.

HOVEDSPOR 3:

UDDANNELSE

Pengeinstituttet skal sikre, at ansatte og pengeinstituttets ledelse har modtaget tilstrækkelig undervisning i hvidvasklovgivningen og relevante krav om databeskyttelse[20]. Kravet om tilstrækkelig uddannelse indebærer også efteruddannelse med passende intervaller[21]. De fleste danske pengeinstitutter gør i dag brug af Finanssektorens Uddannelsescenter, der udbyder et uddannelsesprogram på hvidvask og terrorfinansieringsområdet. Danske Bank og Nordea har udarbejdet egne uddannelsesprogrammer på området.

[20] *Kilde: Hvidvasklovens § 8, stk. 6.*
[21] *Kilde: Finanstilsynets vejledning om hvidvaskloven afsnit 7.*

Statistik og status pr. 14 august 2019[22]:

Antal virksomheder, der bruger Finanssektorens uddannelsescenters onlinekursus til bekæmpelse af hvidvask og terrorfinansiering.

Antal medarbejdere, der har gennemført onlinekurset siden 2017.

Kun få procent består ikke inden for 3 forsøg. I de tilfælde anbefaler Finanssektorens Uddannelsescenter, at virksomheden udarbejder en handlingsplan med medarbejderen i form af mere uddannelse, sidemandsoplæring mv., inden der tildeles et 4. forsøg.

Nordeas uddannelse på området for bekæmpelse af hvidvask og terrorfinansiering:

Nordea har inddelt uddannelsen i tre kategorier:

- Generel uddannelse, funktionsspecifik uddannelse og ekstern certificering.
  Den generelle uddannelse er obligatorisk for alle Nordeas medarbejdere ca. 30.000. Uddannelsen varer en time og gentages hvert år. Det er et krav, at uddannelsen bestås, for at medarbejderen har såkaldt "Licence to work". Uddannelsen omfatter følgende elementer:
  - Kend din kunde
  - Bekæmpelse af hvidvask
  - Bekæmpelse af terrorfinansiering
  - Overholdelse af internationale sanktioner
  - Forebyggelse af bestikkelse og korruption
  - Forebyggelse af skatteunddragelse
- Den funktionsspecifikke uddannelse dækker alle medarbejdere, der har kundekontakt eller arbejder med antihvidvask og terrorfinansiering ca. 13.000 medarbejdere. Medarbejdere med specialistfunktioner vedrørende finansiel kriminalitet får yderligere løbende obligatorisk uddannelsen inden for deres respektive fagområder.
- Den eksterne certificering opnås fra International Compliance Association (ICA) og omfatter medarbejdere, der fuldtid arbejder med bekæmpelse af finansiel kriminalitet. Ultimo 2019 har ca. 465 medarbejdere gennemført et eksternt certificeringsprogram. Programmerne har en varighed på 3-9 måneder.

[22] *Kilde: Data fra Finanssektorens Uddannelsescenter*

Danske Banks uddannelse på området for bekæmpelse af hvidvask og terrorfinansiering:

- Alle Danske Banks medarbejdere gennemgår et grundmodul i bekæmpelse af hvidvask og finansiering af terrorisme.
- Danske Banks uddannelse giver indblik i, hvorfor bekæmpelse af hvidvask og terrorfinansiering er vigtigt for det enkelte individ, samfundet og Danske Bank.
- Derudover har Danske Bank en række forskellige overbygningsmoduler, der er målrettet, alt efter hvilken type af funktion den enkelte medarbejder varetager, f.eks. har Danske Bank moduler om optagelse af nye kunder, sanktioner, overvågning og transaktioner samt korrespondentforbindelser.
- De funktionstilrettede moduler giver indsigt i, hvilke typer af adfærd man skal være særligt opmærksom på inden for det enkelte område.
- Alle modulerne er udviklet til at kunne uddanne medarbejderne i de lovgivningsmæssige krav, og samtidig indeholder de eksempler, cases og instruktioner, der er skræddersyet til Danske Banks processer og rammer.
- Modulerne bliver løbende opdateret og tilrettet ny lovgivning, risikoindikatorer og udvikling på området.
- Danske Bank har også særligt tilrettede træningsprogrammer og sidemandsoplæring for de medarbejdere, der håndterer kundekendskab på nye kunder og løbende opdatering af kundekendskabsoplysninger.
- Derudover anvender Danske Bank også et internationalt certificeret uddannelsesprogram inden for området for bekæmpelse af hvidvask og terrorfinansiering.

Den internationale ICA-uddannelse:
International Compliance Association (ICA) er en international udbyder af uddannelse og certificering inden for compliance og den regulatorisk bekæmpelse af finansiel kriminalitet. ICA udbyder et stort antal uddannelsesprogrammer/certificeringer om blandt andet hvidvaskbekæmpelse, bekæmpelse af terrorfinansiering, bekæmpelse af finansiel kriminalitet, bekæmpelse af korruption, hvidvasklovens regler om kundekendskab m.fl.

