FINANSTILSYNET

Projekt AML/TEK

FINANSTILSYNET

Indholdsfortegnelse

Sammenfatning

Den daværende regering og et bredt flertal i folketinget indgik den 27. marts 2019 en politisk aftale om styrkelse af indsatsen mod finansiel kriminalitet[1]. Det sjette initiativ i aftalen fastsætter, at Finanstilsynet skal understøtte den finansielle sektors arbejde med at opbygge en fælles infrastruktur, der kan styrke virksomhedernes processer for kundekendskab.

Kundekendskabsprocedurer (KYC) er et vigtigt element i bekæmpelsen af hvidvask og terrorfinansiering[2]. Ved at kende kunderne og formålet med kundeforholdet er virksomheder og personer, som er underlagt hvidvaskloven, bedre i stand til at vurdere, om kundernes aktiviteter er usædvanlige. Kundekendskabet opbygges løbende over et kundeforhold gennem:

1. indhentning og løbende ajourføring af relevante oplysninger (stamdata) om de aktuelle kundeforhold

2. løbende overvågning af aktiviteter og transaktioner (transaktionsovervågning) for de aktuelle kundeforhold.

De forpligtede enheder gennemfører den løbende overvågning med henblik på at vurdere, om der opstår afvigelser i transaktioner og aktiviteter i forhold til kendskabet til kunden, eksempelvis i det forventede forretningsomfang. Undringsværdige forhold (mistænkelig adfærd) skal undersøges, og hvis undersøgelsen underbygger en mistanke om hvidvask eller terrorfinansiering, skal Hvidvasksekretariatet underrettes.

Hvidvasksekretariatet er Danmarks finansielle efterretningsenhed, der har til opgave at modtage, analysere og videregive oplysninger om mulig hvidvask eller finansiering af terrorisme til de relevante myndigheder.

Virksomheder og personer underlagt hvidvaskloven udgør dermed spydspidsen i den forebyggende indsats mod hvidvask og terrorfinansiering, og kundekendskabet er afgørende for en effektiv indsats. KYC-procedurerne er derfor vigtige, men kan til tider også være besværlige for kunderne og de forpligtede enheder.

Processen er bl.a. besværlig for kunderne, fordi de typisk skal afgive og indlevere materiale med oplysninger, eksempelvis identifikationsoplysninger som kopi af pas. Kunderne, særligt kunder i langvarige kundeforhold, forstår ofte ikke, hvorfor eksempelvis pengeinstitutterne løbende skal have sådanne oplysninger, og føler det grænseoverskridende at skulle udlevere disse.

For de forpligtede enheder er processen besværlig af andre grunde, herunder:

1. Indhentning og særligt kontrol af stamdata for kunderne er i mange tilfælde en ressourcetung proces. Det skyldes bl.a. den risikobaserede tilgang til indholdet af kundekendskabsprocedurerne, der betyder, at det ikke er ligetil at opstille faste kriterier

[1] Med i aftalen var den daværende regering (Venstre, Liberal Alliance og Det Konservative Folkeparti), Socialdemokratiet, Dansk Folkeparti Radikale Venstre og Socialistisk Folkeparti.
[2] Know Your Customer.

for, hvornår den udførte KYC er tilstrækkelig. Desuden er disse procedurer ofte manuelle.

2. Mulighederne for effektivt og hurtigt at opnå et fyldestgørende kundekendskab, herunder en effektiv indretning af transaktionsovervågningen, kan være begrænset af manglende adgang til relevante datakilder i regi af offentlige myndigheder og begrænset vidensdeling på tværs af de forpligtede enheder og med myndighederne om indikatorer på mistænkelig adfærd.

3. Hvidvasklovens bestemmelser og tavshedspligt begrænser i vid udstrækning muligheden for, at virksomheder og personer underlagt hvidvaskloven indbyrdes kan dele oplysninger om kunder og deres mistænkelige adfærd. Dermed er muligheden for at underbygge kundekendskabet på baggrund af observationer gjort af andre begrænset.

Det er i myndighedernes interesse at understøtte effektive kundekendskabsprocedurer, da en eventuel efterfølgende efterforskning i sager om hvidvask eller terrorfinansiering i høj grad tager udgangspunkt i de oplysninger, de forpligtede enheder har om deres kunder og disses adfærd. Det understreger betydningen af, at det løbende overvejes, om samarbejdet kan forbedres, og om de forpligtede enheder har de rette værktøjer til at løfte deres opgave.

Finanstilsynet vurderer, at det er muligt at optimere infrastrukturen, så kundekendskabsprocedurerne kan udføres mere effektivt og på en måde, der understøtter kampen mod hvidvask og terrorfinansiering bedre og samtidig er mindre besværlig for kunderne og de forpligtede enheder.

Overfor dette står andre hensyn. Det gælder primært hensynet til beskyttelse af persondata og kundernes grundlæggende retssikkerhed. Myndighederne skal dermed foretage en afvejning mellem disse to hensyn, når det overvejes, om man skal gøre yderligere for at understøtte de underretningspligtige.

Finanstilsynet har på den baggrund analyseret en række forskellige tiltag, der anses som egnede til at adressere de angivne problemstillinger[3]. Fokus har bl.a. været på, i hvilket omfang den tilgængelige digitale infrastruktur i Danmark i dag kan udnyttes bedre. Derudover har Finanstilsynet analyseret muligheder for at udvide infrastrukturen. Fokus har i den forbindelse særligt været på de juridiske problemstillinger. Danmark bør, som et af de mest digitaliserede samfund i verden med en stærk historik omkring etablering af en fælles infrastruktur, kunne blive et foregangsland på dette område.

Det er på mange måder svært at kvantificere værdien ved et specifikt tiltag før det testes i praksis. Udgangspunktet for analysen er derfor følgende:

> *Et bedre kundekendskab og en øget indsigt i kriminel adfærd kan bidrage til, at mistænkelig adfærd kan opdages hurtigere og i et større omfang. Kundekendskabet kan forbedres gennem en mere effektiv brug af ressourcer og øget datadeling, og forbedringspotentialet vil stige i takt med, at troværdigheden og omfanget af data stiger. Øget*

[3] Denne analyse blev døbt Projekt AML/TEK.

indsigt i kriminel adfærd kræver bedre samarbejde mellem relevante myndigheder og sektoren.

Tabel 1 opsummerer de tiltag, der præsenteres i rapporten. Tiltagene fordeler sig i to kategorier: Bedre udnyttelse af den eksisterende infrastruktur og udvidelse af den eksisterende infrastruktur.

Tabel 1 – Opsummering af indstillinger

Tiltag	Indstilling	Værdi	Kompleksitet			Afsnit
			Juridisk	Teknisk	Tidshorisont	
Bedre udnyttelse af den eksisterende infrastruktur						
KYC-utilities	Understøtte sektorens arbejde med det formål at sikre en effektiv implementering.	Mellem	Mellem/Høj	Lav	Mellem	4
CVR	Arbejde for etableringen af mekanisme til verificering af virksomhedsdata i CVR.	Mellem	Lav	Lav	Mellem	5
MitID	I takt med at MitID-løsningen implementeres fastslå, om MitID kan anvendes bredere til kontrol af identiteter end NemID.	Mellem	Lav	Lav	Kort	6
Udvidelse af den eksisterende infrastruktur						
PEP-løsning	Etablering af løsning til screening af PEP'er og deres relationer i regi af en offentlig myndighed.	Mellem	Lav	Lav	Kort	7
Generaliserede scenarier	Etablering af sektorfælles samarbejde med fokus på at identificere generaliserede scenarier, der kan bruges i transaktionsovervågningen.	Høj	Lav	Mellem	Mellem	8
Øget adgang til myndighedernes data	Afdækning af mulighederne for, at give adgang til sammenstillede virksom-hedsdata eller vurderinger i regi af ERST. Desuden bør tilgængeligheden af anden offentlig data overvejes.	Mellem/Høj	Mellem	Mellem/Høj	Mellem/Lang	9
Deling af risikoflag	Beslutte om der skal arbejdes for at muliggøre delingen af risikoflag. Enten direkte mellem pengeinstitutter, hvilket kræver en ændring af tavshedsbestemmelserne i hvidvaskdirektivet, eller gennem en offentlig myndighed.	Høj	Høj	Høj	Lang	10

Kilde: Finanstilsynet.

Det videre arbejde er betinget af en fælles forståelse mellem relevante myndigheder og ikke mindst politisk opbakning til at undersøge de relevante tiltag nærmere. Her er netop afvejningen mellem værdien i relation til bekæmpelse af hvidvask og terrorfinansiering og kompleksiteten i tiltaget, særligt den juridiske kompleksitet, central for, om der skal arbejdes videre med tiltaget. Denne afvejning er på ingen måde objektiv, og andre interessenter kan have en anden vægtning end Finanstilsynet. Rapporten indeholder derfor ingen konklusioner, men præsenterer Finanstilsynets forslag til videre arbejde.

Bemærk, at en beslutning om at gå videre med ét tiltag ikke nødvendigvis udelukker, at man samtidig eller på et senere tidspunkt også vil kunne gå videre med andre tiltag. Omvendt kan det også i det videre arbejde vise sig, at et tiltag var forbundet med større problemer eller færre fordele end først antaget.

Fokus kan med fordel også være på de mulige synergier, der kan opstå, for at sikre, at der ikke arbejdes videre med forskellige tiltag med samme formål på tværs af de forpligtede enheder og myndighederne.

Bedre udnyttelse af den eksisterende infrastruktur

Det stigende fokus på at forbedre indsatsen mod hvidvask og terrorfinansiering har gjort, at virksomheder og personer underlagt hvidvaskloven, særligt pengeinstitutterne, over de seneste år har opskaleret deres ressourcer massivt. Finans Danmarks Hvidvask Task Force offentliggjorde den 27. november 2019 en rapport om finanssektorens indsats mod hvidvask og terrorfinansiering. Det fremgår bl.a. af rapporten, at antallet af ansatte i pengeinstitutter, der havde hvidvask og compliance som kerneopgave pr. november 2019, var 4.300, hvilket svarer til årlige lønudgifter på ca. 3,4 mia.

Rapporten indeholder en række anbefalinger, der bl.a. peger på behovet for i højere grad at udvikle fælles IT-løsninger, så ressourcerne kan allokeres og bruges bedre. Det fremhæves, at en forudsætning for, at sektoren kan benytte sådanne standardiserede løsninger, er, at der arbejdes for at etablere en form for minimumsstandard for indholdet af især kundekendskabsprocedurerne.

Kundekendskabsprocedurerne kan ikke standardiseres fuldstændigt, da de altid skal tilpasses den enkelte virksomheds særlige forhold. Hvidvaskloven foreskriver også en risikobaseret tilgang. Finanstilsynet ser dog også potentialet ved at arbejde for en harmonisering og effektivisering af tilgangen i det omfang, det er muligt. Samtidig kan arbejdet understøttes ved at sikre kvaliteten af offentlige løsninger og registre.

Finanstilsynet har inddraget disse overvejelser i arbejdet med rapporten, hvilket har ledt til tre konkrete forslag til et videre arbejde:

1. **Understøttelse af udviklingen af KYC-utilities:** Fokus bør være på at konkretisere udfordringer eller muligheder og klarlægge, i hvilket omfang det vurderes proportionelt at arbejde for de nødvendige infrastrukturelle og lovgivningsmæssige ændringer. Denne øvelse bør understøttes af faktiske observationer fra KYC-utilities, der kan indhentes i takt med, at de går på markedet.

2. **Kvalitetssikring af CVR:** Der igangsættes et arbejde med relevante aktører, herunder Erhvervsstyrelsen, Finans Danmark, FSR og advokatsamfundet, med fokus på at kortlægge, under hvilke vilkår der kan etableres en mekanisme i CVR, hvor advokater og godkendte revisorer kan verificere de registrerede virksomhedsoplysninger.

3. **Øget anvendelsesområde for MitID:** Finanstilsynet forventer, at MitID vil kunne bruges til kontrol af kunders identiteter ud over, hvad NemID kan bruges til i dag. Dette kan først fastslås endeligt, når MitID-loven træder i kraft, og MitID er udstedt bredt til

personer i Danmark. Den videre udvikling af MitID-løsningen bør derfor følges tæt med dette formål in mente.

Tiltag fokuseret på at udvide infrastrukturen

En generel udfordring i forhold til at sikre en effektiv bekæmpelse af hvidvask og terrorfinansiering er, at kundekendskabet til en vis grad er fragmenteret på tværs af de forpligtede enheder og myndighederne. Det betyder, at kundekendskabet som udgangspunkt skal bygges op på ny, hver gang et nyt kundeforhold indledes. Desuden har de forpligtede enheder ikke altid de rette forudsætninger for effektivt af afdække relevante risici i transaktionsovervågningen.

Disse overvejelser er også over de seneste år blevet udtrykt af en lang række europæiske myndigheder og internationale organisationer. The Financial Action Task Force (FATF[4]) udgav bl.a. en rapport i 2017, der understreger potentialet ved en bredere deling af information blandt aktører i den private sektor[5]. Kommissionens handlingsplan for en effektiv bekæmpelse af hvidvask og terrorfinansiering fremhæver også værdien i såkaldte offentligt-private partnerskaber (*Public-Private Partnerships, PPP)*[6]. Derudover har Finans Danmarks Hvidvask Task Force også fremhævet potentialet ved bedre data- og vidensdeling.

Finanstilsynet har identificeret fire tiltag, der har potentiale til at understøtte en mere effektiv indsats. Tiltagene er hver især forbundet med juridiske udfordringer af forskellig karakter, og en konkret vurdering af de juridiske konsekvenser afhænger af, hvilken form tiltagene må få i praksis.

Tre ud af fire forslag er udarbejdet med udgangspunkt i pengeinstitutter. Det skyldes, at behovene varierer afhængigt af branchen, og at potentialet vurderes størst for pengeinstitutter, som spiller en særlig rolle i kampen mod hvidvask og terrorfinansiering. Pengeinstitutterne har det bredeste kundesegment og udbyder det bredeste katalog af produkter. Der har samtidig i det seneste årti været en række eksempler på, at pengeinstitutterne er blevet misbrugt til hvidvask.

Tiltagene kan i forskellig grad også være relevante for andre virksomheder og personer underlagt hvidvaskloven. I det omfang det besluttes at arbejde videre med tiltagene, bør det derfor også overvejes, hvordan tiltagene kan bredes ud til andre forpligtede enheder.

Finanstilsynet indstiller på den baggrund følgende fire initiativer:

1. **Etablering af en PEP-løsning i offentligt regi:** Det besluttes, om der skal arbejdes videre med de to foreslåede løsningsmodeller, og i så fald hvilken, samt i hvilken

[4] The Financial Action Task Force on Money Laundering and Financing of Terrorism (FATF) er et mellemstatsligt samarbejde under OECD, der blev grundlagt i 1989 på initiativ af G7 for at udvikle politikker og anbefalinger til bekæmpelse af hvidvask og terrorfinansiering. FATF's anbefalinger danner grundlag for EU's hvidvaskdirektiver, der er implementeret i dansk ret, bl.a. i hvidvaskloven.
[5] Financial Action Task Force on Money Laundering (FATF), Guidance – Private Sector Information Sharing, November 2017.
[6] Europa-Kommissionen – Communication on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing, Maj 2020.

myndighed PEP-løsningen skal forankres. Begge modeller kræver ændringer af hvidvaskloven og PEP-bekendtgørelsen, som bør igangsættes, hvis det besluttes at arbejde videre hermed.

2. **Udvikling af generaliserede scenarier:** Det besluttes om samarbejdet mellem myndigheder og pengeinstitutter bør udbygges med det formål at udvikle typologier for relevante scenarier (generaliserede scenarier), der bør afdækkes i transaktionsovervågningen. Et sådant arbejde vil være oplagt at placere i regi af en FEHT, hvis eller når en sådan etableres.

3. **Øget adgang til myndighedernes data:** Det besluttes, om der skal igangsættes et arbejde fokuseret på muligheden for, at pengeinstitutter får adgang til sammenstillede virksomhedsdata eller vurderinger i regi af Erhvervsstyrelsen. Beslutningen bør suppleres med overvejelser om, hvorvidt et sådant arbejde også bør berøre muligheder for en bredere adgang til andre myndigheders data.

4. **Deling af risikoflag:** Det besluttes, om der skal igangsættes arbejde fokuseret på at muliggøre delingen af risikoflag mellem pengeinstitutter. Som led i beslutningen bør der tages stilling til, om der skal arbejdes for, at pengeinstitutterne indbyrdes skal kunne dele risikoflag, og hermed for en ændring af tavshedsbestemmelserne i hvidvaskdirektivet, eller om det videre arbejde skal fokuseres på, at delingen udelukkende sker gennem en offentlig myndighed.

Bemærk i den forbindelse, at en afgørende præmis for en effektiv implementering af tiltag fokuseret på data- og vidensdeling om kunder er, at det ikke leder til en øget derisking af kundeporteføljerne (opsigelse af kunder) hos virksomheder og personer underlagt hvidvaskloven. Det skyldes både de retssikkerhedsmæssige betænkeligheder i den forbindelse, og at man risikerer, at kriminelle aktører i stedet vil forsøge at operere på det sorte marked, hvormed de vil blive endnu sværere at opdage.

Rapportens struktur

Afsnit 1 og 2 introducerer henholdsvis kravene til kundekendskabsprocedurer under hvidvaskloven og de overordnede juridiske overvejelser, der bør ligge til grund for en vurdering af en yderligere adgang til deling af data om kunder. Afsnit 3 omhandler overvejelser af mulighederne for en bredere brug af avancerede teknologier. Herefter introduceres tiltagene fokuseret på bedre brug af den eksisterende infrastruktur i afsnit 4, 5 og 6, mens afsnit 7, 8, 9 og 10 omhandler forslag til at udvide infrastrukturen. Afsnit 11 opsummerer processen for et videre internationalt arbejde, særligt i EU-regi, som vil være nødvendigt eller hensigtsmæssigt at forfølge i forhold til at realisere en række af de konkrete initiativer og give dem fuld effekt.