Udbygning

Hvidvask Task Forcen har drøftet området for uddannelse og det uddannelsesgrundlag, der ligger i dag. Det vigtige ved en uddannelse i bekæmpelse af hvidvask og terrorfinansiering er, at der uddannes i hvidvasklovgivningens regler, men også at der er mulighed for, at uddannelsen bliver sektorspecifik og ikke mindst institutspecifik. Medarbejderen skal forstå den overordnede risiko og budskabet i loven og samtidig også forstå, hvordan loven efterleves i den konkrete virksomhed med dennes forretningsmodel og i den konkrete jobfunktion, som medarbejderen varetager. Det enkelte pengeinstitut vil altid individuelt skulle sikre, at medarbejderen har tilstrækkelig uddannelse i pengeinstituttets konkrete foranstaltninger til forebyggelse af hvidvask og terrorfinansiering.

Yderligere casebaseret uddannelse og erfaringsudveksling

Hvidvask Task Forcen har vurderet, at det uddannelsesgrundlag, der er i dag dækker bredt, men også at der er potentiale for, at det kan udvides og forbedres yderligere. Det kan især ske ved at supplere med flere praktisk håndgribelige eksempler eller cases. Herved vil forståelsen for de konkrete dilemmaer kunne øges, der vil kunne ske udveksling af erfaringer baseret på konkrete situationer, og regelgennemgangen vil kunne suppleres med en mere praktisk betonet tilgang.

Som led i uddannelsen og erfaringsudvekslingen vil det være naturligt at arbejde med underretningerne til Hvidvasksekretariatet i SØIK. Herved kan underretningerne i højere grad kvalificeres, standardiseres og udbygges, således at de bedst muligt tjener deres formål. En standardisering vil også kunne understøtte Hvidvasksekretariatets analysearbejde.

Sektorløsninger

Der er også mulighed for at øge samarbejdet og højne uddannelsen på tværs af sektoren ved at benytte sektorens fælles praktiske erfaring. Det kan eksempelvis ske ved at udarbejde cases, der illustrerer kædesvig, socialt bedrageri og andre lignende scenarier, der omfattes af begrebet for hvidvask eller terrorfinansiering. Sådanne cases vil også hjælpe til, at begreberne for hvidvask og terrorfinansiering i højere grad bliver praktisk forståelige for medarbejderen.

Hvidvask Task Forcen anbefaler, at der for medarbejdere på hvidvaskområdet er kurser med erfaringsudveksling, casearbejde og dilemmaer. Herved vil der blive sikret fokus på de mange konkrete beslutninger, der skal træffes med hensyn til kundekendskabsprocedurer, onboarding og off-boarding, risikoinddeling, kriterier for transaktionsmonitorering mv. Det anbefales i forlængelse heraf, at Finans Danmark afholder halvårlige konferencer med mulighed for erfaringsudveksling på området. På denne måde kan der igangsættes en udvikling, der kan medvirke til øget ensartethed i praksis.

Certificering

Hvidvask Task Forcen har i forlængelse af dette vurderet, om der burde indføres en egentlig certificering. Vurderingen har været, at en egentlig certificering ikke vil være en smidig løsning, da den ikke på samme vis kan tilpasses den konkrete forretningsmodel eller suppleres af institutspecifikke forhold. Desuden er det vigtigt, at uddannelsen løbende opdateres for nye regler og erfaringer i sektoren, hvilket nødvendiggør efteruddannelse og herved gør en enkeltstående certificering mindre hensigtsmæssig. Et egentligt krav til certificering skønnes ikke at være i lovens ånd, hvor fokus er på, at ledelsen og medarbejderne skal forstå den forretningsmodel og såkaldte iboende risiko, der følger med forretningsmodellens geografi, kundetyper, produkter og tjenesteydelser, samarbejdspartnere mv. Endvidere vil en certificeringsløsning ikke på samme vis som uddannelse imødekomme behovet for at sikre en kontinuerlig og smidig løsning, der ved ændringer i lovgivningen, i nationale risikovurderinger, i pengeinstituttets egne forretningsgange mv., skal efteruddanne medarbejderen.

HOVEDSPOR 4:

ADFÆRDSPRINCIPPER

Reguleringen af hvidvask er usædvanlig intens. Der er krav om hvidvaskpolitikker, krav til organiseringen af hvidvaskarbejdet, krav om en hvidvaskansvarlig osv. Desuden er straffereglerne gennem flere omgange skærpet meget betydeligt. Selvom lovgivninger, vejledninger, EU-direktiver, EBA-principper mv. om hvidvask er yderst detaljerede, opstår mange dilemmaer og valg, når det gælder den nærmere udmøntning af reglerne i praksis. Pengeinstitutternes konkrete adfærd varierer betydeligt, idet dilemmaer og valg håndteres forskelligt i de forskellige pengeinstitutter. Der har været tale om forskellige kulturer i forhold til at løfte indsatsen. Alle med udgangspunkt i lovgivning – men også med udgangspunkt i egne systemer, uddannelser og fokus. Hvidvask Task Forcen har på den baggrund ønsket at komme med et sæt fælles adfærdsprincipper til bekæmpelse af hvidvask og terrorfinansiering, som kan ensarte kulturen på tværs.

Hvorfor er fælles adfærdsprincipper et gode?

Formålet er at forbedre indsatsen mod hvidvask og terrorfinansiering og sikre en ambitiøs indsats. Som led heri er det et mål, at alle medlemmer af Finans Danmark følger ensartede principper, hvilket også understøtter opfattelsen af, at der ikke bør være tale om et konkurrenceparameter, men netop en fælles indsats baseret på fælles adfærd. Hertil kommer et ønske om at synliggøre ændringer og forbedre transparensen af pengeinstitutternes indsats. Endelig ser Hvidvask Task Forcen fælles adfærdsprincipper og en fælles kultur som en bærende forudsætning for, at sektoren i højere grad kan samarbejde på tværs og gennemføre Task Forcens anbefalinger inden for de andre hovedspor.