Afsnittene 4-7 og 10 er stukturet sådan, at indledningen opsummerer analysen og de primære resultater. De resterende underafsnit for hvert afsnit udgør den faktiske analyse og de juridiske overvejelser. I afsnit 8 og 9 præsenteres analysen indledningsvis, hvorefter underafsnittene berører de juridiske overvejelser.

1. Kundekendskabsprocedurer under hvidvaskloven

Hvidvaskloven fastsætter krav om, at de forpligtede enheder skal identificere og vurdere den iboende risiko for, at de bliver brugt til hvidvask eller finansiering af terrorisme. Den iboende risiko følger af den valgte forretningsmodel (produktudbud, kundetyper, geografiske områder mv.), uden at der tages højde for de foranstaltninger, som er implementeret for at begrænse denne risiko.

Hvidvaskloven fastsætter også krav om, at virksomheder og personer omfattet af loven skal gennemføre kundekendskabsprocedurer ved etablering af en forretningsforbindelse med en kunde, når kundens relevante omstændigheder ændrer sig, og i øvrigt på passende tidspunkter. Kundekendskabsprocedurerne skal gennemføres for både fysiske og juridiske personer, og afhængigt af kundetypen omfatter det indhentelse af:

1. Kundens eller de reelle ejeres identitetsoplysninger og informationer, der kan afklare, om kunden er en politisk eksponeret person (PEP) eller en nærtstående til en PEP (PEP-screening)
2. Information om formålet med kundeforholdet
3. Oplysning om forretningsforbindelsens tilsigtede beskaffenhed eller kundens forventede brug af produktet. Det kan eksempelvis være den forventede type, størrelse, antal eller frekvens af transaktioner, som kunden forventer gennemført.

De forpligtede enheder skal som led i kundekendskabsprocedurerne også gennemføre en risikoklassifikation af kundeforholdet. Denne risikoklassifikation udgør et væsentligt led i procedurerne, da den betinger omfanget af disse med udgangspunkt i det specifikke kundeforhold. Risikoklassifikationen er bl.a. med til at sætte rammerne for frekvensen af den løbende vedligeholdelse af kundekendskabet samt omfanget og karakteren af den efterfølgende overvågning af kundeforholdet. Den kan i nogle tilfælde medføre, at virksomheden skal indhente yderligere oplysninger, før kundeforholdet initieres eller fortsættes. Risikoklassificeringen kan dermed medføre, at de forpligtede enheder skal gennemføre lempede eller skærpede kundekendskabsprocedurer for et givent kundeforhold.

Det vil og skal altid være de forpligtede enheders ansvar, at kundekendskabet er tilstrækkeligt.

Hvidvaskloven fastsætter også krav om, at de forpligtede enheder løbende overvåger sine kunder og undersøger baggrunden for og formålet med alle transaktioner, der er komplekse, usædvanligt store, foretages i et usædvanligt mønster i forhold til kendskabet til kunden eller ikke har et åbenbart økonomisk eller lovligt formål (transaktionsovervågningen). De observerede og undringsværdige forhold i transaktionsovervågningen er også kendt som risikoflag, der rejses på en transaktion foretaget af en kunde, hvis adfærd er mistænkelig.

Bliver en forpligtet enhed på baggrund af en undersøgelse af et risikoflag vidende om, får mistanke om eller rimelig grund til at formode, at en transaktion, midler eller en aktivitet har eller har haft tilknytning til hvidvask eller finansiering af terrorisme, skal den omgående underrette Hvidvasksekretariatet. Transaktionsovervågningen skal desuden hjælpe den forpligtede enhed til at lære kunden bedre at kende med henblik på den fremtidige overvågning.

2. Generelle juridiske overvejelser ved deling af data

Deling af data om kunder (virksomheder og personer) mellem virksomheder og personer underlagt hvidvasklovens krav vil, uanset hvilken model der konkret benyttes, skulle overholde det generelle krav om, at der er hjemmel til at behandle data. Samtidig vil der være et hensyn at tage til retssikkerheden for den eller de personer, oplysningerne vedrører. Retssikkerhed skal i den forbindelse navnlig forstås som personens mulighed for at vide, hvilke oplysninger der udveksles om denne, og forsikring om, at personen ikke mødes med sanktioner eller reaktioner på baggrund af oplysninger, som denne ikke har kunnet imødegå eller få kendskab til. Endelig skal mere omfattende modeller for deling af oplysninger uden samtykke overvejes i forhold til bl.a. retten til privatliv.

De juridiske overvejelser ved deling af data enten mellem de forpligtede enheder eller mellem myndigheder og de forpligtede enheder angår navnlig tre ting:

1) Indgrebets proportionalitet
2) Retsvirkningen overfor den, data angår
3) Hjemlen til at behandle data.

Indgrebets proportionalitet

Ordninger, der giver adgang til at udveksle oplysninger om en eller flere fysiske eller juridiske personer uden samtykke fra pågældende, vil efter omstændighederne kunne udgøre et indgreb i retten til privatliv, der følger af artikel 8 i Den Europæiske Menneskerettighedskonvention (EMRK).

Artikel 8 har et bredt anvendelsesområde, der løbende tilpasses den teknologiske udvikling. Bestemmelsen omfatter derfor også personoplysninger mv.[7] Myndigheder må derfor kun registrere og opbevare sådanne oplysninger ud fra saglige og tungtvejende grunde og skal behandle oplysningerne på en måde, som er retssikkerhedsmæssig forsvarlig, så de ikke uberettiget videregives. Tilsvarende krav gælder for private virksomheder, hvor staten har pligt til at sikre sine borgere mod privates indgreb i borgernes frihedsrettigheder, som eksempelvis indgreb i retten til privat- og familieliv.

Artikel 8(2) indebærer, at ethvert indgreb i privat- og familielivet skal have hjemmel og være nødvendigt i et demokratisk samfund (proportionalt) for at varetage vægtige hensyn til samfundets eller andres rettigheder.

Finanstilsynet vurderer umiddelbart, at udveksling af oplysninger om eksempelvis stamdata eller risikovurderinger af kunder, herunder risikoflag rejst som led i pengeinstitutternes transaktionsovervågning, eller lignende oplysninger vil kunne udgøre et indgreb i retten til privatliv efter artikel 8.

En eventuel ordning, der indebærer en sådan udveksling, vil derfor skulle have lovhjemmel og varetage vægtige samfundshensyn. Det følger af artikel 8, at det bl.a. kan være hensynet

[7] Se bl.a. *Leander* (1987, para. 48) og *Amann* (2000, para. 65 og 69).

til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, at forebygge uro eller forbrydelse, at beskytte sundheden eller sædeligheden eller at beskytte andres rettigheder og friheder.

Udveksling af oplysninger om risikoflag, risikovurdering o.l. vil skulle ske med henblik på mere effektivt at forebygge hvidvask og terrorfinansiering. Følgende fremgår af præambelbetragtning nr. 42 til EU's 4. hvidvaskdirektiv (uddrag):

> *"Bekæmpelse af hvidvask af penge og finansiering af terrorisme er anerkendt som en vigtig samfundsinteresse af alle medlemsstater."*

Finanstilsynet vurderer, at der på denne baggrund, og idet der er tale om et indgreb, der har til formål at forebygge forbrydelser, kan lægges til grund, at bekæmpelse af hvidvask og terrorfinansiering må anses som et vægtigt samfundsmæssigt hensyn i artikel 8(2)'s forstand. Et indgreb, der dermed vil kunne retfærdiggøre indgreb i retten til privat- og familieliv.

Lægges til grund, at indgrebet vil være legitimt efter artikel 8, vil det forsat skulle vurderes, om indgrebet er proportionalt i forhold til det hensyn, der forfølges. Proportionalitetsvurderingen består af tre elementer:

1. Egnethed: Indgrebet skal være egnet til at opnå sit formål.
2. Nødvendighed: Indgrebet skal være nødvendigt for at opnå formålet.
3. Forholdsmæssighed: Indgrebet skal afspejle et rimeligt forhold mellem mål og midler.

Det bør dermed for enhver model vurderes, om indgrebet er proportionalt. Navnlig vil en vurdering af nødvendigheden og forholdsmæssigheden afgøre, om de foreslåede modeller vil kunne udgøre et lovligt indgreb i artikel 8. Et indgreb vil kun være nødvendigt, hvis samme resultat ikke kan opnås med et mindre vidtgående indgreb.

Generelt indebærer overvejelserne, at jo mere vidtgående en model for deling af oplysninger er, jo mere vil proportionalitetsvurderingen fylde, og jo vigtigere bliver det at kunne forklare nødvendigheden og forholdsmæssigheden.

Retsvirkningen overfor den, som data angår
Ordninger, der indebærer, at der uden samtykke kan udveksles oplysninger om fysiske og juridiske personer, giver anledning til overvejelser om, hvad retsvirkningen af disse oplysninger vil være, herunder adgangen til at få kendskab til og eventuelt efterprøvet rigtigheden af oplysningerne.

Det bør dermed sikres, at en model med udveksling af oplysninger uden samtykke ikke indebærer, at kunder hos virksomheder og personer underlagt hvidvaskloven risikerer at blive udelukket fra at være kunder på baggrund af oplysninger, som de ikke har kendskab til, og som de ikke har mulighed for at få prøvet rigtigheden af (blacklisting). Det vil derfor være betænkeligt for den enkeltes retssikkerhed, hvis deling af oplysning om risikoflag, vurdering af risikoflag og risikovurderinger indebærer, at kunder mødes med reaktioner på baggrund af oplysninger om deres forretninger, som de hverken er bekendte med eller kan få indsigt i.

Der vil eksempelvis kunne være tilfælde, hvor en kunde nægtes at åbne en konto i et pengeinstitut på baggrund af oplysninger om kundens tidligere transaktioner, som det nye pengeinstitut har modtaget uden kundens viden. Disse betænkeligheder forstærkes i tilfælde, hvor der ikke alene er tale om objektive oplysninger, men også om vurderinger af disse oplysninger.

Samtidig bør det overvejes, hvilken adgang den, som dataene angår, har eller skal have til at påklage eventuelle registreringer eller risikovurderinger, som den pågældende mener er fejlagtige. Det vil altså være forbundet med retssikkerhedsmæssige betænkeligheder, hvis oplysninger om kunder tillægges retsvirkning overfor kunderne, uden at den enkelte kunde kan få kendskab til oplysningerne eller adgang til at få efterprøvet rigtigheden af dem. Det gælder navnlig, hvis de pågældende data deles i en videre kreds.

Hertil kommer, at alle forbrugere ifølge god skik-reglerne har ret til en basal indlånskonto. Det følger af § 11 i lov om betalingskonti, at pengeinstitutter skal tilbyde en forbruger en basal betalingskonto, medmindre åbning af en sådan konto vil føre til en overtrædelse af hvidvaskloven. Pengeinstitutterne kan desuden afvise at stille en basal betalingskonto til rådighed for en forbruger, hvis forbrugeren:

1. ikke kan påvise en reel interesse i en basal betalingskonto
2. har udøvet strafbare handlinger mod pengeinstituttet, eller
3. har optrådt til gene for pengeinstituttets øvrige kunder eller ansatte.

Retsvirkningerne af de udvekslede oplysninger vil dermed skulle sammenholdes med forbrugeres ret til en basal indlånskonto og en basal betalingskonto. Et pengeinstitut kan altså ikke afvise at oprette en basal indlåns- eller betalingskonto til en forbruger, hvis betingelserne i lov om betalingskonti i øvrigt er opfyldt.

Hjemlen til at behandle data
Deling af data om kunder rejser spørgsmål om behandling af kunders data, herunder navnlig de forpligtede enheders adgang til at behandle og udveksle oplysninger om private kunder uden samtykke fra den pågældende.

Overvejelserne i forhold til databeskyttelsesforordningen er kun relevante for oplysninger om fysiske personer, da forordningen ikke finder anvendelse for juridiske personer.

Det følger af forordningen, at enhver behandling af personoplysninger skal overholde kravene om lovlighed, rimelighed og gennemsigtighed. Hertil kommer, at indsamlede data som udgangspunkt kun må benyttes til det konkrete formål, de er indsamlet til (formålsbegrænsningen).

Det vil dermed altid kræve et lovligt grundlag for behandling (behandlingshjemmel) for forpligtede enheder eller offentlige myndigheder at behandle personoplysninger, eksempelvis som led i kundekendskabsprocedurer eller bekæmpelse af finansiel kriminalitet. De forpligtede enheder og de offentlige myndigheder skal altså sikre, at det rette regelgrundlag er til stede, inden de deler, indhenter eller på anden måde behandler personoplysninger.

Databeskyttelsesforordningen indeholder adgang til at behandle personoplysninger uden samtykke fra den, som oplysningerne angår. For at en forpligtet enhed kan behandle oplysninger uden samtykke, kræver det som udgangspunkt en klar behandlingshjemmel.

Behandling af personoplysninger på grundlag af reglerne i hvidvaskdirektiverne anses for at være i samfundets interesse, jf. hvidvaskdirektivets artikel 43, hvilket udgør en lovlig behandlingshjemmel efter persondataforordningen artikel 6, stk. 1, litra e, jf. stk. 3, litra a. Virksomheder og personer underlagt hvidvaskloven har dermed i dag hjemmel til at foretage databehandlinger omfattet af hvidvaskloven.

Det bør ved de enkelte mulige tiltag overvejes, om der er formålslighed mellem det, oplysningerne er indsamlet til, og den videre behandling.

Finanstilsynet vurderer, at det uanset model bør sikres, at der er en klar hjemmel til den ønskede behandling, uanset om det er udveksling mellem de forpligtede enheder eller udveksling mellem en forpligtet enhed og en offentlig myndighed.

3. Potentialet ved avanceret teknologi

Der er generelt stort internationalt fokus på anvendelsesområdet for mere avancerede teknologiske løsninger, såsom maskinlæring, i forhold til indsatsen mod hvidvask og terrorfinansiering. Det tyske formandskab for FATF har det også som et af fokusområderne for FATF's arbejde frem mod 2022 og har igangsat et projekt, som Finanstilsynet deltager i[8].

En af udfordringerne ved at bruge maskinlæring, bl.a. til transaktionsovervågning, er, at det i mange tilfælde kan være svært at forklare modellens beslutningsprocesser. Det kan have konsekvenser for, i hvilket omfang resultaterne af sådanne modeller kan lægges til grund for underretninger til Hvidvasksekretariatet og faktiske sanktioner mod kunden. Krav til forklarlighed, enten internt i en forpligtet enhed eller eksternt i forhold til Finanstilsynet eller Hvidvasksekretariatet, vil forventeligt variere, alt efter hvor indgribende resultatet af en model er. Eksempelvis kan en model med meget lav forklarlighed godt finde anvendelse i en proces om overvågning og screening, hvor personer eller selskaber udtages til manuel kontrol. Træffes en mere indgribende beslutning, eksempelvis om underretning af Hvidvasksekretariatet, vil der forventeligt være krav om, at modellens resultat kan forklares udførligt. Det betyder i praksis på nuværende tidspunkt, at de mest avancerede versioner af maskinlæring ikke bør bruges til autonomt at træffe beslutninger med betydning for personer. Grundlæggende er det vigtigste her, at det interne governance-setup er tilstrækkeligt robust til, at sådanne vurderinger finder sted og ikke tilsidesættes i farten.

Kvaliteten af en maskinlæringsmodel er desuden betinget af omfanget af tilgængeligt historisk data til træning af modellen. Det gælder særligt information om de faktiske resultater, som modellen skal bruges til at identificere. Det kan være problematisk i forhold til brugen af maskinlæring i transaktionsovervågning, da de forpligtede enheder som udgangspunkt kun har adgang til information om undringsværdige forhold, der identificeres under eksisterende processer, samt faktiske underretninger til Hvidvasksekretariatet. Muligheden for at få indsigt i resultaterne af myndighedernes undersøgelser af sager på baggrund af de specifikke underretninger er derimod begrænset. Bruges faktiske underretninger til Hvidvasksekretariatet eksempelvis som succeskriterie i træningen af en maskinlæringsmodel, vil kvaliteten af modellen derfor være betinget af kvaliteten af processerne for transaktionsovervågningen. Det medfører en risiko for, at ineffektive processer for transaktionsovervågning kan skabe bias i modellen, jf. afsnit 10.4.

Finanstilsynets undersøgelse af regeloverholdensen for transaktionsovervågningen i pengeinstitutterne viste også, at brugen af maskinlæringsteknikker ikke er så udbredt i dag[9]. Potentialet vurderes dog at være særligt stort i forhold til hhv. netværksanalyser, prioriteringen af rejste alarmer samt kalibreringen af eksisterende scenarier og udviklingen af nye. Maskinlæringsteknikker menes derfor i første omgang at kunne bruges som et effektiv redskab i transaktionsovervågningen og ikke som et alternativ til eksisterende processer, jf. afsnit 10.1.

Finanstilsynet har i regi af Finanstilsynets innovation hub fulgt udviklingen, hvad angår mulighederne for bedre datadeling ved brug af nye teknologier. Finanstilsynet deltog bl.a. på

[8] FATF, Objectives 2020-2022,
[9] Udgangspunktet for analysen af mulighederne for at dele risikoflag, jf. afsnit 10.