Hvidvask Task Forcen har ladet sig inspirere af lignende såkaldte "Codes of Conduct" eller "Guidelines" i andre lande. Således har fx Holland arbejdet meget med guidelines.

Holland: Den hollandske bankforening NVB har udarbejdet en ed for de ansatte i den hollandske banksektor. Denne "bankers' oath" indeholder følgende retningslinjer:

Oath and discipline

Along with the introduction of a social charter and updating the Banking Code, the Dutch banking industry has also taken the initiative to implement an ethics statement [see annexe]. The Dutch banks intend this to show that everyone working in the industry is bound by the codes of conduct attaching to this statement for the ethical and careful practice of his/her profession. Employees have personal responsibility for complying with those codes of conduct and can be held accountable for non-compliance.

Since early 2013, policymakers and supervisors of financial institutions have by law had to sign the ethics statement, now better known as the bankers' oath. The initiative to have all bank employees take the oath will be a significant tool in creating the new culture wanted in the banking industry. A form of disciplinary scheme will be introduced to ensure that taking the oath is not without meaning. Bank employees will, therefore, be accountable to society as a whole.

Bankers' Oath

Form for the oath/affirmation by an employee other than a director or member of a body charged with supervision of policy and the general affairs of the business.*

I swear/promise that within the limits of the position I hold at any time in the banking industry:

- I will execute my function ethically and with care;
- I will draw a careful balance between the interests of all parties associated with the business, being the customers, shareholders, employees and the society in which the business operates;
- when drawing that balance, I will make the customers' interests central;
- I will comply with the laws, regulations and codes of conduct that apply to me;
- I will keep confidential that which has been entrusted to me;
- I will not abuse my knowledge;
- I will act openly and accountably and I know my responsibility to society;
- I will make every effort to retain and improve trust in the financial sector.

So help me God/This I declare and promise.

The oath/affirmation was taken/made in the above form on [date], at [place], before [name of person who administered the oath] in the presence of [name of other representative of the business or industry or professional organisation].
Furthermore, [name of the person] confirmed his/her acceptance of the enforcement of the codes of conduct by the Disciplinary Committee and the exercise of authority by the Director General pursuant to the disciplinary scheme in the banking industry codes of conduct.

Name [signature]

* The final text will be brought into line with the text of the Dutch Financial Supervision Act

Finanstilsynet stiller nu krav om en politik, der skal sikre sund virksomhedskultur. Kravet følger af den politiske aftale af 19. september 2018.

Forpligtelsen til at have en politik for sund virksomhedskultur gælder for pengeinstitutter, e-pengeinstitutter og betalingsinstitutter. Politikken skal vedtages af bestyrelsen og skal udtrykke forventningerne til samtlige medarbejderes adfærd og aktive medvirken til forebyggelse af blandt andet hvidvask og anden økonomisk kriminalitet. De nærmere krav til politikken vil Finanstilsynet indarbejde i en bekendtgørelse[23].

Det er imidlertid afgørende, at adfærdsprincipperne føles naturligt for pengeinstitutterne i Danmark i deres hverdag, og det er derfor valgt at udforme principperne ud fra et ønske om at lade den danske kontekst få afgørende indflydelse.

På den baggrund er der lagt afgørende vægt på den daglige adfærd, herunder kulturen i pengeinstitutterne med hensyn til de samfundsmæssige opgaver. Dette ligger i naturlig forlængelse af Finanstilsynets øgede fokus på netop sund virksomhedskultur.

Pengeinstitutternes opgaver er først og fremmest af økonomisk og rådgivningsmæssig karakter, hvor fokus er på afkast, renter, investering, omkostninger osv. Den økonomiske dagsorden er imidlertid gennem de senere år blevet suppleret med samfundsopgaver og samfundsansvar i form af forebyggelse og bekæmpelse af hvidvask og terrorfinansiering, ligesom bæredygtighed, social ansvarlighed mv. fylder stadig mere. Det er naturligt, at der på den baggrund er behov for en nuancering af kulturen, således at samfundsansvaret bliver en mere integreret og synlig del af pengeinstitutternes hverdag. Det synes tilsvarende naturligt, at dette sker på sektorniveau, således at der etableres ensartethed og fælles fodslag i stedet for silotænkning og siloløsninger.

Som led i ønsket om at videreudvikle pengeinstitutternes indsats med hensyn til forebyggelse og bekæmpelse af hvidvask og terrorfinansiering har Hvidvask Task Forcen derfor udarbejdet 6 adfærdsprincipper. Adfærdsprincipperne er baseret på en række udtrykkelige grundholdninger om pengeinstitutternes indsats i relation til forebyggelse og bekæmpelse af hvidvask og terrorfinansiering. Disse er markeret i de indledende bemærkninger. Med dette udgangspunkt opstilles et hovedprincip i en overskrift. Dette udmøntes herefter i et par nærmere beskrivelser af, hvad det betyder for pengeinstitutternes daglige adfærd og indsats i arbejdet med forebyggelse og bekæmpelse af hvidvask og terrorfinansiering.