FCA's TechSprint i 2019, som havde fokus på, hvordan krypteringsteknikker *(private enhancing technologies)* kan facilitere øget data- og vidensdeling i sektoren[10]. Det ledte til en efterfølgende dialog med et af de deltagende selskaber, hvis løsning gør det muligt at sammenkøre forskellige virksomheders data og foretage transaktionsovervågningen på baggrund af disse. Hensigten er at tillade deling af al relevant transaktionsdata mellem eksempelvis alle pengeinstitutter, uden at hverken persondata eller betalingsdata udveksles. Krypteringen sikrer, at al lovgivning er overholdt, samtidigt med at transaktionsovervågningens kvalitet forbedres. En sådan løsning kan eksempelvis gøre det muligt, at følge pengene gennem et netværk af pengeinstitutter. Denne løsning indebærer dog også, at det skal være muligt at afkryptere data, eksempelvis som følge af en dommerkendelse, hvis de skal kunne ligge til grund for en eventuel efterforskning.

Et eksempel som dette fremhæver det store potentiale i brugen af mere avancerede teknologier. Udviklingen og anvendelsen af sådanne teknologier er dog fortsat på et tidligt stadie. Forpligtede enheder kan samtidigt også være forbeholdne overfor at gennemføre større investeringer i sådanne løsninger, bl.a. grundet usikkerheden omkring, hvordan man indretter en tilstrækkelig governance med sådanne løsninger, men sandsynligvis også grundet risikoen ved at være first-mover.

Finanstilsynet vurderer derfor, at tiltag, der bygger på avancerede teknologier, er forbundet med en længere tidshorisont, før de i praksis ville kunne bruges bredt. Myndighedernes fokus bør fortsat være på at følge udviklingen tæt, og særligt på at sikre den rette vejledning for brugen af nye teknologier. I 2019 udgav Finanstilsynet eksempelvis sit første bud på, hvad finansielle institutioner bør have på plads, inden de bruger superviseret maskinlæring[11]. Arbejde som dette skal særligt understøtte, at sektoren på en betryggende måde tager de nye teknologier til sig.

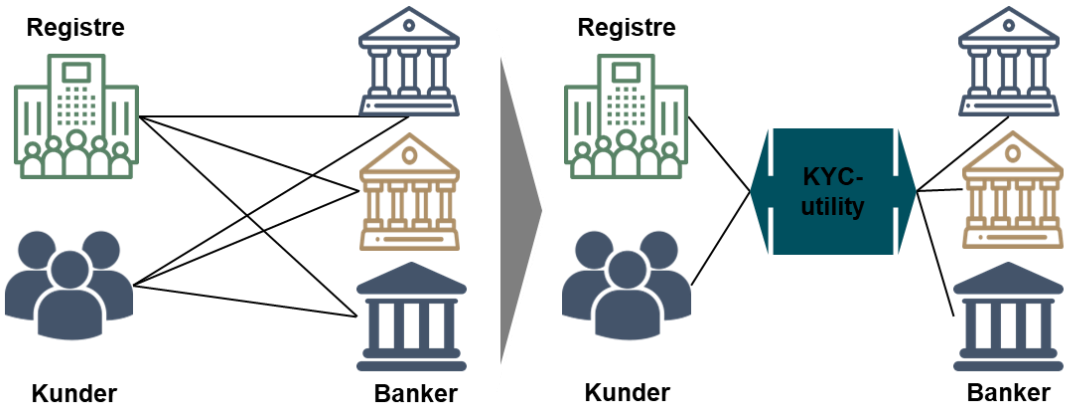
[10] En del af at dette arrangement var, at en række selskaber konkurrerede om at vise, hvordan sådanne teknologier bedst kan bruges til at bekæmpe hvidvask og terrorfinansiering.
[11] Finanstilsynets *God praksis ved brug af superviseret machine learning* - https://www.finanstilsynet.dk/Nyheder-og-Presse/Pressemeddelelser/2019/Machine_learning_10719

4. Deling af kundeoplysninger gennem KYC-utilities

Finanstilsynet indstiller, at Finanstilsynet fortsat følger og understøtter udviklingen af de beskrevne og andre lignende KYC-utilities. Fokus bør være på at konkretisere udfordringer eller muligheder og klarlægge, i hvilket omfang det vurderes proportionelt at arbejde for de nødvendige infrastrukturelle og lovgivningsmæssige ændringer. Denne øvelse bør understøttes af faktiske observationer fra KYC-utilities, der kan indhentes i takt med, at de går på markedet.

Omfanget af oplysninger (stamdata), der skal indhentes og kontrolleres som led i kundekendskabsprocedurerne, særligt i relation til virksomheder, kan være stort og kræver en del ressourcer. Disse ressourcer kunne potentielt bruges mere effektivt andetsteds, hvis indhentelsen og kontrollen af kundernes stamdata i højere grad kunne standardiseres og centraliseres, jf. figur 4.1. Derudover vil der være en stor fordel for kunderne, der kan nøjes med at afgive og opdatere informationer ét sted og derfra styre, hvem der har adgang til disse informationer.

Figur 4.1 – Øget centralisering gennem KYC-utilities



Kilde: Finanstilsynet.

Pengeinstitutterne er selv i gang med at udvikle forskellige tiltag til at løfte denne opgave og dermed både løfte niveauet for sektorens indsats mod hvidvask og terrorfinansiering og mindske omkostningerne ved denne. Det gøres ved så vidt muligt at sikre et fælles udgangspunkt og IT-infrastruktur for kundekendskabsprocedurerne (KYC-utilities). Finanstilsynet har løbende fulgt og delvist vejledt to af disse tiltag. Formålet med tiltagene er grundlæggende at forbedre udbyttet af de ressourcer, der bliver brugt på området:

- Et dansk initiativ, som søger at højne niveauet for kundekendskabsprocedurerne i danske pengeinstitutter for segmentet bestående af danske privatkunder med bopæl i Danmark.

- Et skandinavisk initiativ, der samler de mest nødvendige informationer til udførelse af pengeinstitutters kundekendskabsprocedurer for store erhvervskunder.

Andre virksomheder har desuden bevæget sig ind på området.

Finanstilsynet vurderer, at etableringen af KYC-utilities har betydelig værdi, da de både mindsker besværet for kunderne og mængden af ressourcer, som de forpligtede enheder skal allokere for at opnå et tilstrækkeligt kundekendskab. Arbejdet med udviklingen og implementeringen af sådanne tiltag bør derfor følges og understøttes af relevante myndigheder for at sikre en effektiv implementering. Det indebærer bl.a.:

- at det så vidt muligt tydeliggøres, hvilke kundeoplysninger de forpligtede enheder bør indhente, herunder hvornår en kundeoplysning er tilstrækkeligt kontrolleret. En præmis for et sådant arbejde er, at offentlige løsninger og registre er tilgængelige og troværdige, jf. afsnit 5, 6, 7 og 9

- yderligere harmonisering og så vidt muligt standardisering af hvidvaskreglerne, hvad angår kundekendskabsprocedurer, herunder definitionerne på de stamdata, de forpligtede enheder skal indhente og kontrollere, jf. afsnit 11. Det gælder eksempelvis definitionen på reelle ejere.

KYC-utilities kan potentielt også medvirke til at berige grundlaget for kundekendskabsprocedurerne. De vil have adgang til informationer omkring kunder og deres adfærd på tværs af en række forpligtede enheder, eksempelvis sammenfald i bopælsadresser for forskellige reelle ejere på tværs af virksomhedskunder i forskellige pengeinstitutter. Det videre arbejde bør derfor også afdække, om der kan være værdi i at gennemføre de nødvendige regulatoriske ændringer, der sikrer, at pengeinstitutterne mv. kan få adgang til sådanne oplysninger. Derudover kan det overvejes, om disse løsninger kan understøtte en højere kvalitet af offentlige registre, hvis der etableres effektive feedback-mekanismer.

Ingen af disse tiltag er dog endnu implementeret i praksis. En konkret stillingstagen til, i hvilket omfang KYC-utilities kan bidrage bredere end til det umiddelbare formål, bør derfor afvente faktiske observationer i takt med, at de går på markedet.

4.1. Finans Danmarks standard for kundekendskabsprocedurer

Finans Danmarks Hvidvask Task Force offentliggjorde som led i deres rapport en vision om at implementere en fælles centraliseret KYC-utility. Denne vision bygger på en målsætning om, at kundekendskabsprocedurerne i den nære fremtid kan udføres på en anden og mere effektiv måde end i dag.

Standarden for kundekendskabsprocedurer (standarden) er en del af første trin ud af tre i denne vision[12]. Den er resultatet af en sektorfælles aftale, udarbejdet af en arbejdsgruppe med repræsentanter fra en række pengeinstitutter, Hvidvask Task Forcen og andre bidragsydere. Finanstilsynet gav sine bemærkninger til standarden den 19. december 2019.

Formålet med standarden er at sikre et fælles grundlag for danske pengeinstitutters kundekendskabsprocedurer og dermed hæve niveauet i sektoren. Standarden har tre konkrete mål:

- At sikre et solidt fundament for et stærkt sektorsamarbejde, herunder et fælles sprog og definitioner

[12] For nærmere indsigt heri henvises til rapporten udarbejdet af Finans Danmarks Task Force.

- At hjælpe institutterne til at øge kvaliteten af deres dokumentation omkring kundekendskabsprocedurer

- At understøtte den langsigtede ambition om at kunne dele oplysninger på tværs af sektoren for hermed bedre at kunne forhindre eller bekæmpe hvidvask og/eller finansiering af terrorisme.

Standarden vil ikke kunne erstatte den risikobaserede tilgang til kundekendskabsprocedurerne i hver enkelte pengeinstitut. Udgangspunktet var derfor også at blive enige om den letteste delmængde – en minimumsstandard for danske privatkunder bosiddende i Danmark.

Det er i den forbindelse værd at bemærke, at standarden basalt set består af en række tjekspørgsmål, som pengeinstitutterne bør overveje, hver gang de indleder eller opdaterer et kundeforhold. Der findes dermed ikke en decideret skabelon, som institutterne kan følge slavisk i deres processer. Derudover er der ingen klar vejledning til, hvordan hvert trin, eksempelvis "indsamling af kundeoplysninger", skal udføres. Derimod fremgår der informationskilder, som sektoren er blevet enige om kan bruges.

Finanstilsynet vurderer, at standarden er væsentlig, særligt visionen om med tiden at etablere en KYC-utility. Værdien af et sådant initiativ er dog i høj grad betinget af, at der så vidt muligt kan fastsættes klare rammer for indholdet af kundekendskabsprocedurerne.

Tydeliggørelse af indholdet af kundekendskabsprocedurerne
En måde at understøtte sektoren i dette arbejde er at tydeliggøre, hvilke oplysninger de forpligtede enheder kan indhente i forbindelse med kundekendskabsprocedurer, og hvornår oplysningerne er tilstrækkeligt kontrolleret. Det kræver bl.a., at myndighederne og sektoren løbende er i dialog om, hvilke offentlige registre og løsninger de forpligtede enheder kan bruge, og særligt i hvilket omfang kvaliteten af disse er tilstrækkelige i forhold til hvidvasklovens krav. Finanstilsynet beskriver og anbefaler i denne rapport bl.a. en række tiltag, der kan hjælpe sektoren til at blive mere effektiv, jf. afsnit 5, 6, 7 og 9.

Finanstilsynet skal i en sådan vejledning afveje ønsket om at understøtte sektoren med hensynet til fortsat at kunne oppebære et effektivt tilsyn med de forpligtede enheder. Det er en klassisk tilsynsmæssig afvejning: Jo mere vejledning tilsynsmyndigheden giver, jo sværere er det efterfølgende at føre tilsyn.

Det er under ingen omstændigheder muligt at designe en *one-size-fits-all*-løsning for kundekendskabsprocedurerne. Risikoklassificeringen af et givent kundeforhold skal altid betinge omfanget af kundekendskabsprocedurerne. Det betyder bl.a., at nogle kontrolkilder kun vil kunne stå alene for kunder med en given risikoklassificering, mens der for andre kunder vil skulle gøres mere.

Udfordringer som disse understreger også værdien i at afdække mulighederne for en yderligere harmonisering af kravene i hvidvaskdirektivet, jf. afsnit 11.

4.2. KYC-utility i regi af Invidem

Invidem er blevet til på initiativ af seks store nordiske pengeinstitutter[13]. Formålet er at etablere en KYC-utility, der gør det mere effektivt at gennemføre kundekendskabsprocedurer på store erhvervskunder i Norden[14,15]. Løsningen vil grundlæggende gøre det muligt for alle pengeinstitutter at hente nødvendige oplysninger om deres virksomhedskunder fra ét centralt sted, mens det for virksomhedskunderne betyder, at de kun skal ajourføre oplysninger ét sted. Løsningen afspejler et ønske om besparelse hos både pengeinstitutterne og de erhvervsdrivende. Der er bl.a. eksempler på større virksomheder, der har et tocifret antal medarbejdere ansat til at ajourføre denne type data hos deres finansielle modparter. Invidem er derudover et par trin længere fremme end Finans Danmark, og forventningen er, at deres KYC-utility bliver implementeret bredt i løbet af 2021.

En minimumsversion skal etableres for så muligvis at blive udbygget efterfølgende på samme måde som for det danske projekt. Samtidig gælder det også her, at det enkelte pengeinstitut ikke kan være sikker på, at al nødvendig data kan hentes. Informationer fra Invidem skal dermed suppleres med information indhentet af det enkelte institut, i det omfang det er nødvendigt.

Potentialet ved en feedback-mekanisme

Når et pengeinstitut skal etablere et nyt kundeforhold, vil pengeinstituttet skulle indhente og verificere en række stamdata fra kunden. Løsningen har til formål at indsamle, opbevare og løbende verificere disse data fra kunden på vegne af pengeinstituttet. Validiteten af data kontrolleres gennem en række betroede tredjeparter, såsom CVR i Danmark og tilsvarende i andre lande. Det betyder bl.a., at Invidem vil kunne opdage uoverensstemmelser mellem de data, som kunden har oplyst, og data indhentet fra forskellige registre. Disse uoverensstemmelser kan skyldes forskellige forhold, eksempelvis at oplysninger om kunden i nogle tilfælde ikke er korrekt gengivet i offentlige registre.

Alle, herunder pengeinstitutterne, har interesse i at data i offentlige registre er så retvisende som muligt, jf. afsnit 5. Derfor kunne der med fordel ses nærmere på værdien i at etablere en effektiv form for feedback-mekanisme, hvormed data i offentlige registre kunne berigtiges på baggrund af observationer gjort af sådanne KYC-utilies. Det er Finanstilsynets forståelse, at dialogen omkring berigtigelser i dag foregår via mail, hvilket kan føre til uhensigtsmæssigt lange behandlingstider og manuelle processer.

Harmonisering af indhold af stamdata på tværs af landegrænser

Invidems løsning skal til at starte med være tilgængelig på tværs af de nordiske lande. Det indebærer, at indholdet af relevante stamdata for pengeinstitutterne så vidt muligt skal standardiseres på tværs af landene. Dette kan dog være vanskeligt på nogle områder, herunder i relation til definitionen af reelle ejere og kortlægningen af koncernstrukturer. Hvidvaskdirektivet opstiller eksempelvis ikke en entydig definition på reelle ejere. Det kan derfor være forskelligt, hvordan reelle ejere defineres på tværs af lande. Det kan på samme måde være forskelligt, hvordan forskellige lande definerer en modervirksomhed. Sådanne forskelle kan have konsekvenser for kvaliteten af løsningerne, herunder mulighederne for en yderligere integration og standardisering af kundekendskabsprocedurer på tværs af Norden og EU.

[13] Danske Bank, DNB, Handelsbanken, Nordea, SEB og Swedbank.
[14] Projektet gik oprindeligt under navnet KYC-Nordic.
[15] På sigt er målsætningen også, at løsningen kan udbredes til mindre virksomheder.

Yderligere datadeling mellem pengeinstitutter gennem KYC-utilities

Forretningsmodellen for KYC-utilities som Invidem indebærer, at KYC-utilities vil ligge inde med en stor mængde oplysninger om forskellige virksomheder og deres kundeforhold hos pengeinstitutter. Der vil derfor sandsynligvis også opstå situationer, hvor det sammenstillede data giver dem et overblik over virksomhederne, relationerne mellem disse og relationerne til pengeinstitutterne. Det kan give KYC-utilities viden, som kan medvirke til at identificere mistænkelige kunder. Det kunne eksempelvis være viden om simultan initiering af onboarding i flere pengeinstitutter eller personsammenfald i kundeforhold på tværs af pengeinstitutter, som det enkelte pengeinstitut ikke ville kunne identificere på egen hånd.

En bredere mulighed for at dele denne form for indsigt vil kunne bidrage til et forbedret værn og en mere effektiv indsats mod hvidvask og terrorfinansiering på tværs af pengeinstitutterne. Det kunne eksempelvis være i form af indsigt i sammenfald i ejerkredsen i flere selskaber og indsigt i situationer, hvor adskillige selskaber med forbindelse til forskellige pengeinstitutter deler adresse.

4.3. Juridiske overvejelser

Anvendelse af stamdata via KYC-utilities

Arbejdet med at etablere de ovenfornævnte KYC-utilities indebærer, at der vil blive oprettet en form for databank, der indeholder faktuelle oplysninger om kunder på tværs af pengeinstitutter. Der er dermed tale om verificerede stamdata, der opbevares et centralt sted. Det betyder, at kunder kan nøjes med at oplyse og have såkaldte stamdata opbevaret ét centralt sted. Kunder vil vide, at alt relevant data fremgår her, og pengeinstitutterne kan fremsøge alt relevant data samme sted. Forudsætningen for, at pengeinstituttet kan tilgå de opsamlede data om en kunde, er som minimum, at pengeinstituttet har samtykke fra kunden.