[23] *Kilde: Lov om finansiel virksomhed § 70 a, stk. 5, og lov om betalinger § 25 a, stk. 5.*

Adfærdsprincipper om forebyggelse af hvidvask og terrorfinansiering i pengeinstitutterne

✓ Vi påtager os loyalt og ansvarligt at bekæmpe økonomisk kriminalitet.

✓ Vi anerkender, at forebyggelse og bekæmpelse af hvidvask og terrorfinansiering ikke er et konkurrenceparameter, og at samarbejde og fælles løsninger derfor er ønskelige.

✓ Vi vil sikre, at ledelse og medarbejdere arbejder efter disse 6 adfærdsprincipper med tilhørende handleanvisninger:

1. Vi sætter altid etik før profit

a. Vi sætter bekæmpelse af hvidvask og terrorfinansiering over indtjening, og arbejder ud fra princippet om at hvad der ikke kan forklares, kan ikke forsvares.

b. Vi vil kun have kunder, hvor der er et klart og acceptabelt forretningsmæssigt formål - og står fast uanset hvem kunden er.

c. Vi holder fast på at kende vores kunder, deres forretning og måden hvorpå de bruger pengeinstituttet – også selv om det er kilde til modspil.

2. Vi følger loven og lovens ånd

a. Vi forklarer vores kunder baggrunden for reglerne og formålet med vores bestræbelser – følg og forklar.

b. Vi gør vores yderste for at udgøre en effektiv dørvogter i forhold til eksempelvis lande med forhøjet risiko, usædvanlige transaktioner, sindrige og uigennemsigtige selskabskonstruktioner, store kontantbeløb mv.

c. Vi gør vores yderste for at udgøre en effektiv dørvogter i forhold til sort arbejde og socialt bedrageri, og vi indretter vores systemer derefter.

3. Vi vil gerne kigges i kortene

a. Vi anerkender behovet for at øge gennemsigtigheden og har fokus på, at praksis kan tåle at komme i offentlighedens søgelys.

b. Vi vil i ledelsesberetningen redegøre for hovedindholdet af vores hvidvaskpolitik samt på vores hjemmeside offentliggøre oplysninger om vores konkrete arbejde med bekæmpelse af økonomisk kriminalitet.

c. Vi vil udarbejde standarder ud fra fælles formater, som kan gøres til genstand for uafhængig gennemgang og udformning af best practise.

4. Vi arbejder målrettet med vores virksomhedskultur

a. Vi sikrer, at varetagelse af ikke-økonomiske hensyn også inddrages, når det gælder rekruttering, forfremmelse, aflønning mv. herunder at opfyldelse af regulering indgår i relation til programmer med variabel aflønning.

b. Vi understøtter bekæmpelse af hvidvask og terrorfinansiering i vores daglige virksomhedsdrift, i vores kultur, i vores uddannelse og i vores kommunikation.

c. Vi lader os inspirere af andre professioner, der kan bidrage til at styrke kulturen og sikre, at bekæmpelsen af hvidvask og terrorbekæmpelse forankres i alle dele af organisationen.

5. Vi påtager os ledelsesansvar og sikrer, at alle medarbejdere tager ansvar i forhold til bekæmpelse af hvidvask og terrorfinansiering.

a. Vi sikrer tonen fra toppen, når det gælder formidling og synliggørelse af samfundsansvaret, da ledelserne er kulturbærere.

b. Vi sikrer, at alle led i organisationen krystalklart og konstant betoner vigtigheden af bekæmpelse af hvidvask og terrorfinansiering – uanset hvilke arbejdsopgaver den enkelte medarbejder har.

c. Vi sørger for relevant og tilstrækkelig uddannelse af medarbejderne, så de er klædt på til at varetage deres opgaver med bekæmpelse af hvidvask og terrorfinansiering.

6. Vi samarbejder konstruktivt med alle interessenter, herunder myndighederne.

a. Vi arbejder målrettet med underretningerne til Hvidvasksekretariatet, sådan at bekæmpelse af hvidvask og terrorfinansiering kan ske så effektivt som muligt.

b. Vi deltager konstruktivt i Hvidvaskforum+ og andre samarbejdsfora, hvor udviklingen i den underliggende kriminalitet drøftes og bekæmpelsen af hvidvask og terrorfinansiering forbedres.

c. Vi sikrer adgangen til en effektiv, anonym og beskyttet whistleblowing.

Det er selvsagt afgørende, at adfærdsprincipperne kommer til at leve i praksis. Hvidvask Task Forcen anbefaler derfor, at Finans Danmark understøtter implementeringen af principperne i sektoren.

HOVEDSPOR 5:

ØGET TRANSPARENS

Ud over de fire hovedspor har Hvidvask Task Forcen vurderet, at der er behov for et særligt fokus på at øge gennemsigtigheden i indsatsen i sektoren. Hvidvask Task Forcen har derfor valgt at lade øget transparens være et femte hovedspor i arbejdet.

Arbejdet med øget transparens har ført til en række anbefalinger til, hvordan det enkelte pengeinstitut og sektoren i fællesskab kan bidrage til, at offentligheden får større indsigt i indsatsen og udfordringerne på området. Hvidvask Task Forcens anbefalede initiativer skal løftes på institutniveau og ved en fælles indsats på sektorniveau via Finans Danmark.