Initiativet er sammenfaldende med de tanker, man i EU-regi har gjort sig i forbindelse med hvidvaskdirektivets tilblivelse. Følgende fremgår blandt andet i betragtning nr. 35 til EU's hvidvaskdirektiv (uddrag):

> *"For at undgå, at gentagne kundekendskabsprocedurer fører til forsinkelser og ineffektivitet, bør det med forbehold af passende sikkerhedsforanstaltninger være tilladt for forpligtede enheder at modtage nye kunder, som er identificeret andetsteds. Benytter en forpligtet enhed sig af tredjemand, bør det endelige ansvar for gennemførelsen af kundekendskabsprocedurerne påhvile den forpligtede enhed, som kunden modtages i."*

Overvejelser om harmonisering

Ovenstående eksempel peger på, at der så vidt muligt bør ske en harmonisering på tværs af landegrænser i forhold til de indsamlede data for at skabe den bedste løsning. Specifikt har der vist sig forskelle i tilgangen til identifikation af reelle ejere, og der er også forskelle på, hvordan landene eksempelvis definerer en modervirksomhed.

Kravene til, hvilke oplysninger der skal indsamles i forbindelse med pengeinstitutternes kundekendskabsprocedurer, stammer fra EU-direktivet, som finder anvendelse i alle EU's medlemslande. Som eksempel kan nævnes, at udtrykket reelle ejere er defineret i AMLD4, art.

3, nr. 6. Definitionen stammer fra FATF's anbefalinger[16]. Der vil derfor også være en vis lighed i definitionen udenfor EU's grænser. Det er dog muligt for de enkelte lande at fastsætte skærpede regler.

For at sikre den mest effektive procedure på tværs af landegrænser kan det være nødvendigt at sikre en øget harmonisering af standarderne for indsamling af oplysninger, jf. afsnit 11. Alternativt vil de opbevarede stamdata være udtryk for en form for minimumspakke, og nogle landes institutter skal udover disse data selv indhente yderligere oplysninger for at leve op til hjemlandets lovgivning.

Deling af sammenstillede data i regi af KYC-utilities

Den afledte effekt af central indsamling af oplysninger om kunder på tværs af virksomheder og personer underlagt hvidvaskloven til brug for deres kundekendskabsprocedurer er, at en central aktør får adgang til en lang række data, som vil kunne sammenstilles på tværs.

Oplysningerne kan eksempelvis omhandle samtidig initiering af kundeforhold i flere institutter eller oplysninger om fysiske personers tilknytning til flere forskellige virksomheder. Sådanne oplysninger kan bl.a. være relevante at tage højde for i risikoklassifikationen af kunderne.

Finanstilsynet vurderer, at en sådan deling af sammenstillede data med pengeinstitutterne vil indebære de samme juridiske overvejelser som deling af sammenstillet data i regi af Erhvervsstyrelsens grafdatabase, jf. afsnit 9.1.

[16] Anbefaling nr. 24, samt tilhørende fortolkende note

5. CVR som kilde til kontrol af virksomhedsoplysninger

Finanstilsynet indstiller, at der igangsættes et arbejde med relevante aktører, herunder Erhvervsstyrelsen, Finans Danmark, FSR og advokatsamfundet, med fokus på at kortlægge, under hvilke vilkår der kan etableres en mekanisme i CVR, hvor advokater og godkendte revisorer kan verificere de registrerede virksomhedsoplysninger.

Hvidvaskloven stiller krav om, at de forpligtede enheder skal indhente og kontrollere identitetsoplysninger på deres virksomhedskunder og samtidig gennemføre rimelige foranstaltninger for at indhente og kontrollere identiteten på disse kunders reelle ejere, herunder indirekte ejere i tilfælde af, at den reelle ejer er en virksomhed.

For danske virksomhedskunder er det nærliggende at bruge det centrale danske virksomhedsregister (CVR) i regi af Erhvervsstyrelsen som led i overholdelsen af denne forpligtigelse. Registret indeholder alle relevante stamdata om danske virksomheder, herunder navn, adresse, CVR-nummer, direktions- og bestyrelsesmedlemmer, juridiske og reelle ejere og deres adresser mv.

Troværdigheden af data i CVR kan i nogle tilfælde være begrænset. Det skyldes, at virksomhederne selv giver oplysningerne, som ikke – eller kun i begrænset omfang – undergår en uafhængig manuel kontrol af Erhvervsstyrelsen. Det hænger sammen med et politisk ønske om, at det skal være lettere at være iværksætter, og at de tilgængelige ressourcer i Erhvervsstyrelsen begrænser muligheden for at håndtere alle kontroller manuelt.

Registreringsprocessen for virksomheder er derfor blevet automatiseret. Det indebærer, at en virksomhed selv indtaster de nødvendige oplysninger, når den oprettes eller ajourføres, og at Erhvervsstyrelsen kun udvælger et udsnit af disse registreringer til manuel kontrol ud fra en automatiseret risikovurdering. Virksomheder kan på den måde sløre de reelle ejerforhold eller andre oplysninger, uden at det nødvendigvis bliver opdaget. Finanstilsynet har derfor hidtil fastholdt, at de forpligtede enheder kun kan bruge CVR som eneste kilde til at kontrollere virksomhedsoplysninger for kunder underlagt lempede kundekendskabsprocedurer.

Finanstilsynet vurderer dog samtidig, at et bredere anvendelsesområde for CVR i forbindelse med kundekendskabsprocedurer gennem en yderligere digitalisering vil kunne mindske omkostningsfulde manuelle processer hos virksomheder og personer omfattet af hvidvaskloven. Det kan eksempelvis ske ved at fjerne behovet for at indhente yderligere dokumentation fra kunder i de tilfælde, hvor det i dag vurderes, at CVR ikke alene udgør en tilstrækkelig kilde til kontrol.

Finanstilsynet har derfor været i dialog med Erhvervsstyrelsen om troværdigheden af data i CVR. Det har givet en bredere forståelse af det forholdsvist sofistikerede system, der løbende udvikles for at kontrollere validiteten af data. Med det sagt, så bekræftede Erhvervsstyrelsen, at det fortsat ikke i alle tilfælde er sikkert, at de indsendte oplysninger i forbindelse med virksomhedsregistreringer og ændringer er retvisende. Samtidig kan opdateringer af data for virksomheder registeret i CVR være forsinket og potentielt også udestå, da virksomhederne også selv bærer ansvaret for at indberette ændringer, hvilket ikke nødvendigvis sker umiddelbart efter, at ændringerne er indtruffet.

Finanstilsynet har sideløbende været i dialog med Invidem, der udvikler et KYC-utility for en række nordiske pengeinstitutter med fokus på større erhvervskunder, jf. afsnit 4.2. Invidems løsning er derfor afhængig af tilgængeligheden af troværdige virksomhedsregistre og gør brug af sådanne registre i en lang række lande. Invidem bemærkede, at CVR ligger helt i top, hvad angår troværdigheden af data, til trods for at virksomheden fortsat observerer fejlregistreringer[17].

Tillades det, at CVR kan stå alene som kilde til kontrol af virksomhedsoplysninger, vil det begrænse Finanstilsynets og andre myndigheders muligheder for at sanktionere og reagere overfor de forpligtede enheder, hvad angår deres kundekendskabsprocedurer. Det kunne eksempelvis være i tilfælde, hvor data fra CVR ikke er retvisende, men fortsat bruges til kundekendskabsprocedurer for virksomhedskunder med fare for, at mistænkelige kunder overses. Eksempler på sådanne tilfælde er:

1. virksomheder, hvor den offentlig kendte ejer- og kontrolstruktur ikke er retvisende, eksempelvis stråmandsvirksomheder

2. relevante virksomhedsændringer, der bl.a. kan have konsekvenser for risikovurderingen af kunden, som ikke fremgår af CVR.

Finanstilsynet vurderer derfor, at CVR, som det er i dag, i udgangspunktet ikke kan stå alene som kilde til kontrol af virksomhedsoplysninger, uden at det kan have konsekvenser for effekten af indsatsen mod hvidvask og terrorfinansiering. En mulighed for at kunne bruge CVR bredere ville være, at advokater og godkendte revisorer fik adgang til at verificere virksomhedsoplysninger i CVR. Det forudsætter, at:

1. der i regi af Erhvervsstyrelsen implementeres en funktionalitet, hvormed advokater og godkendte revisorer kan verificere de registrerede oplysninger

2. der tages stilling til, i hvor lang tid en verificering er gyldig, idet kundekendskabsprocedurerne kun bør godtage gyldige verificeringer

3. advokat og godkendte revisorer i praksis er villige til at påtage sig ansvaret og at virksomheder, der gennemgår kundekendskabsprocedurer, vil påtage sig omkostningen i den forbindelse.

5.1. Hvidvasklovens krav

Det fremgår af § 11, stk. 1., litra b), i hvidvaskloven, at de forpligtede enheder skal indhente identitetsoplysninger på virksomhedskunder (juridiske personer), og af § 11, stk. 2, at disse oplysninger skal kontrolleres på baggrund af uafhængig og pålidelig kilde.

Finanstilsynets vejledning til hvidvaskloven[18] præciserer, at omfanget af disse kontroller beror på en risikovurdering. Det vil derfor i nogle tilfælde være nok med et opslag i CVR for

[17] Formålet med KYC-utilities er at verificere kundeinformation indhentet som led i de finansielle virksomheders kundekendskabsprocedurer og løbende ajourføre disse oplysninger. Hertil bruges en række kilder som kontrol, hvorfor KYC-utilities i nogle tilfælde vil blive bevidste om forskelle mellem oplysninger i CVR og de faktiske forhold i virksomhederne.
[18] https://www.finanstilsynet.dk/-/media/Tilsyn/hvidvask/seminar/Hvidvaskvejledning_November_2020.pdf

danske virksomhedskunder. I andre tilfælde vil det kræve noget mere, eksempelvis indhentelse af oplysninger fra Skatteforvaltningen eller en kopi af vedtægter og stiftelsesdokumenter.

Derudover fremgår det af hvidvasklovens § 11, stk. 3, at de forpligtede enheder skal indhente identitetsoplysninger på den eller de reelle ejere af en given virksomhed og gennemføre rimelige foranstaltninger for at kontrollere den eller de reelle ejeres identitet, så de med sikkerhed ved, hvem de reelle ejere er. Er en eller flere reelle ejere en juridisk person, skal de forpligtede enheder gennemføre rimelige foranstaltninger for at klarlægge den samlede ejer- og kontrolstruktur.

Der er tale om en konkret risikoklassificering i forhold til, hvor indgående undersøgelser de forpligtede enheder skal iværksætte for at klarlægge den enkelte kundes ejer- eller kontrolstruktur. I tilfælde med begrænset risiko kan det være tilstrækkeligt med et organisationsdiagram, der viser ejerandele eller oplysninger indhentet via CVR, mens det i andre tilfælde kan være påkrævet at indhente dokumentation for ejerandele i form af vedtægter eller lignende.

5.2. Kendte problematikker hvad angår virksomhedskunder

Der vil i mange tilfælde være tale om såkaldte stråmandsselskaber, når virksomhedskunder opretter konti med kriminelle formål. Et stråmandsselskab er en virksomhed, hvor den indsatte direktion, reelle ejere o.lign. som regel er faktiske personer, der ikke har en kriminel historik, men heller ikke i praksis har noget med virksomheden at gøre. De vil i stedet, for at kunne agere på selskabernes vegne, have videregivet de nødvendige identitetsoplysninger til kriminelle aktører, enten tilsigtet eller utilsigtet, jf. afsnit 6.5. Den primære udfordring ved at lade CVR stå alene som kilde til verificering denne type virksomhedsoplysninger er derfor, at der ikke er sikkerhed for, at de registrerede identiteter i praksis også driver og ejer virksomheden.

Derudover er der en risiko for, at selv virksomheder, der ønsker at overholde lovens krav, ikke altid får opdateret de relevante informationer, når der sker ændringer i eksempelvis ejer- og kontrolstrukturen. Sådanne ændringer kan i nogle tilfælde medføre, at risikoklassificeringen af kundeforholdet bør ændres, eksempelvis ved overdragelser af ejerandele fra en dansk virksomhed til en udenlandsk virksomhed i skattely eller lignende.

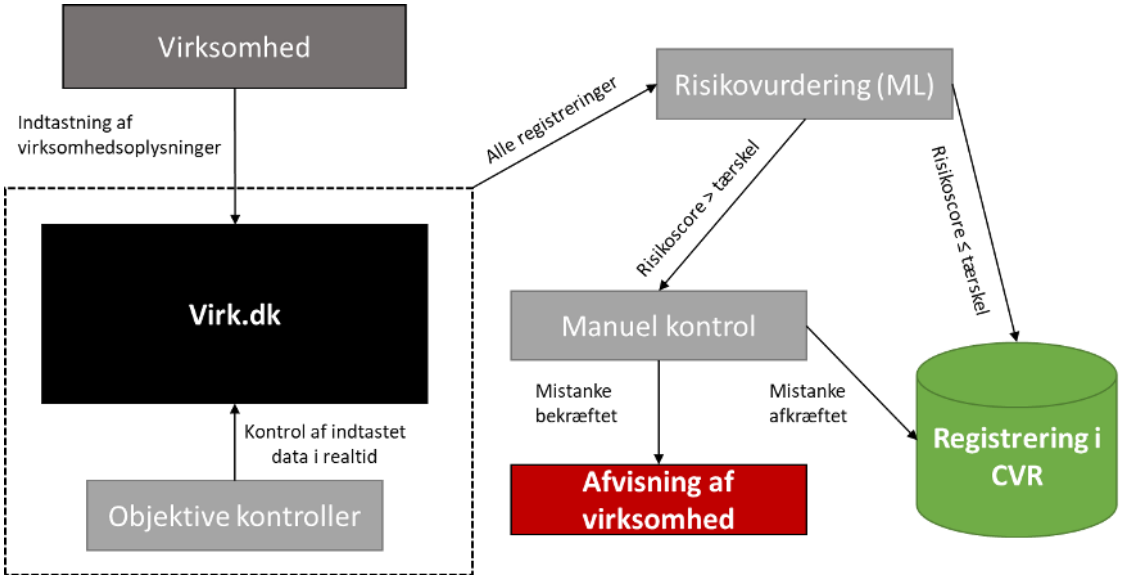
5.3. Kontrolmiljøet for registreringer i CVR

Finanstilsynet og Erhvervsstyrelsen har drøftet, hvilke tiltag der er implementeret for at sikre, at virksomheder ikke oprettes med fejlagtige data, eller at virksomheder ikke oprettes på et falsk grundlag.

CVR er helt generelt begrænset af, at virksomheder selv bærer ansvaret for at registrere relevante ændringer. Det begrænser muligheden for at lade registeret stå alene som kilde til kontrol af virksomhedsoplysninger. CVR indeholder desuden kun danske virksomheder. Det betyder, at de forpligtede enheder, der skal kortlægge ejer- og kontrolstrukturen, oplever, at sporet stopper, når den juridiske ejer er en udenlandsk virksomhed. I disse tilfælde er de afhængige af udenlandske virksomhedsregistre el. lign. for at kortlægge den fulde ejer- og kontrolstruktur.

Figur 5.1 viser den overordnede proces for den digitale registrering af en virksomhed i CVR eller efterfølgende ajourføring af relevante oplysninger. Virksomheden indtaster selv de nødvendige oplysninger, der gennemgår kontroller baseret på objektive kriterier i realtid. Herefter foretages en automatiseret risikovurdering af virksomheden. Den faktiske risikoscore har helt overordnet til formål at angive sandsynligheden for, at virksomheden i praksis oprettes med et andet formål end det beskrevne. Virksomheder med en risikoscore over en prædefineret tærskelværdi sendes til manuel kontrol og registreres kun, hvis risikoen afkræftes. Alle andre virksomheder registreres direkte i CVR.

Figur 5.1 – Procesoverblik for registrering af virksomhed i CVR



Kilde: Finanstilsynet.

Objektive kontroller

På Erhvervsstyrelsens webplatform er indbygget en række såkaldte objektive kontroller, der i det omfang, det er muligt, sammenholder de indtastede stamdata med andre kilder for at sikre, at informationerne er korrekte. Disse kontroller fungerer også som naturlige stopklodser for den videre registrering. Hvis informationerne ikke kan verificeres, kan registreringen ikke fortsættes. Eksempler på disse objektive kontroller er:

1. Verificering af indtastede CPR-numre ved at krydstjekke med CPR – eksisterer det registrerede CPR-nummer, og svarer navn mm. til de indtastede informationer?

2. Sammenkædning af udenlandske personer uden CPR-nummer med allerede kendte personer med samme pasnummer.

3. Krydstjek af adresse Bygnings- og Boligregisteret (BBR) – eksisterer den registrerede adresse, er der bygninger på adressen, og er andre selskaber registreret på adressen?

Udvælgelse til manuel kontrol

Risikovurderingen gennemføres ved brug af maskinlæring og sker i real tid. Systemet benytter en række maskinlæringsmodeller med hvert sit fokusområde, der alle er trænet på Erhvervsstyrelsens datagrundlag[19]. Det betyder, at risikoen ved nye virksomheder vurderes på baggrund af historiske observationer om virksomheder. Nogle modeller er fokuseret på tidligere forhold, eksempelvis om en registreret reel ejer tidligere har været involveret i mange oprettelser og afviklinger af virksomheder. Andre kan bruges til at verificere troværdigheden af et angivet pasnummer eller adresse for en udenlandsk person. Mere avancerede modeller kigger på generelle mønstre for den specifikke virksomhed og observerer eksempelvis nye sammenhænge, der skiller sig ud fra tidligere. Kendetegnende for modellerne er, at de bliver bedre og mere præcise i takt med, at man få mere data om en given virksomhed. Modellerne vil dermed kunne vurdere risikoen bedre, når virksomheden har været registreret i en længere periode og har indberettet årsrapporter mv.

Erhvervsstyrelsen fastsætter derudover selv grænseværdierne for de enkelte modeller, der ligger til grund for udvælgelsen til manuel kontrol. Værdierne fastsættes ud fra en vurdering af modellens resultater (både når den udvikles, og når den bruges), og en afvejning mellem risikoappetitten og de tilgængelige ressourcer. Dette er også i tråd med den politiske prioritering af, at det så vidt muligt skal være ligetil at oprette en virksomhed. Omvendt betyder det også, at virksomheder med kriminelt formål, der i det nuværende kontrolmiljø ikke får en risikoscore over den fastsatte grænseværdi, vil blive direkte registreret i CVR.