Øget transparens i pengeinstituttet

Ledelsesberetning

Hvidvask Task Forcen anbefaler, at de enkelte pengeinstitutter forpligter sig til i deres ledelsesberetning at redegøre overordnet for, hvordan de arbejder med bekæmpelse af hvidvask og terrorfinansiering, herunder deres hvidvaskpolitik. Dette går videre end, hvad pengeinstitutterne i forvejen er forpligtet til efter bekendtgørelse om finansielle rapporter for kreditinstitutter og fondsmæglerselskaber m.fl.

Dedikeret hjemmeside

Hvidvask Task Forcen anbefaler desuden, at pengeinstitutterne på deres hjemmeside opretter en dedikeret

Pengeinstitutter, som har værdipapirer optaget til handel på et reguleret marked i et EU-/EØS-land, skal supplere ledelsesberetningen med en redegørelse for samfundsansvar. Redegørelsen skal indeholde oplysninger om institutternes arbejde med CSR, herunder deres politikker for samfundsansvar, hvordan deres politikker omsættes til handling, og hvad instituttet har opnået, og forventninger til fremtiden[24].
I forlængelse af reglerne om samfundsansvar anbefaler Hvidvask Task Forcen, at det enkelte pengeinstitut redegør overordnet for sit arbejde med at bekæmpe hvidvask og terrorfinansiering.

side, hvor de målrettet og tilgængeligt for den brede offentlighed kan oplyse, hvordan de arbejder med bekæmpelse af hvidvask og terrorfinansiering. Som det er nu, er der forskellige tilgange til, hvilke oplysninger de enkelte pengeinstitutter offentliggør. For at gøre det nemmere for offentligheden at få indsigt i pengeinstitutternes indsats anbefaler Hvidvask Task Forcen derfor, at pengeinstitutterne som minimum offentliggør følgende:

- Hvordan man arbejder efter Finans Danmarks adfærdsprincipper på hvidvaskområdet
- Hovedindholdet i pengeinstituttets hvidvaskpolitik
- Pengeinstituttets organisatoriske setup/forsvarslinjer på området
- Hvordan man overordnet monitorerer sine kunder
- Hvordan man uddanner sit personale på området
- Hvordan man håndterer whistleblowerbeskyttelsen.

Ovenstående initiativer vil bidrage til at give offentligheden en bedre indsigt i de enkelte pengeinstitutters tiltag på området og muliggøre en øget dialog mellem pengeinstituttet og dets interessenter. Oplysningerne skal tage højde for, at finansielle kriminelle ikke får indblik i for mange detaljer, så de kan svække forsvarslinjerne – men nok til at øge gennemsigtigheden for samfundet.

Øget transparens i sektoren via Finans Danmark

Årlig konference

Hvidvask Task Forcen anbefaler, at Finans Danmark årligt afholder en konference, der tematiserer nogle af de udfordringer og dilemmaer, der er i forhold til finansiel kriminalitet. Konferencen skal også være en mulighed for at indgå i dialog med interessenterne på området og med Finans Danmarks interne og eksterne samarbejdspartnere.

Årsrapport

Hvidvask Task Forcen anbefaler, at Finans Danmark årligt udarbejder en rapport, der går mere i detaljen i forhold til sektorens arbejde på området, herunder beskriver udviklingen i antal underretninger, brug af ressourcer, ansatte mv. i sektoren. Rapporten skal redegøre for, hvilke risikoområder sektoren ser, herunder inden for hvilke overordnede typer sager, man foretager underretninger til myndighederne. Endelig skal rapporten redegøre for, hvad der er på vej af nye sektortiltag, eventuelle standarder fra europæiske nabolande samt søge at komme med forslag til, hvordan man løbende kan gøre samarbejdet mellem myndighederne og pengeinstitutterne om bekæmpelse af hvidvask og terrorfinansiering mere effektivt. Rapporten skal deles med offentligheden og offentliggøres på den årlige konference.

Information til kunderne

Hvidvask Task Forcen anbefaler, at Finans Danmark øger informationsmaterialet til pengeinstitutternes kunder, der nærmere redegør for, hvad pengeinstitutterne gør på området, og hvilke krav der er i forhold til pengeinstitutterne, herunder i forhold til indhentelse af kundeoplysninger, og hvad de skal bruges til. Dette kan gøres ved informationskampagner, brug af sociale medier, pjecer og direkte brev/mail til pengeinstitutternes kunder.

Yderligere initiativer

Ud over de fem hovedspor og anbefalinger til disse har Hvidvask Task Forcen vurderet en række andre tiltag, som også kan styrke sektorens rolle i bekæmpelsen af hvidvask og terrorfinansiering. Hvidvask Task Forcen har haft særlig fokus på, konkrete initiativer, som kan sikre videndeling i samfundet, støtte forskning og styrke samarbejdet mellem sektoren og andre organisationer. På baggrund af dette er Hvidvask Task Forcen kommet frem til en række sektorinitiativer.

Støtte til whistleblowere

Hvidvask Task Forcen anbefaler, at de respektive bestyrelser - udover at sikre whistleblower-ordninger i alle banker – overvejer, hvordan whistleblowere kan understøttes, f.eks. ved at bistå med advokatbistand.

Samarbejde med SØIK

Hvidvask Task Forcen anbefaler, at sektoren i form af "Den Fælles Efterretningsenhed for Hvidvask og Terrorfinansiering" stiller medarbejderne til rådighed i

[24] *Kilde: Bekendtgørelse om finansielle rapporter for kreditinstitutter og fondsmæglerselskaber m.fl. § 135.*

et udvekslingsforløb med fokus på videndeling for en periode op til 3 måneder.