Muligheden for indsigelse mod registrering

Til trods for, at kontrolmiljøet altså både er omfattende og af høj kvalitet, er troværdigheden af data fortsat begrænset af, at det er virksomhederne selv, der forestår registreringen af de nødvendige oplysninger. Der er altså stadig en risiko for, at dygtige kriminelle aktører kan have held med at sløre hensigten med en virksomhedsregistrering.

De objektive kontroller er med til at sikre, at der er tale om faktiske personer, adresser mv. De indebærer dog ikke en verificering af, om oplysningerne for den givne virksomhed er korrekte. Kontrollerne er derudover særligt begrænsede for udenlandske personer, da der for disse af gode grunde ikke kan angives CPR-nummer, men navn, adresse og pasnummer. Risikovurderingen tilføjer et ekstra sikkerhedslag, men den kan ikke garantere, at alle potentielle kriminelle virksomheder undersøges manuelt af sagsbehandlere.

I forhold til kontrollen af de tilknyttede personers identitet er der dog indbygget et ekstra sikkerhedslag ved registrering af personer i CVR. Danske personer modtager en notifikation om deres registrering i e-boks, mens udenlandske personer modtager fysisk post på den angive adresse. Formålet med dette er både at gøre personer opmærksomme på deres registrering og at give dem muligheden for at gøre indsigelse mod denne registrering.

For danske personer må dette ekstra sikkerhedslag anses for at være særligt effektivt til at undgå utilsigtede registreringer. Er en registrering omvendt tilsigtet, vil den pågældende person være bevidst om registreringen og vil som følge deraf ikke have incitament til at gøre

[19] Indebærer også registerdata fra andre myndigheder, grundet Erhvervsstyrelsen relativt brede hjemmel til indsamling af data, jf. lov om Erhvervsstyrelsens behandling af data af den 8. maj 2018.

indsigelse. For udenlandske personer er sikkerhedslaget særligt begrænset. Det skyldes, at den fysiske post sendes til den adresse, virksomheden selv har registreret på personen.

5.4. Verificering ved advokater og godkendte revisorer

I forhold til hvidvasklovens krav vurderer Finanstilsynet, at det eksisterende kontrolmiljø ikke i tilstrækkelig grad sikrer, at CVR kan anvendes bredere som kilde til kontrol af virksomhedsoplysninger. Accepteres CVR som en tilstrækkelig kilde, er en mulig konsekvens, at barrierne for kriminelle aktører mindskes. Det begrænser bl.a. Finanstilsynet og andre myndigheders muligheder for at sanktionere eller reagere som følge af mangelfulde kundekendskabsprocedurer. Kommunikeres det, at det er tilstrækkeligt at kontrollere de nødvendige oplysninger i CVR, kan myndighederne i sagens natur ikke klandre virksomhederne for at gøre netop dette.

Problemet består som nævnt i, at kvaliteten af data i CVR ikke i alle tilfælde er tilstrækkelig. Denne problemstilling kan dog potentielt imødekommes ved, at advokater og godkendte revisorer får mulighed for at verificere virksomhedsoplysninger i CVR. Det skyldes, at de besidder et betroet erhverv, og at en sådan mekanisme kan sidestilles med andre vitterlighedspåtegninger, hvorigennem advokater og godkendte revisorer påtager sig et ansvar på vegne af deres kunder. Det gælder eksempelvis en revisorerklæring af en godkendt revisor i en årsrapport. I og med at advokater og godkendte revisorer også er underlagt hvidvaskloven, bør de kunne gennemføre verificeringen på baggrund af de informationer, de selv indhenter som led i deres kundekendskabsprocedurer. En sådan verificering af oplysningerne i CVR bør derfor kunne betrygge den forpligtede enhed og Finanstilsynet i, at de angivne informationer og identiteter er retvisende. Er det ikke tilfældet, kan ansvaret tilbageføres til både virksomheden og advokaten eller den godkendte revisor, der har gennemført verificeringen.

Da det i mange tilfælde også er advokater og godkendte revisorer, der opretter virksomheder og ajourfører data i CVR på vegne af deres kunder, kan opgaven med at verificere ses som en naturlig videreudvikling af deres rolle. Samtidig vil godtgørelsen sandsynligvis udgøre en mindre andel af det samlede salær.

En sådan mekanisme behøver dog ikke at blive gennemført som et krav for, at en virksomhed kan registreres i CVR. Derimod vil etableringen af muligheden gøre, at virksomhedskunder selv kan vælge det til, hvis de vurderer, at gevinsterne er store nok. Eksempelvis vil de ikke skulle indsende dokumentation til deres pengeinstitut, når der sker virksomhedsændringer, eller når kundekendskabet vedligeholdes, hvilket kan være en omkostningsfuld proces, særligt for større virksomheder[20]. I stedet vil de kunne bede deres godkendte revisor eller advokat genverificere data i CVR. Virksomheder og personer underlagt hvidvaskloven vil samtidig have et økonomisk incitament til at stille krav om gennemførelsen af en sådan verificering. Det skyldes bl.a., at mængden af ressourcer, de skal bruge på at kontrollere virksomhedsoplysninger som led i kundekendskabsprocedurerne, vil blive mindre.

For at denne funktionalitet kan fungere, er det dog afgørende, at der kan fastsættes klare rammer for, hvor længe en verificering kan anses som troværdig, og at det fremgår klart,

[20] Der kan bl.a. findes eksempler på større virksomheder, der har et tocifret antal medarbejdere ansat til at ajourføre denne type data hos sine finansielle modparter, jf. afsnit 4.2.

hvilke specifikke oplysninger der er verificeret. Det vil bl.a. være uhensigtsmæssigt, hvis virksomhedsstrukturen tilpasses efter, at en godkendt revisor har verificeret den i CVR, og at ændringen ikke registreres i CVR. Dette kan dog løses gennem krav om, at oplysninger kun kan bruges, hvis de er verificeret på ny. Der kunne eksempelvis være krav om periodisk opdatering af verificeringen og om, at risikoklassificeringen af den givne kunde betinger frekvensen.

Finanstilsynet vurderer samlet, at en øget brug af CVR til kontrol af oplysninger om virksomhedskunder bør undersøges nærmere, henset til de potentielle gevinster forbundet med dette.

6. Kontrol af identiteter ved brug af MitID

Finanstilsynet forventer, at MitID vil kunne bruges til kontrol af kunders identiteter ud over, hvad NemID kan bruges til i dag. Dette kan først fastslås endeligt, når MitID-loven træder i kraft, og MitID er udstedt bredt til personer i Danmark. Den videre udvikling af MitID-løsningen bør derfor følges tæt med dette formål in mente.

Virksomheder og personer underlagt hvidvaskloven skal som led i deres kundekendskabsprocedurer identificere og kontrollere deres kunders identitet. Det gøres i dag på forskellige måder. Hvad, der er tilstrækkeligt, afhænger både af risikoklassificeringen af kundeforholdet og af, om kunden møder fysisk op.

Kunder, som ikke møder fysisk frem hos virksomheden eller personen underlagt hvidvaskloven, kaldes distancekunder. I dag kontrolleres disse kunders identitet ofte gennem indsendelse af kopier af en række identifikationsdokumenter, såsom pas, kørekort og sygesikring. NemID er også en bredt anvendt kontrolkilde. Finanstilsynet tillader dog kun, at NemID står alene som kontrolkilde, når kunden, som følge af risikoklassificeringen, er underlagt lempede kundekendskabsprocedurer. I andre tilfælde vil yderligere dokumentation skulle indhentes.

En række aktører i sektoren har i lang tid haft et ønske om, at NemID skal kunne bruges bredere og som minimum stå alene som kontrolkilde for alle distancekunder, der grundet risikoklassificeringen ikke er underlagt skærpede kundekendskabsprocedurer. Det skyldes, at kunder i stigende grad onboardes uden fysisk fremmøde, og at processerne vedrørende kontrol af identitetsoplysninger i dag ofte er manuelle og derfor forbundet med betydelige omkostninger. Det har samtidig vist sig, at mange forbrugere finder det indgribende, at de løbende skal indsende dokumentation til eksempelvis deres pengeinstitut, eksempelvis deres pas. Endelig er indsendelse af kopier af identitetsdokumenter ikke nødvendigvis den sikreste måde at verificere kunders identitet på, og der er potentielt ikke bare mulighed for en nemmere og mindre indgribende verifikation, men også for en mere sikker verifikation.

Finanstilsynets vurdering af anvendelsesområdet for NemID stammer fra 2013. Begrænsningen i anvendelsesområdet af vurderingen skyldtes primært, at hvidvaskreglerne historisk har været indrettet sådan, at distancekunder per definition skulle underlægges skærpede kundekendskabsprocedurer. I de senere år har der været en stigende accept af, at elektroniske identitetsløsninger skal kunne bruges på lige fod med fysiske identitetspapirer. Der er eksempelvis blevet åbnet op for, at digitale identitetsløsninger i højere grad skal kunne bruges, både under hvidvaskdirektivet og den tilhørende vejledning udstedt af EBA. Der er også blevet implementeret et rammeværk for vurderingen af sikkerheden for disse løsninger i form af eIDAS-forordningen, der skal understøtte grænseoverskridende brug af elektroniske identitetsløsninger[21].

Trods denne udvikling fastholder Finanstilsynet vurderingen af anvendelsesområdet for NemID i vejledningen til hvidvaskloven fra november 2020[22]. Det skyldes bekymringer omkring sikkerhedsniveauet i NemID-løsningen, særligt at processerne for kontrol af identiteter ved udstedelsen af NemID historisk ikke har været tilstrækkelige i forhold til hvidvasklovens krav,

[21] Europa-Parlamentet og Rådets forordning (EU) nr. 910/2014.
[22] https://www.finanstilsynet.dk/nyheder-og-presse/sektornyt/2020/hvidvask_vejledning_031120

jf. afsnit 6.4. Samtidig er det Finanstilsynets forståelse, at kriminelle aktører ofte bruger videregivne NemID'er til deres aktiviteter, jf. afsnit 6.5.

I Danmark er Digitaliseringsstyrelsen godt i gang med at udvikle en ny elektronisk identitetsløsning, det såkaldte MitID, der skal erstatte NemID. Formålet er at skabe en løsning, der er mere sikker end NemID, og som derfor kan bruges bredere i både offentligt og privat regi. MitID er endnu ikke færdigudviklet, men forventes at være tilgængeligt i løbet af 2021.

Finanstilsynet har med udgangspunkt i løsningens nuværende design og Finanstilsynets nuværende vejledning om tilstrækkelige kontrolprocesser for distancekunder set nærmere på anvendelsesområdet for MitID. Analysen sammenholder udfordringerne ved NemID med mulighederne i MitID:

1. Sikkerheden ved MitID-løsningen, herunder særligt kontrollen af identiteten af de personer, et MitID udstedes til

2. I hvilket omfang løsningen kan medvirke til at mindske risikoen for, at et kundeforhold misbruges som følge af en videregivelse af et MitID.

Finanstilsynet vurderer, at et MitID på niveau "betydelig" under eIDAS-forordningen vil kunne stå alene som kontrolkilde for distancekunder, der ikke er underlagt skærpede kundekendskabsprocedurer. Det skyldes, at processerne for kontrol af identiteter ved udstedelsen af et MitID er mindst lige så sikre, som hvad Finanstilsynet som udgangspunkt forventer er tilfældet for distancekunder under hvidvaskloven, jf. afsnit 6.7. Derudover er sikkerhedsniveauet ved autentificeringsmidlerne i MitID-løsningen højere end i NemID-løsningen.

En betingelse er, at virksomheder og personer underlagt hvidvasklovens krav fortsat har indrettet deres procedurer for risikoklassificeringen af kundeforhold sådan, at risikoen for misbrug som følge af videregivelse af et MitID mindskes i tilstrækkelig grad.

Finanstilsynet vurderer, at MitID-løsningen også kan understøtte disse processer, jf. afsnit 6.7. Det skyldes muligheden for, at MitID-brokers[23] ved brug af såkaldte risikodata får mulighed for at etablere ekstra kontroller, der bl.a. kan fungere som indikatorer på videregivelse. En betingelse for dette er, at MitID-loven sikrer, at virksomheder har adgang til at inddrage udfaldet af de ekstra sikkerhedslag i deres kundekendskabsprocedurer.

Kommunikation omkring et bredere anvendelsesområde for MitID end NemID vil skulle gennemføres via en opdatering af vejledningen til hvidvaskloven. Det bør i den forbindelse understreges, at Finanstilsynets vurdering udelukkende relaterer sig til verificering af identiteten på kunder. Virksomheder og personer omfattet af hvidvaskloven vil fortsat skulle gennemføre andre nødvendige elementer af kundekendskabsprocedurerne[24].

Vurderingen forudsætter, at den videre udvikling af MitID-løsningen ikke ændrer på de forhold, der lægges til grund for vurderingen.

[23] Tjenesteudbydernes (pengeinstitutter mv.) adgang til MitID-løsningen, jf. afsnit 6.4.
[24] I forhold til det konkrete kundeforhold kan der være behov for at indhente andre oplysninger, eksempelvis om forretningsforbindelsens formål og tilsigtede beskaffenhed, jf. afsnit 1, og om kundens økonomi og mv.

6.1. Fokus på bredere brug af eletroniske identitetsløsninger i EU

Historisk har det ligget i hvidvaskreglerne, at etablering af kundeforhold med distancekunder per definition er forbundet med øget risiko for hvidvask og terrorfinansiering. Det fremgik specifikt af artikel 12, stk. 2, i det tredje hvidvaskvaskdirektiv (AMLD3), der trådte i kraft i 2005[25], at:

> *"Hvis kunden ikke har været fysisk til stede for at legitimere sig, pålægger medlemsstaterne disse institutter og personer at træffe særlige, passende foranstaltninger til at opveje den højere risiko."*

Dette specifikke krav bortfaldt med implementeringen af det fjerde hvidvaskdirektiv i 2015 (AMLD4)[26]. Ordlyden blev i stedet, at kundekendskabsprocedurerne skulle gennemføres ud fra en risikobaseret tilgang. Det indebærer, at der ikke per automatik skal gennemføres skærpede kundekendskabsprocedurer for distancekunder. Den reviderede udgave af AMLD4 fra 2018 understreger videre, at reguleringen bør være teknologineutral[27]. Det fremhæves i præambel 22, at den seneste teknologiske udvikling inden for digitalisering af transaktioner og betalinger muliggør sikker fjernidentifikation eller elektronisk identifikation, og at der i lyset af eIDAS-forordningen bør tages hensyn til brugen af sådanne identifikationsmidler.

Det samme kommer til udtryk i de reviderede retningslinjer til AMLD4, der er udarbejdet af EBA i samspil med ESMA og EIOPA[28]. Retningslinjerne fokuserer på virksomhedernes kundekendskabsprocedurer, herunder hvilke risikofaktorer virksomheder skal være opmærksomme på i forbindelse med risikovurderingen og risikoklassificeringen af kundeforholdet.

Retningslinjerne berører specifikt distancekunder under punkt 4.29, 4.30 og 4.31. Af punkt 4.29 og 4.30 fremgår det, at virksomhederne skal tage tilstrækkelige skridt for at sikre:

1. At den angivne identitet og den faktiske person er den samme,
2. at virksomheden forholder sig til, om det giver anledning til øget risiko, at kundeforholdet ikke etableres fysisk, samt
3. at der gennemføres skærpede kundekendskabsprocedurer, herunder vurderes om det er nødvendigt med skærpede procedurer for kontrol af identiteter, hvis kundeforholdet er forbundet med en øget risiko.

Det pointeres dog under punkt 4.31, at brugen af et elektroniske identitetsløsninger som kontrolkilde ikke i sig selv giver anledning til øget risiko. Særligt ikke, hvis sikkerhedsniveauet kan kvalificeres som "højt" under eIDAS-forordningen:

> *"Firms should have regard to the fact that the use of electronic means of identification does not of itself give rise to increased MLTF risk, in particular where these electronic means provide a high level of assurance under Regulation (EU) 910/201420"*

[25] Europa-Parlamentets og Rådets Direktiv 2005/60/EF af 26. oktober 2005.
[26] Europa-Parlamentets og Rådets Direktiv (EU) 2015/849 af 20. maj 2015.
[27] Europa-Parlamentets og Rådets Direktiv (EU) 2018/843 af 30. maj 2018.
[28] EBA guidelines (EBA/GL/2021/02) af 1. marts 2021.

Det bemærkes samtidig under punkt 4.33, at virksomheder, der gør brug af teknologiske løsninger, skal vurdere, om sådanne løsninger håndterer eller potentielt øger risiko for hvidvask eller terrorfinansiering. Her fremhæves bl.a. risikoen for svindel med identiteter.

Ændringen afspejler en erkendelse af, at onboarding af distancekunder ikke nødvendigvis fører til højere risiko, hvis der bruges troværdige elektroniske identitetsløsninger[29]. FATF har fastslået det samme i deres vejledning om digitale identiteter fra marts 2020[30].

Finanstilsynet vurderer i lyset af dette, at der bør tages stilling til, under hvilke omstændigheder MitID og andre lignende elektroniske identitetsløsninger kan bruges i forbindelse med virksomhedernes kundekendskabsprocedurer.

6.2. Finanstilsynets vurdering af NemID i 2013

Finanstilsynet offentliggjorde den 13. marts 2013 en konkret vurdering af anvendelsesområdet for NemID[31]. Vurderingen gælder fortsat. Den fastsætter, at NemID med tilknyttet OCES-certifikat kan bruges som eneste kontrolkilde for kunder med lav risiko, hvis:

1. Kunden underskriver dokumenter ved anvendelse af NemID som bekræftelse på kundens navn (identitet), og

2. at virksomheden sammenholder de fra kunden modtagne oplysninger med oplysningerne i CPR-registret, som bekræftelse på kundens adresse og CPR-nr.

Vurderingen af, at NemID kun kan stå alene (sammen med CPR-nummer) som kilde til kontrol af lavrisikokunders identitet, tog udgangspunkt i den daværende hvidvasklov fra 2013[32], der i § 19, stk. 2, fastsatte et specifikt krav om, at virksomhederne gennemførte skærpede kundekendskabsprocedurer for distancekunder[33].

> *"I de situationer, hvor et kundeforhold etableres, uden at den pågældende kunde har været fysisk til stede for at legitimere sig, stilles der krav om skærpede legimitationsprocedurer."*

Kravene i § 19 blev gennemført i 2006 som led i implementeringen af AMLD3. Af bemærkningerne til lovforslagets § 19, stk. 2, fremgår det, at[34]:

> *"Den skærpede opmærksomhed kan eksempelvis ske ved at modtage supplerende legitimation. Hvis den almindelige legitimation sker ved f.eks. kørekort eller pas, kan*

[29] Af præambel 18 til AMLD4 fremgår: "Dette direktiv bør også gælde for aktiviteter, som de forpligtede enheder, der er omfattet af direktivet, udfører over internettet". Af præambel 19 fremgår endvidere: "Nye teknologier bibringer virksomheder og kunder tids- og omkostningseffektive løsninger, og der bør derfor tages højde for dem, når der foretages en risikovurdering."
[30] "Non-face-to-face customer-identification and transactions that rely on reliable, independent digital ID systems with appropriate risk mitigation measures in place, may present a standard level of risk, and may even be lower-risk".
[31] www.finanstilsynet.dk/Tilsyn/Tilsynsreaktioner/Vejledende-fortolkninger/Hvidvask-12-19-NemID
[32] Bekendtgørelse af lov om forebyggende foranstaltninger mod hvidvask af udbytte og finansiering af terrorisme af 13. august 2013.
[33] Af bemærkninger til § 19, stk. 1, fremgår det, at distancekunder dengang per definition var forbundet med en øget risiko: "De skærpede legitimationsforanstaltninger skal ske på grundlag af en vurdering af risikoen og i situationer, som i sig selv indebærer en øget risiko for hvidvask af penge og finansiering af terrorisme."
[34] Forslag til Lov om forebyggende foranstaltninger mod hvidvask af udbytte og finansiering af terrorisme fremsat den 9. november 2005.

den supplerende legitimation f.eks. være sygesikringsbevis. Kontrollen af de udleverede dokumenter kan f.eks. ske ved at sammenholde dokumenterne eller, hvis der er tale om et dokument udstedt af en af de nævnte virksomheder eller personer, ved at kræve en bekræftende attestering af dokumentet."

I bemærkningerne til § 19, stk. 2, tages der ikke specifikt stilling til anvendelsesområdet for NemID. En gennemgang af de efterfølgende ændringer frem mod hvidvaskloven fra den 13. august 2013 viser, at hverken § 19 eller bemærkningerne hertil er blevet ændret, siden de blev inkluderet i hvidvaskloven.

En gennemgang af de historiske dokumenter relateret til Finanstilsynets vurdering af anvendelsesområdet for NemID underbygger, at vurderingen er baseret på § 19, stk. 2. Eksempelvis henviste Finanstilsynet den 4. februar 2011 til § 19, stk. 2, i et svar på et paragraf 20-spørgsmål[35]:

"I de tilfælde, hvor en kunde ikke kommer fysisk til stede for at legitimere sig, stiller hvidvaskloven krav om, at virksomhederne træffer yderligere foranstaltninger for at sikre kundens identitet. Det kan f.eks. være indhentelse af supplerende dokumentation, eller krav om at de udleverede dokumenter attesteres af relevant myndighed eller advokat.

Det betyder således, at virksomhederne ved etablering af et kundeforhold ikke alene kan basere sig på digital signatur eller NemID, da hvidvaskningsloven forpligter virksomhederne yderligere."

Undtagelsen for kunder med lav risiko var derfor en lempelse i forhold til ordlyden i både den daværende hvidvasklov og AMLD3.

6.3. Hvidvaskloven efter AMLD4

I 2017 blev det 4. hvidvaskdirektiv implementeret i dansk lov. Det medførte bl.a., at § 19 i den daværende hvidvasklov bortfaldt. Af bemærkningerne fremgår følgende[36]:

"I overensstemmelse med 4. hvidvaskdirektiv anser Erhvervs- og Vækstministeriet det for hensigtsmæssigt at begrænse antallet af tilfælde, hvor der i hvidvaskloven stilles skærpede krav til kundekendskabsprocedurer. Dette betyder blandt andet, at det, at en kunde ikke har været fysisk til stede for at legitimere sig, fremover ikke automatisk medfører øget risiko for hvidvask og terrorfinansiering. Dette vil i stedet bero på en konkret risikovurdering."

Derudover fremgår det af § 11, stk. 3:

"Virksomheder og personer skal gennemføre alle kundekendskabskrav, jf. stk. 1 og 2. Omfanget af kundekendskabsproceduren kan dog gennemføres ud fra en risikovurdering."

[35] Spørgsmålet var: "Er ministeren enig med Finansrådet i, at NemID eller en digital signatur ikke er tilstrækkeligt til at identificere en bankkunde i forhold til "hvidvaskloven"?"
[36] Forslag til lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme fremsat den 13. oktober 2016.

De forpligtede enheder har dermed fået en større fleksibilitet til at fastlægge deres procedurer, men bærer fortsat ansvaret for at sikre, at procedurerne er tilstrækkelige. Kontrollen af kundernes identitetsoplysninger er fortsat et delelement af virksomhedernes kundekendskabsprocedurer, men de specifikke krav er udgået, hvad angår distancekunder.

Risikoklassificeringen af kundeforholdet ligger til grund for omfanget af kundekendskabsprocedurerne. I forhold til kontrollen af en kundens identitet har risikoklassificeringen primært indflydelse på omfanget af processerne, altså hvor mange kontroller der skal gennemføres for en given identitet.

Finanstilsynets beskriver i vejledningen til hvidvaskloven en række tiltag, der kan medvirke til at sikre en tilstrækkelig kontrol af distancekunders identitet, og fastholder, at distancekunder kan være forbundet med øget risiko. Det tilskrives forhold, som eksempelvis at billedlegitimation sendt over internettet ikke giver den samme sikkerhed, som hvis kunden møder fysisk op med billedlegitimation.

Vejledningen berører også brugen af NemID og andre former for elektroniske identitetsløsninger som kontrolkilde og præciserer, at NemID kan betragtes som en pålidelig og uafhængig kilde på linje med pas eller kørekort. I tråd med vurderingen fra 2013 fastholdes det også, at NemID kun kan stå alene som kontrolkilde, hvis kunden er underlagt lempede kundekendskabsprocedurer. I andre tilfælde skal andre kontrolkilder eller mitigerende tiltag inddrages sammen med NemID.

At NemID kun kan stå alene for kunder underlagt lempede kundekendskabsprocedurer skyldes en bekymring, som udspringer af, at processen for kontrol af identiteter ved onboarding til NemID-løsningen historisk ikke har været sikker nok[37]. Samtidig er nøglekortet relativt let at videregive sammen med andre relevante oplysninger til kriminelle aktører, så en identitet kan misbruges til hvidvask eller terrorfinansiering. Det er eksempelvis ligetil at tage billede af papkortet og sende det i en mail sammen med CPR-nummer og adgangskode.

6.4. Højere sikkerhed ved MitID end NemID

MitID-løsningen udvikles og skal drives i et samarbejde mellem Digitaliseringsstyrelsen og Finans Danmark (MitID-partnerskabet). Modsat NemID, der var ejet og styret af Nets, og fungerer som to separate systemer (en hybrid offentlig og privat løsning), bliver MitID ét samlet system (MitID-kernen). Det har en række sikkerhedsmæssige fordele, og denne arkitektur er samtidig lettere at udbygge i takt med, at nye behov og trusler opstår. Samtidig betyder det, at der fremadrettet kun vil eksistere én offentlig elektronisk identitetsløsning.

Sikkerhedsniveau "betydelig" under eIDAS er udgangspunktet

MitID-løsningen vil blive anmeldt på to sikkerhedsniveauer (betydelig og høj) under eIDAS-forordningen. Det samlede sikkerhedsniveau fastsættes ud fra en vurdering af tre forhold:

- **Identity Assurance Level (IAL):** Beskriver styrken af registreringsprocessen, herunder identitetssikringsprocessen, dvs. hvor sikker udstedelsen af et MitID er.

[37] Det skyldes bl.a., at digitale signaturer blev migreret til NemID, og særligt, at pengeinstitutterne har forestået udstedelsen af mange NemID uden at kontrollere identiteten i tilstrækkelig grad i forhold til hvidvaskloven.

- **Authenticator Assurance Level (AAL):** Beskriver sikringsniveauet af identifikationsmidlerne, der kan bruges til autentifikationen, dvs. hvor sikker brugen af MitID er.

- **Federation Assurance Level (FAL):** Beskriver sikringsniveauet af selve MitID-løsningen, dvs. både sikkerheden ved løsningen og de udbydere, der indgår i løsningen.

I MitID regnes sikkerhedsniveauet ud som minimum af IAL, AAL og FAL. Forventningen er, at det gængse MitID vil blive udstedt på niveau "betydelig".

Udgangspunktet for identitetssikringsprocessen (udstedelse) under MitID er, at vedkommende, der skal have MitID udstedt, er fysisk tilstede og fremviser et bevis for sin identitet, som er anerkendt af staten, og som kontrolleres for sin validitet, eksempelvis et pas. Derudover gennemføres en række andre kontroller, eksempelvis sammenholdning af de angivne informationer for personer med et CPR-nummer med informationer i CPR[38]. Kravene er mere restriktive end de krav, der historisk har været gældende for NemID, og svarer også til kravene for godtgørelse og kontrol af identitet på sikkerhedsniveau "høj" under eIDAS-forordningen, jf. afsnit 2.1.2. i eIDAS' gennemførselsforordning[39].

Brugen af den rette teknologi kan dog sikre, at der kan etableres lige så sikre identifikationsmetoder til at kontrollere identiteten ved udstedelser til distancekunder som ved fysisk fremmøde. Eksempelvis har mange nye pas indbygget en chip, som ved aflæsning bl.a. giver adgang til et billede af ejeren. Ved at etablere de rette processer kan aflæsningen af chippen i passet være lige så sikker som et fysisk fremmøde. Et eksempel er brugen af digitale teknikker til ansigtsgenkendelse, der kan sammenholdes med billedet af personen i passet. Partnerskabet overvejer derfor også, i hvilket omfang sådanne alternativer kan bruges, eksempelvis ved onboarding gennem en app. Sådanne metoder er særligt relevante for brugere, der skal migreres fra NemID til MitID. Det vil nemlig være en omkostningsfyldt og tidskrævende proces, hvis alle brugere skal møde fysisk op hos eksempelvis borgerservice for at få udstedt MitID. MitID med sikkerhedsniveau "betydelig" eller "høj" vil dog kun kunne udstedes, enten som nyt eller ved en migrering fra NemID, hvis identitetsverificeringen vurderes ligeså sikker som ved fysisk fremmøde.

Den primære forskel mellem et MitID på sikkerhedsniveau "betydelig" og et på sikkerhedsniveau "høj" er altså ikke processen for kontrol af identitet, men derimod det tilknyttede identifikationsmiddel.

Nøglekortet, som vi kender det fra NemID, vil udgå med MitID. Identifikationsmidlerne omfatter i stedet en app, en kodeviser, en chipløsning og en kodeoplæser. De to første løsninger er primært rettet mod almindelige borgere, som vil få adgang til appen som autentifikationsmekanisme, hvilket er en opgradering af sikkerheden i forhold til nøglekortet[40]. MitID-chippen er primært rettet mod brugere med adgang til følsomme personhenførbare oplysninger. Kodeoplæsere er rettet mod borgere, der ikke kan læse en kode, såsom svagtseende og blinde.

[38] Andre mulige kontroller er verificering af pas/kørekort i rigspolitiets register, kontrol ved vidne, andre ægtheds- og gyldighedskontroller af anvendte kontrol identitetsdokumenter mv.
[39] Kommissionens gennemførselsforordning (EU) 2015/1502 af 8. september 2015.
[40] Det skyldes 1) at der eksisterer et ekstra sikkerhedslag i form af indtastning af pinkode til både telefon og brugernavn og pinkode til appen, samt 2) at appen – og MitID generelt – kun kan bruges i realtid (autentifikation sendes først til appen efter indtastning af brugernavn og password i loginvindue) modsat nøglekortet (hvor alle koder kan tilgås så snart nøglekortet besiddes).

Der gælder følgende krav til en autentifikationsløsning på sikkerhedsniveau "betydelig", jf. afsnit 2.2.1 i eIDAS gennemførselsforordningen:

1. Det elektroniske identifikationsmiddel gør brug af mindst to autentifikationsfaktorer fra forskellige kategorier.

2. Det elektroniske identifikationsmiddel er udformet, så det antages, at det kun kan bruges af den person, som det tilhører, og som har kontrol over og er i besiddelse af det.

For en autentifikationsløsning på niveau "høj" gælder samme krav, foruden følgende:

3. Det elektroniske identifikationsmiddel er beskyttet mod kopiering, manipulation og angribere med stor angrebskapacitet.

4. Det elektroniske identifikationsmiddel er udformet, så den person, som det tilhører, kan beskytte det sikkert mod, at andre bruger det.

Det forventes ikke, at appen kan opnå sikkerhedsniveau "høj". Det skyldes ikke sikkerheden ved selve appen, men derimod sikkerheden ved den platform, den installeres på (eksempelvis mobiltelefonen). Blandt nogle europæiske myndigheder eksisterer der stadig tvivl om, hvorvidt hardwaren i en mobiltelefon eller computer kan modstå forsøg på kopiering eller manipulation.

Det forventes derimod, at MitID-chippen vil blive registreret på sikkerhedsniveau "høj". Der er dog flere omkostninger ved udstedelsen af en MitID-chip end ved appen. Den vil derfor kun blive udstedt i særlige tilfælde, med mindre brugeren selv betaler. Særlig tilfælde er eksempelvis, når en person har adgang til følsomme personhenførbare oplysninger i offentligt regi såsom personers sundhedsdata.

Ekstra sikkerhedslag ved brokeren
MitID-kernen håndterer de kritiske funktioner for løsningen som registrering af identiteter i en ID-database og udstedelse af identifikationsmidler. Brugere af løsningen vil udelukkende tilgå kernen gennem de såkaldte MitID-brokere, der står for integrationen mellem MitID-kernen og tjenesteudbyderne. Aftaleforholdene bliver derfor tredelte (kernen til brokere og brokere til tjenesteudbydere) fremfor todelte (kernen til tjenesteudbyder), som de var under NemID.

Det betyder bl.a., at brug af MitID, eksempelvis når en kunde vil logge ind på sin netbank, sker gennem en broker. Brokeren modtager brugerens loginoplysninger, når de bruges til at få adgang til tjenesteudbyderen, og sender dem videre til kernen, som autentificerer dem. Autentifikationssvaret sendes så tilbage til brokeren sammen med en række risikodata, herunder angivelse af sikkerhedsniveauet ved det givne MitID. Brokeren kan bruge disse risikodata til at bygge ekstra sikkerhedslag, jf. afsnit 6.7. Det kan eksempelvis være oplysninger om brugerens geolokation eller antal mislykkede loginforsøg, som tjenesteudbyderen kan bruge til at vurdere, om det er den korrekte bruger, der anvender MitID'et.

6.5. Videregivelser og misbrug af NemID i praksis

Finanstilsynet har været i dialog med relevante myndigheder for at afdække, hvordan videregivne NemID'er i praksis kan misbruges.

Der findes generelt to måder, hvorpå et NemID kan videregives: tilsigtet og utilsigtet. Tilsigtet videregivelse er, hvis en person efter udstedelsen bevidst overdrager NemID'et til en tredjepart, eksempelvis ved at sælge det. Det kan også ske ved, at personen trues til at videregive det, eller bevidst lader en anden bruge det uden at sætte sig ind i årsagen. Utilsigtet videregivelse sker, hvis et NemID bruges, uden at indehaveren er bevidst om det. Det kan eksempelvis ske ved, at en kriminel aktør aflurer brugernavn og adgangskode og kopierer eller stjæler det tilknyttede nøglekort.

Det er Finanstilsynet forståelse, at tilsigtet videregivelse af NemID udgør en væsentligt udfordring i forhold til bekæmpelsen af hvidvask. Problemet opstår typisk ved, at en kriminel aktør opnår adgang til en række NemID'er. Derved kan den kriminelle bagmand opnå adgang til eksempelvis en række bankkonti, som er oprettet af andre personer, og som kan bruges til sløring af midlers oprindelse eller anden form for hvidvask. Det kan både ske gennem private kundeforhold og kundeforhold for virksomheder, hvor en given person er indsat som stråmand, jf. afsnit 5.2. Dette er særligt problematisk, da det i retten kan være svært at bevise, at personen, hvis NemID er blevet brugt, har været bevidst om videregivelsen af NemID'et, og at personen har været bevidst om formålet.

Det er Finanstilsynets forståelse, at brugen af mere end én kilde til kontrol af identiteten af en kunde (eksempelvis NemID og kopi af pas) ikke nødvendigvis vil begrænse problemet med tilsigtet videregivelse af NemID. Det skyldes, at personer, der er villige til at videregive deres NemID, i de fleste tilfælde også vil være villige til at videregive andre identitetsdokumenter såsom pas og kørekort. Videregivelsesproblematikken relaterer sig derved primært til, at det i praksis er meget svært løbende at kontrollere identiteten på en kunde, der ikke er fysisk til stede ved iværksættelsen af en transaktion. Det gælder eksempelvis når der foretages en betaling gennem en kundes netbank.