Evaluering af underretninger
Hvidvask Task Forcen anbefaler, at sektoren årligt evaluerer pengeinstitutternes underretninger i samarbejde med Hvidvasksekretariatet i SØIK med det formål at sikre, at de har den rette kvalitet i forhold til at undersøge mistænkelige forhold og at undgå, at sektoren sender unødvendige underretninger. En årlig evaluering af sektorens underretninger ville eventuelt kunne faciliteres af den nye efterretningsenhed Den Fælles Efterretningsenhed for Hvidvask og Terrorfinansiering.

Bankbokse
Hvidvask Task Forcen anbefaler, at sektoren indsamler et overblik over bankbokse. Baggrunden for at fokusere på bankbokse er, at de kan bruges til at opbevare kriminelt hittegods, narkotika, sorte penge eller andet. Sektoren ser derefter nærmere på, hvordan der kan etableres et betryggende niveau af foranstaltninger og processer, når pengeinstitutterne udbyder denne service. Task Forcen anbefaler i den forbindelse, at sektoren indgår i en dialog med Finanstilsynet om, hvad vejledningen til sektoren bør være i forhold til effektivt at overvåge bankbokse som led i kravene om kundekendskabsprocedurer og overvågning.

Forslag til fremtidige politiske initiativer

Hvidvask Task Forcen har i sit arbejde haft fokus på sektorens egne arbejdsgange, systemer, udfordringer og dermed løsninger målrettet disse. Sideløbende har det i Hvidvask Task Forcen været debatteret, hvilke initiativer man kunne iværksætte ikke kun i sektoren – men også politisk. Dette kapitel vil gennemgå en række forslag til fremtidige politiske initiativer.

Adgang til udbygget samarbejde mellem sektor og myndigheder
Det er vigtigt at benytte det allerede gode samarbejde mellem sektor og myndigheder til at udvikle nye veje til informations- og videndeling. Dermed vil myndighederne drage nytte af den ekspertise, som pengeinstitutterne udvikler i praktikken og i efterlevelsen af reglerne på hvidvaskområdet, ligesom pengeinstitutterne vil drage nytte af de informationer, der ligger hos en række offentlige myndigheder. I det omfang det er muligt og hensigtsmæssigt at dele flere oplysninger, kan indsatsen kvalificeres og fokus kan lægges der, hvor risiciene er størst.

Bankforum under Hvidvaskforum+
Det foreslås som et supplerende politisk initiativ, at der ud over Hvidvaskforum for myndighederne og Hvidvaskforum+ for myndigheder og brancheorganisationer - etableres et "Bankforum" med fokus på pengeinstitutter og med deltagelse fra Finans Danmark og repræsentanter fra medlemsvirksomheder. Et sådant forum vil give mulighed for en detaljeret og sektorspecifik videndeling fra begge sider, og samtidig vil det give rum for konkrete drøftelser.

Fælles Efterretningsenhed for Hvidvask og Terrorfinansiering (FEHT)
I forlængelse af ønsket om udbygget samarbejde, ønskes der et juridisk grundlag for, at der i Danmark kan etableres en Fælles Efterretningshed for Hvidvask og Terrorfinansiering. [Der henvises til rapportens gennem-

gang af hovedspor 2: Øget samarbejde med myndighederne). For at skabe et rum, hvor alle ressourcer, ekspertiser og indsamlede oplysninger kan få den mest effektive anvendelse med myndighederne som ansvarlig "for bordenden", er der behov for, at der politisk bliver arbejdet for en hjemmel til en dansk FEHT.

EU+

Hvidvask Task Forcen anbefaler, at Finans Danmark arbejder for, at det i den fremadrettede EU-regulering indsættes som en eksplicit mulighed, at medlemslandene kan etablere et organ lig FEHT, og at det muliggøres, at disse nationale enheder kan udveksle informationer med hinanden på tværs af grænserne.

Vejledning til hvidvaskloven

Finanstilsynets vejledning til hvidvaskloven er et vigtigt værktøj, som stiller nogle overordnede rammer og forventninger for den risikobaserede lovgivning. Der ønskes derfor et fortsat fokus på, at der til hvidvasklovgivningen følger vejledning, der er aktuel, og som særligt underbygger de regelområder, hvor anden lovgivning krydser med hvidvasklovgivningen samt yderligere konkret vejledning om konkrete situationer, hvor der er sparsom vejledning at finde i reglernes forarbejder. Dernæst er der fortsat behov for vejledning til virksomhederne om, hvilke tendenser og scenarier, der indikerer hvidvask og særligt indikerer terrorfinansiering. Terrorfinansiering er generelt sværere at opdage, ofte fordi der kan være tale om legitime midler, der benyttes til ulovlige formål. Virksomhederne har derfor stort behov for at kende til de aktuelle scenarier, der skal være fokus på i virksomhedernes overvågning af kunder og transaktioner.

BILAG

Bilag 1: Politiske tiltag på hvidvaskområdet

Området for forebyggelse og bekæmpelse af hvidvask og terrorfinansiering har været og er fortsat et særligt fokusområde politisk både i Danmark og i EU.

Danmark

De seneste år er der indgået en række politiske aftaler i Danmark, der overordnet skal styrke indsatsen mod finansiel kriminalitet, hvidvask og terrorfinansiering. Aftalerne supplerer de regler, der følger af EU's hvidvaskdirektiver, som hovedsagelig er implementeret i den danske hvidvasklov.

De politiske aftaler mod finansiel kriminalitet, hvidvask og terrorfinansiering:

- Aftale om styrket indsats mod hvidvask mv. i den finansielle sektor af 21. juni 2017: Se aftalen her. https://bit.ly/2KGVDrS
- Aftale om yderligere initiativer til styrkelse af indsatsen mod hvidvask og terrorfinansiering af 19. september 2018: Se aftalen her. https://bit.ly/2Xyqmws
- Aftale om styrkelse af indsatsen mod finansiel kriminalitet af 27. marts 2019: Se aftalen her. https://bit.ly/2O8CPnC

De politiske aftaler fra 2017-2019 har blandt andet medført indgåelse af en national hvidvaskstrategi, højere bødeniveauer, øgede ressourcer til Finanstilsynet og Hvidvasksekretariatet i SØIK, skærpede fit and proper krav, øget beskyttelse af whistleblowere mv. Endvidere blev der med den seneste aftale sat et mål om, at Danmark skal have en af EU's skrappeste lovgivninger på området.

De politiske initiativer er hovedsagelig blevet implementeret ved lovændringer i hvidvaskloven i 2018 og 2019[25]. Finans Danmark bakker aftalerne op, ligesom Finans Danmark har spillet konstruktivt ind i udformningen af alle aftaler.

Senest har regeringen besluttet at oprette et operativt myndighedsforum med deltagelse af SØIK, Hvidvasksekretariatet, PET, Rigspolitiet, Finanstilsynet, Erhvervsstyrelsen, Skattestyrelsen og Spillemyndigheden for at styrke det tværgående myndighedssamarbejde om bekæmpelse af hvidvask og terrorfinansiering.

Finans Danmark finder det afgørende, at der er en klar men risikobaseret regulering på området, som følger med udviklingen i samfundet og også de kriminelle miljøer og tendenser, som løbende ændrer sig i takt med, at det bliver vanskeligere at misbruge det finansielle system. Finans Danmark støtter initiativerne, hvoraf mange går hånd i hånd med sektorens egen forstærkede indsats. Det er således godt, at der afsættes flere ressourcer til Finanstilsynet og ikke mindst SØIK, så de har de fornødne ressourcer, og der er bedre muligheder for at følge op på pengeinstitutternes indsats.

Finans Danmark bidrager også ved blandt andet at deltage i Finanstilsynets arbejde med vejledningen til

hvidvaskloven og ved et intensiveret samarbejde med de relevante myndigheder på områder med fokus på en god og konstruktiv dialog og videndeling. Samarbejdet med myndighederne om de fremtidige tiltag er nærmere beskrevet nedenfor.

EU

De danske hvidvaskregler er overordnet en implementering af EU's hvidvaskdirektiver, foruden de særregler, der som nævnt er implementeret efter de politiske aftaler.

Det gældende EU-direktiv er det såkaldte 4. hvidvaskdirektiv fra 20. maj 2015, der blev suppleret af nogle ændringer og stramninger med 5. hvidvaskdirektiv fra 30. maj 2018. Disse ændringer og stramninger vil være endeligt implementeret i den danske hvidvasklov den 10. januar 2020.

Som en del af indsatsen mod hvidvask og terrorfinansiering har EU-Kommissionen den 12. september 2018 fremsat et forslag til styrkelse af Den Europæiske Banktilsynsmyndigheds (EBA) rolle på både nationalt og EU-plan. Med forslaget vil det europæiske tilsyn skulle samles hos EBA, og EBA vil få en styrket rolle i forhold til dels at udstede vejledninger til medlemslande dels i forhold til at kunne gribe ind i konkrete sager.

Finans Danmark støtter initiativet, da det kan være med til at understøtte de nationale myndigheders indsats og sikre et mere ensartet niveau på tværs af EU. Det daglige tilsyn bør dog ligge hos de nationale myndigheder.

I EU bliver det også overvejet, om den europæiske hvidvaskregulering fremover skal fastsættes i en forordning i stedet for i et direktiv. En forordning adskiller sig ved, at den gælder direkte i medlemslandene.