6.6. Tilgangen i andre nordiske lande

Finanstilsynet har overordnet drøftet anvendelsesområdet for elektroniske identitetsløsninger med tilsynsmyndighederne i hhv. Norge, Sverige og Finland. Formålet var at afklare, i hvilket omfang de tillader, at sådanne løsninger kan stå alene som kilde til kontrol. Ingen af disse lande udbyder dog en offentlig løsning, derimod er forskellige sektordrevne løsninger tilgængelige. Den mest anvendte løsning i Sverige og Norge kaldes BankID.

Helt generelt er holdningen på tværs af det nordiske samarbejde, at elektroniske identitetsløsninger som udgangspunkt bør kunne stå alene som kilde til kontrol af identiteter. Det tilskrives særligt, at teknologien i dag er på et niveau, hvor løsningerne kan gøres meget sikre og i nogle tilfælde mere sikre, end hvad der er praksis for kontrollen af identiteter i dag. Alle tre lande henviste i den forbindelse også til eIDAS-forordningen, men der var forskellige udmeldinger om, hvorvidt sikkerhedsniveauet skulle være på "betydelig" eller "høj". Alle landene var enige om, at risikoklassificeringen fortsat bør kunne lede til, at der skal gøres yderligere for at kontrollere identiteten, eksempelvis grundet risikoen for videregivelse.

Det Norske Finanstilsyn fulgte op på dialogen per mail og bekræftede, at de som udgangspunkt tillader brug af elektroniske identitetsløsninger, jf. § 4-3, tredje led, i hvitvaskingsforskriften[41]. De pointerede også, at sikkerheden i løsningen bør være på niveau "højt" under eIDAS, og fastholdt, at anvendelsesområdet altid bør betinges af en risikoklassificering af kundeforholdet grundet risikoen for videregivelse.

6.7. MitID i forhold til hvidvasklovens krav

Hensigten er, at den gængse bruger får udstedt et MitID på sikkerhedsniveau "betydelig" og vil bruge nøgleappen som autentifikationsmiddel. Finanstilsynets vurdering er derfor baseret på dette scenarie.

MitID er som udgangspunkt tilstrækkeligt

Vurderingen af, om et MitID kan stå alene som identifikationsfaktor for distancekunder, tager udgangspunkt i følgende eksempel på en tilstrækkelig proces for en dansk kunde, der ikke er underlagt skærpede kundekendskabsprocedurer:

1. Kunden oplyser navn og CPR-nummer.
2. Kunden underskriver med et OCES-certificeret NemID, og CPR-nummeret sammenholdes med CPR.
3. Der indhentes yderligere kontroldokumenter, eksempelvis i form af kopi af pas eller lønseddel.

I det opstillede eksempel på en tilstrækkelig identifikationsproces kontrolleres identiteten først og fremmest ved brug af NemID og CPR. Den forpligtede enhed skal dog også gennemføre en ekstra kontrol ved at indhente en kopi et kundens pas. Formålet er primært at sikre, at det benyttede NemID faktisk er udstedt til den person, som det er registeret til.

Som beskrevet i afsnit 6.4 indebærer identifikationsprocessen ved udstedelse af MitID, at kunden møder fysisk op med et pas, eller at den forpligtede enhed gennemfører en tilsvarende sikker kontrol af kundens identitet. Derudover sammenholdes de angivne oplysninger også med CPR.

Finanstilsynets vurderer derfor, at et MitID udstedt på niveau "betydelig" bør være tilstrækkelig kilde til kontrol af kunder, der ikke er underlagt skærpede kundekendskabsprocedurer. Det skyldes, at processen for kontrol af identiteter ved udstedelsen af MitID som udgangspunkt er mindst lige så omfattende, som hvidvaskloven kræver i dag.

Vurderingen underbygges desuden både af EBA's vejledning til hvidvaskdirektivet, jf. afsnit 6.1, og at den ekstra sikkerhed ved at modtage et kopi af identifikationsdokumenter i forhold til at kunne opdage aktiviteter som følge af videregivne identiteter er marginal, jf. afsnit 6.5. Samtidig anses vurderingen langt hen af vejen for at være på linje med retstilstanden hos vores nordiske naboer, jf. afsnit 6.6.

[41] Forskrift om tiltak mot hvitvasking og terrorfinansiering af 14. september 2018.

Finanstilsynet vurderer også, at andre elektroniske identitetsløsninger kan stå alene som kilde til kontrol af en kundens identitet, hvis sikkerheden er på samme niveau, som angivet i vurderingen af MitID, og kunden ikke er underlagt skærpede kundekendskabsprocedurer.

Risikoen for videregivelse bør indgå i risikoklassificeringen

Det er ikke tilstrækkeligt, at et MitID med høj grad af sikkerhed er udstedt til den rette person, hvis det er let at videregive. De forpligtede enheder vil derfor fortsat altid skulle vurdere, om det er nødvendigt at underlægge en given kunde skærpede kundekendskabsprocedurer og dermed tage yderligere risikobegrænsende tiltag i brug i forbindelse med kontrollen af identitet. Videregivelser, og primært tilsigtede videregivelser, er et reelt problem i praksis, når det kommer til hvidvask og terrorfinansiering, jf. afsnit 6.5. Det understøttes også af EBA's vejledning til hvidvaskdirektivet, jf. afsnit 6.1.

Det vil altid være muligt tilsigtet at videregive oplysninger med henblik på misbrug af identitet. I det opstillede eksempel på en tilstrækkelig identifikationsproces for distancekunder i dag kan en person eksempelvis videregive sine personoplysninger, logininformationer, pas og nøglekortet til NemID. Et af problemerne med NemID er netop, at nøglekortet let kan videregives, jf. afsnit 6.3. Det kan ikke afvises, at problemstillingen omkring tilsigtet videregivelse også vil gøre sig gældende ved MitID-løsningen.

I henhold til eIDAS vil risikoen for utilsigtet videregivelse også forsat eksistere for et MitID på sikkerhedsniveau "betydelig", jf. afsnit 6.4. Autentifikationsmidler på dette niveau vil dog alt andet lige være mere sikre end nøglekortet, når det kommer til risikoen for en utilsigtet videregivelse. Det skyldes bl.a., at det vil være lettere at kopiere et nøglekort, end det vil være at kopiere de nye autentifikationsmidler som eksempelvis en app eller en nøgleviser. Som udgangspunkt vil en kriminel aktør enten skulle hacke en telefon eller kende pinkoden til telefonen og stjæle denne for at få adgang til MitID-appen. Et nøglekort kan derimod affotograferes eller stjæles. Nøglerne på et stjålet nøglekort vil desuden være tilgængelige og kunne bruges uden, at personen, det er udstedt til, løbende bliver opmærksom på det. I MitID-appen vil brugeren få en notifikation om godkendelse, hver gang MitID'et bruges.

Finanstilsynet fremhæver i vejledning til hvidvaskloven, at det, afhængigt af risikoklassificeringen, kan være nødvendigt at gennemføre såkaldte mitigerende tiltag, når NemID bruges. Det kan eksempelvis ske ved at:

- kunden modtager en unik kode på sit mobiltelefonnummer, som kunden efterfølgende kan oplyse som en yderligere kontrol

- kundens geolokation kontrolleres ud fra den anvendte IP-adresse, hvormed det kan ses, om kunden er aktiv fra en placering, som adskiller sig fra, hvor kunden sædvanligvis er aktiv – eksempelvis et andet land.

Eksemplerne på mitigerende tiltag i vejledningen kan anses som tiltag, der har til hensigt at besværliggøre processen for kriminelle. Det vil i alle tilfælde også være sværere at opdage en videregivelse, når et kundeforhold oprettes, end efter at kundeforholdet er etableret. Det skyldes, at der ikke kan lægges faktisk adfærd, som eksempelvis er observeret i forbindelse med transaktionsovervågningen, til grund for vurderingen på dette tidspunkt. I det løbende

kundeforhold vil der være flere kontaktpunkter, og det vil derfor være lettere at identificere mistænkelig kundeadfærd.

I MitID-løsningen har MitID-brokeren mulighed for at opstille ekstra sikkerhedslag på baggrund af de risikodata, som et autentifikationssvar suppleres med, jf. afsnit 6.4. Det indebærer også muligheden for at identificere brugerens geolokation, bl.a. på baggrund af den observerede IP-adresse for den platform, som autentifikationsmidlet er installeret på. Andre eksempler er observationer af, hvornår MitID'et er registeret, tidspunktet for seneste autentifikation og antallet af tidligere fejlidentifikationer. Nogle risikodata skal aggregeres for at kunne videregives til broker, mens andet kan videregives som rådata. Derudover er det endnu uvist, i hvilket omfang brokere kan videregive disse data til tjenesteudbyderne.

Finanstilsynet vurderer, at MitID-løsningen derfor også her har større potentiale end NemID-løsningen til at understøtte en troværdig kontrol af kundens identitet. Det skyldes muligheden for at bygge ekstra sikkerhedslag, der kan understøtte risikoklassificeringen af kundeforholdet med henblik på at tage højde for mulige videregivelser ved både oprettelse og løbende vedligeholdelse af kundeforholdet. Rigtigt angrebet bør sådanne sikkerhedslag også som minimum kunne mitigere risikoen for videregivelse i samme omfang, som eksemplerne på mitigerende tiltag i vejledningen til hvidvaskloven.

Disse sikkerhedslag er ikke bygget ind i MitID-løsningen. Det er derfor op til de forpligtede enheder at sikre, at den benyttede broker har etableret dem. Derudover er det nødvendigt, at de forpligtede enheder kan få adgang til de relevante risikodata eller analyser, så de kan inddrages i kundekendskabsprocedurerne. Finanstilsynet har oplyst Digitaliseringsstyrelsen om dette behov i sit høringssvar til lov om MitID og NemLog-in.

7. PEP-løsning i regi af en offentlig myndighed

Finanstilsynet indstiller, at det besluttes, om der skal arbejdes videre med de to foreslåede løsningsmodeller, og i så fald hvilken, samt i hvilken myndighed PEP-løsningen skal forankres. Begge modeller kræver ændringer af hvidvaskloven og PEP-bekendtgørelsen, som bør igangsættes, hvis det besluttes at arbejde videre hermed.

Virksomheder og personer underlagt hvidvaskloven er forpligtet til at undersøge, om en kunde er en politisk eksponeret person (PEP), eller om kunden er nærtstående eller har nære forretningsforbindelser til en PEP. Erhvervsministeriet understøtter i dag denne proces ved at lade Finanstilsynet føre en offentlig tilgængelig liste over PEP'er, som de forpligtede enheders undersøgelse kan tage udgangspunkt i.

Processen for screening af PEP'er og deres relationer er en tung manuel proces for de forpligtede enheder. Det skyldes især, at de ikke har adgang til at afdække alle relationer mellem en kunde og en PEP i CPR, og at de ikke kan slå personer op på baggrund af CPR-numre i CVR. Det begrænser mulighederne for at automatisere processen og betyder bl.a., at de i stedet er tvunget til at indhente en række personoplysninger om deres kunder for at afdække alle mulige relationer til PEP'er. Kvaliteten af screeningen er samtidig betinget af troværdigheden af de informationer, kunden deler, eller af opslag i andre registre på baggrund af kundens navn og adresse.

Finanstilsynet har derfor undersøgt, under hvilke forudsætninger det er muligt at understøtte sektoren i en mere effektiv screening af PEP'er og særligt disses nærtstående familiemedlemmer og nære forretningsforbindelser (PEP-løsningen). Analysen gennemgår både en registerbaseret model og en model baseret på realtidsopslag. Begge modeller indebærer en berigelse af Finanstilsynets PEP-liste med CPR-numre på PEP'er. Løsningen indebærer også, uanset valget af model, behandling af persondata. En forudsætning er derfor, at det delte data begrænses til kun at omfatte, hvad der er nødvendigt og lovligt at indhente om en given kunde.

Finanstilsynet vurderer, at oprettelsen af en PEP-løsning vil øge kvaliteten og mindske omkostningerne ved PEP-screeningen, minimere omfanget af personoplysninger, virksomhederne skal indsamle om deres kunder, og begrænse adgangen til oplysninger om PEP'er og deres relationer til de virksomheder og personer, der er underlagt hvidvaskloven. Denne vurdering understøttes af anbefalingerne fra Finans Danmarks Task Force, hvori der indgår et konkret forslag til et sektorfælles og myndighedsdrevet PEP-register. Forsikring & Pension (F&P) har også understreget værdien af et sådant tiltag overfor Finanstilsynet.

Finanstilsynet vurderer også, at persondataforordningen og databeskyttelsesloven ikke er til hinder for etableringen af de foreslåede løsninger, men at en API-baseret løsning (Application Programming Interface)[42] er at foretrække ud fra et databeskyttelsesperspektiv. Det bør dog overvejes, om hensynet til en effektiv og sikker PEP-screening bør veje højere end det konkurrenceretlige hensyn til private aktører, der leverer tilsvarende ydelser.

[42] Et API er en softwaregrænseflade, som gør det muligt, at to stykker software kan kommunikere og udveksle oplysninger ud fra nogle klart definerede regler. Populært er et API blevet sammenlignet med en stikkontakt, hvorfra der kan hentes præcist defineret data. Gennem et API kan dele af et system eller en infrastruktur gøres tilgængelig for andre, så de kan integrere eller udvikle egne systemer ovenpå.

Der kan grundlæggende være en bekymring forbundet med et register med oplysninger om PEP'er og disses nærtstående og nære forretningsforbindelser. Den samme bekymring blev udtrykt i forbindelse med etableringen af den nuværende (mere begrænsede) PEP-liste i regi af Finanstilsynet. Det er dog vigtigt at holde sig for øje, at de omfattede virksomheder under alle omstændigheder skal indsamle disse oplysninger og kortlægge PEP'ers relationer. Finanstilsynet vurderer, at et register eller en API-løsning i regi af en offentlig myndighed – med passende begrænsninger på adgang til informationer – rent faktisk vil sikre et højere niveau af databeskyttelse end det modsatte.

Implementeringen af de skitserede løsninger vil ikke kunne løftes alene med Finanstilsynets nuværende kompetencer og ressourcer. Det vil derfor kræve ekstern hjælp i form af konsulentydelser eller ved samarbejde med andre myndigheder, hvis PEP-løsningen skal udvikles i regi af Finanstilsynet. Ud over udviklings- og etableringsomkostninger vil der også tilgå løbende omkostninger til drift af den valgte løsning og til håndtering af virksomhedernes adgang til denne.

7.1. De nuværende regler

Virksomheder skal som led i deres kundekendskabsprocedurer undersøge, om en kunde er en PEP, eller om kunden er nærtstående eller en nær samarbejdspartner til en PEP. Det fremgår af § 18 i hvidvaskloven.

Erhvervsministeren er forpligtet til at føre en offentlig liste over indenlandske PEP'er, jf. hvidvasklovens § 18, stk. 7. Listen skal indeholde navn, stilling, fødselsdato samt dato for tilføjelse eller sletning. PEP-listen bliver ført på baggrund af indberetninger fra de indberetningspligtige, bl.a. politiske partier og Folketingets Ledelsessekretariat, og er tilgængelig på Finanstilsynets hjemmeside. Listen omfatter både aktuelle PEP'er og personer, som har været registreret PEP'er de seneste 12 måneder, jf. PEP-bekendtgørelsen § 2, stk. 3.

Listen indeholder ikke oplysninger om nærtstående eller nære samarbejdspartnere[43]. Virksomhederne skal derfor som led i deres kundekendskabsprocedurer selv afdække potentielle relationer til en PEP.

Det fremgår af hvidvasklovens § 2, nr. 6, at nærtstående til PEP'er omfatter:

- *En politisk eksponeret persons ægtefælle, registrerede partner, samlever eller forældre samt børn og disses ægtefæller, registrerede partnere eller samlevere.*

Det fremgår derudover af hvidvasklovens § 2, nr. 7, at nære forretningsforbindelser til PEP'er omfatter:

a) *En fysisk person, som er reel ejer af en virksomhed eller anden form for juridisk person i fællesskab med en eller flere politisk eksponerede personer.*
b) *En fysisk person, der på anden måde end nævnt i litra a har en nær forretningsmæssig forbindelse med en eller flere politisk eksponerede personer.*

[43] Listen indeholder heller ikke udenlandske PEP'er.

c) *En fysisk person, der som den eneste er reel ejer af en virksomhed eller anden form for juridisk person, som det vides er blevet oprettet til fordel for en politisk eksponeret person.*

7.2. Virksomheders adgang til en PEP-løsning

En tilstrækkelig adgangsmekanisme skal etableres, så virksomheder og personer underlagt hvidvaskloven kan tilgå PEP-løsningen. Finanstilsynet vurderer, at der skal etableres to adgangsløsninger, for at løsningen kan bruges effektivt af alle forpligtede enheder. Begge løsninger indebærer, at der kan modtages filtreret data fra CPR og CVR om kundens eventuelle relationer til PEP'er på baggrund af kundens CPR-nummer.

Først og fremmest bør et API etableres i regi af en offentlig myndighed, som giver mulighed for, at virksomheder kan integrere deres systemer direkte med PEP-løsningen. Det vil for nogle virksomheder være en stor fordel i relation til at undgå manuelle procedurer. Det vil dog ikke være optimalt for alle forpligtede enheder, da det indebærer, at deres tekniske infrastruktur skal kunne håndtere dette. Derfor bør der også etableres en adgangsmekanisme gennem en webportal, hvorfra der kan logges ind på en hjemmeside, som giver mulighed for at søge på kunders CPR-numre.