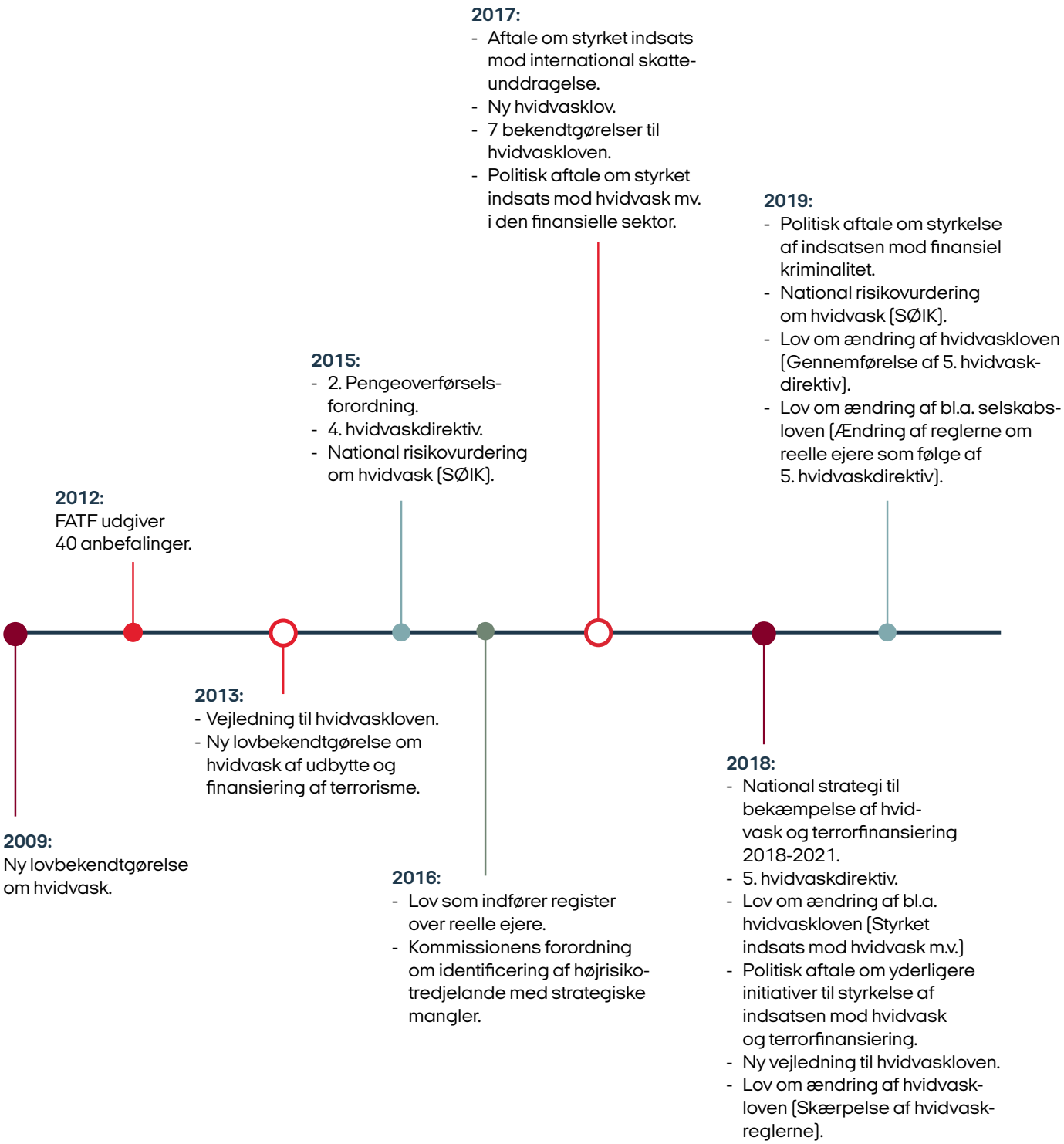
Både Rådet og Europa-Parlamentet har for nylig bedt Europa-Kommissionen om at evaluere området samt forholde sig til spørgsmålet om, hvorvidt hvidvaskreguleringen fremover skal fastsættes ved en forordning, hvilket Kommissionen hvilket synes at hælde til.

Kommissionen har på baggrund heraf den 24. juli 2019 offentliggjort en meddelelse og fire rapporter, der gør status på området i forhold til de mangler, man mener at have identificeret i blandt andet lovgivningen og tilsynet, samt kommer med en række anbefalinger til forbedringer.

Særligt relevant at fremhæve er Kommissionens konklusion, at pengeinstitutter og nationale tilsynsmyndigheder har truffet væsentlige foranstaltninger, men at der stadig skal gøres mere. Der er er behov for yderligere harmonisering. Endvidere fremhæves FIU'erne (Financial Intelligence Units) – Hvidvasksekretariatet i SØIK er Danmarks FIU. Her er Kommissionens vurdering, at der ikke er tilstrækkelig mulighed for samarbejde og udveksling af oplysninger mellem FIU'erne.

[25] *Kilde: Lov nr. 1535 af 18/12/2018, lov nr. 706 af 08/06/2018, lov nr. 533 af 07/05/2019.*

Bilag Tidslinje – hvidvaskområdet de sidste 10 år



ORDLISTE:

SØIK	Statsadvokaten for Særlig Økonomisk og International Kriminalitet
PET	Politiets Efterretningstjeneste
JMLIT	Joint Money Laundering Intelligence Taskforce
KYC	Know Your Customer (Kend din kunde)
CDD	Customer Due Diligence
ODD	Ongoing Due Diligence
AML/CTF	Anti-Money Laundering/Counter Terrorist Financing
PEP/RCA	Politisk Eksponerede Personer/Nærtstående og nære samarbejdspartnere (på engelsk: Relatives and Close Associates).
FEHT	Fælles Efterretningsenhed for Hvidvask og Terrorfinansiering
OPP	Offentligt og Privat Partnerskab
FATF	Financial Action Task Force
FE	Forsvarets Efterretningstjeneste
TAX3	The EU Special Committee on Financial Crime, Tax Evasion and Tax Avoidance (TAX3)
EBA	European Banking Authority
ICA	International Compliance Association

Grafisk design: Wundergeist.dk
Foto: Finans Danmark og Unsplash

Finans Danmark
Amaliegade 7
1256 København K

Telefon 3370 1000
www.finansdanmark.dk