Da løsningen skal behandle persondata, er det afgørende, at det kun er de forpligtede enheder, der har adgang til den, jf. afsnit 7.5, og at de oplysninger, der kan tilgås, minimeres til kun at omfatte data, som er relevante for PEP-screeningen af den specifikke kunde. Der skal derfor også etableres og tildeles en unik adgang til PEP-løsningen. Adgangen kan bestå af en adgangskode, krypteret nøglefil eller lignende, og den kan tildeles i takt med, at de forpligtede enheder enten opnår tilladelse underlagt hvidvaskreglerne eller hvidvaskregistreres.

Desuden kan og bør løsningen laves således, at de forpligtede enheder ikke får direkte adgang til det bagvedliggende data, men alene mulighed for at slå den enkelte kundes CPR-nummer op og modtage de nødvendige oplysninger om:

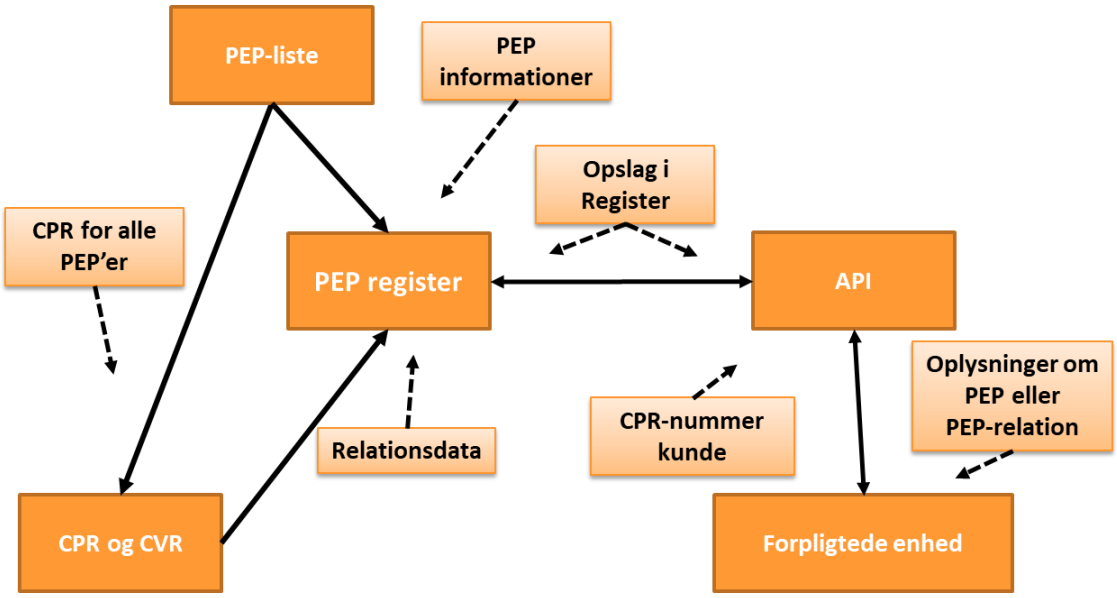
1) hvorvidt kunden er en PEP, og
2) hvorvidt kunden har en relation til en PEP, og i så fald hvilken PEP samt hvad deres relation er.

7.3. Registerbaseret PEP-løsning

En registerbaseret løsning indebærer, at der på vegne af Erhvervsministeriet etableres et register, hvor den eksisterende PEP-liste beriges med nære relationer fra CPR og nære samarbejdspartnere fra CVR.

Figur 7.1 illustrerer arkitekturen for en sådan løsning. PEP-listen beriges ved, at alle relevante relationer til alle PEP'er hentes i hhv. CPR og CVR og efterfølgende optages i et register i regi af en offentlig myndighed. Ovenpå registeret bygges et API, hvor aktører, der skal PEP-screene en kunde, på baggrund af kundens CPR-nummer vil kunne tilgå de relevante oplysninger ved enten at integrere API'en med egne systemer eller gennem direkte opslag i webportalen.

Figur 7.1 – Arkitektur for registerbaseret tilgang



Kilde: Finanstilsynet.

Berigelse med data fra CPR

Offentlige myndigheder kan gennem CPR få adgang til følgende data, som er relevante for sektorens PEP-screening efter nærtstående til PEP'er, jf. § 2, 6, i hvidvaskloven:

- Børn (inkl. CPR-nummer)
- Ægtefælle, samlever eller registreret partner (inkl. CPR-nummer)
- Forældre (inkl. CPR-nummer).

Myndigheder har dermed også mulighed for at identificere en PEP's ægtefælle, samlever eller registrerede partner, forældre samt børn og disses ægtefæller, samlevere eller registrerede partnere.

Offentlige myndigheder kan få adgang til disse data gennem enten Datafordeleren eller direkte hos CPR gennem CPR Services. Datafordeleren er drevet af Styrelsen for Dataforsyning og Effektivisering og har til formål at give private virksomheder og offentlige myndigheder adgang til offentlige grunddata gennem API'er. CPR Services består af en række tjenester, CPR-kontoret stiller til rådighed, som tilbyder opslagsmuligheder i XML-format.

Finanstilsynet vurderer, at både Datafordeleren og CPR Services kan bruges til at indhente data fra CPR til brug for identificering af nærtstående til PEP'er. Datafordeleren bygger dog på nyere teknologi og indeholder data fra både CPR og CVR. Den vil derfor være mere egnet til at danne grundlag for en PEP-løsning på langt sigt. Derudover kan datafordeleren modsat CPR Services bruges, uden at det indebærer en betaling per opslag.

Berigelse med data fra CVR

Datafordeleren vil på et tidspunkt også kunne understøtte søgninger på CPR-numre i CVR. Det er usikkert, hvornår denne funktionalitet bliver implementeret. Styrelsen for Dataforsyning og Effektivisering har tilkendegivet, at det vil ske i den nærmeste fremtid.

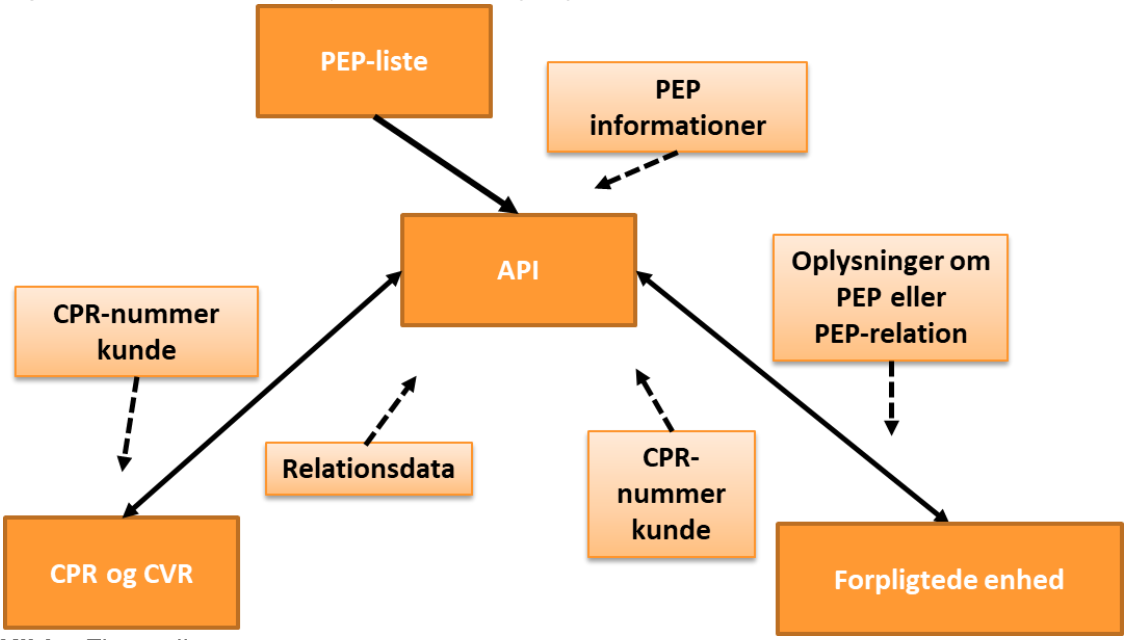
CVR tilbyder også en såkaldt system-til-system-adgang, som giver offentlige myndigheder mulighed for at foretage søgninger på CPR-numre og derigennem indhente oplysninger om en given persons engagementer i forskellige virksomheder. Med system-til-system-adgangen kan offentlige myndigheder på baggrund af et CPR-nummer dermed identificere en PEP's nære forretningsforbindelser omfattet af hvidvaskloven § 2, nr. 7, litra a.

7.4. API-løsning med realtidsopslag

Den primære fordel ved at etablere en API, som laver realtidsopslag er, at det ikke vil være nødvendigt at føre et selvstændigt register, hvor alle PEP'ers relationer lagres, med de databeskyttelsesudfordringer, som dette medfører. Samtidig vil denne løsning kunne opfylde formålet mere effektivt, da oplysninger trækkes direkte fra kilden og derfor altid vil være ajourførte. Der vil dermed ikke være behov for at opdatere et selvstændigt register løbende. Det vil udelukkende være den aktuelle PEP-liste, der løbende skal ajourføres, og som ikke altid er fuldt up-to-date. Dette er også tilfældet i dag.

Omvendt vil tilgængeligheden af denne løsning være afhængig af den samlede tekniske infrastruktur. Tekniske fejl i CVR og CPR vil dermed få større konsekvenser, og behovet for løbende og hurtig vedligeholdelse vil derfor også være større. Det vil eksempelvis være nødvendigt at tilpasse API'et, hvis dataformaterne i CVR eller CPR bliver ændret.

Figur 7.2 – Arkitektur for dynamisk API-tilgang



Kilde: Finanstilsynet.

Figur 7.2 illustrerer arkitekturen bag sådan en løsning. De forpligtede enheder, der skal foretage en PEP-screening af en kunde, vil også her kunne tilgå de relevante oplysninger gennem enten en integrering af egne systemer med API'et eller via direkte opslag i webportalen. I stedet for at lave opslag i et register vil denne løsning slå op direkte i CPR og CVR, sammenholde med PEP-listen og dermed i realtid identificere, om kunden er en PEP, eller har relationer til en PEP, og videreformidle resultatet.

Både Datafordeleren og system-til-system-adgangen til CVR tillader realtidsopslag. Berigelsen vil derfor kunne gennemføres på samme måde som ved den registerbaserede løsning, dog med udgangspunkt i kundens CPR-nummer. Den primære forskel er, at denne funktionalitet skal ligge i API'et og ikke gennemføres som en sideløbende opdatering af registeret separat fra API'et. Finanstilsynet har diskuteret kompleksiteten ved en sådan løsning med F&P, der har gode erfaringer med etableringen af denne type tekniske løsninger. F&P vurderede, at det hverken er specielt kompliceret eller omkostningsfuldt at implementere en sådan løsning.

7.5. Juridiske overvejelser

Hvidvasklovens regler om offentliggørelse af PEP'er, jf. § 18, stk. 6, omfatter ikke disses relationer. Derfor er PEP-løsningen, og særligt den registerbaserede løsning med berigelse af PEP-listen, forbundet med en række juridiske overvejelser. En mulighed er ændringer i Finanstilsynets hjemmel til at føre og drive en PEP-liste. Samtidig skal det sikres, at den yderligere behandling af persondata, der eksempelvis er ved at føre et register, er nødvendig i forhold til formålet om effektiv foranstaltning mod hvidvask og terrorfinansiering.

Begge modeller vil fjerne behovet for at føre en offentlig liste med PEP'er. Finanstilsynet vurderer derfor, at PEP-løsningen, uanset valg af model, muliggør en forbedret beskyttelse af PEP'ers persondata end den nuværende løsning.

Nødvendige ændringer i hvidvaskloven og PEP-bekendtgørelsen

PEP'er registreres i dag med navn, stilling, fødselsdato og dato for tilføjelse eller sletning, jf. hvidvasklovens § 18, stk. 7. Begge modeller kræver, at PEP-listen udvides til at indeholde CPR-numre. Det skyldes, at opslag på navn i Datafordeleren (eller direkte i CPR og CVR) ikke vil kunne føre til definitive svar om tilstedeværelsen af relevante relationer, hvis ikke der benyttes en unik identifikationsmarkør. Flere personer kan eksempelvis godt dele både navn og fødselsdagsdato.

Dette vil kræve en ændring i både hvidvasklovens § 18, stk. 7, og i PEP-bekendtgørelsen, så CPR-nummer bliver inkluderet i de oplysninger, de myndigheder og organisationer mv., der i henhold til PEP-bekendtgørelsen skal indberette til Finanstilsynet vedrørende PEP'er. Ingen af modellerne vil dog give brugerne adgang til PEP'ernes CPR-numre. De vil udelukkende blive brugt til at kortlægge potentielle sammenfald eller relationer til de kunder, som brugerne gennemfører PEP-screening på. Derudover bør der også foretages enkelte mindre ændringer af PEP-bekendtgørelsens §§ 2, stk. 1-3, så den bliver tilpasset den valgte model.

Persondataforordningen og dataminimering

En teknisk løsning, der igennem CPR, CVR og Finanstilsynets PEP-liste giver adgang til PEP'ers navne og PEP'ers relevante relationer til kunder, vil indebære behandling af almindelige personoplysninger, jf. afsnit 9.1.

Formålet med behandlingen af personoplysninger er at understøtte de forpligtede enheder med at gennemføre PEP-screeninger. Med den foreslåede PEP-løsning vil behandlingen ske gennem en mekanisme, som kan hjælpe virksomhederne med at identificere PEP'er og deres nærtstående og nære samarbejdspartnere.

Behandling af personoplysninger på grundlag af reglerne i hvidvaskdirektiverne anses for at være i samfundets interesse og vil derfor udgøre en lovlig behandlingshjemmel, jf. afsnit 2. Det betyder, at der vil kunne gives hjemmel til, at de forpligtede enheder i forbindelse med deres kundekendskabsprocedurer kan få adgang til konkrete registre, der er egnet til at opfylde formålet. I vurderingen af, hvilke af de to foreslåede modeller der er mest proportionel (egnet, nødvendig og forholdsmæssig), er det derfor afgørende at skelne mellem, hvordan modellerne hver især behandler persondata.

Behandlingen af PEP'ers almindelige personoplysninger sker allerede i forbindelse med, at Finanstilsynet driver og offentliggør en PEP-liste. De foreslåede løsninger vil dog indebære, at også PEP'ers relationer til en given kunde fremover skal behandles. Vælges en register-baseret løsning, vil samtlige relevante relationer fremover skulle registreres i et særskilt PEP-register. Det betyder, at den nuværende registrerede personkreds vil blive større, jf. afsnit 7.1.

I henhold til art. 5 i persondataforordningen er det væsentligt, at den valgte løsning begrænser behandlingen af oplysninger og kun behandler de nødvendige informationer (dataminimering).

I den forbindelse har den foreslåede API-løsning med realtidsopslag den fordel, at den ikke vil kræve udvidelse af den registrerede personkreds. API'en vil kunne identificere den relevante personkreds for hver enkelt PEP gennem realtidsopslag i de relevante registre og vil derfor ikke være betinget af en udvidelse af den registrerede personkreds.

Derudover vil begge løsninger bl.a. kunne foretage følgende beskyttelsesforanstaltninger:

- Den valgte løsning angiver kun, om CPR-nummeret har en relation til en PEP, og i givet fald hvilken PEP kunden har relationen til, og hvori relationen består. Her er det vigtigt, at der ikke skelnes mellem samlever, ægtefælle eller registreret partner, da en sådan skelnen medfører, at der behandles følsomme personoplysninger, hvilket ikke er nødvendigt for at opfylde formålet.

- PEP-listen vil ikke længere være offentlig tilgængelig, men den vil gennem datadelingsmekanismen kunne tilgås af de forpligtede enheder.

- Alle søgninger i systemet logges. Omfanget og de juridiske konsekvenser af en sådan logning bør i den forbindelse vurderes.

Begge løsninger opfylder kravene om egnethed, men den API-baserede løsning opfylder i højere grad kravet om nødvendighed, da den ikke kræver en udvidelse af den registrerede personkreds.

Finanstilsynet vurderer, at PEP-løsningen vil være egnet til at mindske omkostningerne ved PEP-screeningen på tværs af sektoren uanset valget af model. Ressourcerne vil kunne bruges mere effektivt, hvilket kan bidrage til, at de forpligtede enheder bedre kan overholde hvidvaskloven. Desuden vil kvaliteten af PEP-screeningen sandsynligvis også forbedres.

Konkurrenceretlige overvejelser

CPR-loven sætter rammerne for private virksomheders adgang til CPR. Selvom pensionskasser, forsikringsselskaber og pengeinstitutter har en udvidet adgang til oplysninger i CPR, som udover at give adgang til de oplysninger, som er listet i CPR-loven § 38, stk. 2, også giver adgang til civilstand og civilstandsdato, så giver adgangen ikke virksomheder fyldestgørende indblik i kunders nærtstående relationer efter hvidvasklovens § 2, nr. 6.

Hvad angår data fra CVR til screening af nære forretningsforbindelser efter § 2, nr. 7, litra a, i hvidvaskloven, så kan alle danske virksomheder tilgå grunddata om danske virksomheder, herunder se oplysninger om ejerforhold gennem Erhvervsstyrelsens webservice (virk.dk og cvr.dk) eller gennem den åbne API (cvrapi.dk), som er frit tilgængelig. Den offentlige adgang til CVR giver dog ikke mulighed for at foretage søgninger på CPR-nummer.

Finanstilsynet vurderer derfor, at offentlige myndigheder grundet deres særlige adgang til CPR og CVR kan etablere en mere effektiv PEP-løsning end private virksomheder, i forhold til personkredsen i hvidvasklovens §§ 2, nr. 6 og nr. 7, litra a.

Det kan dog ikke udelukkes, at en sådan løsning ville fjerne hele eller dele af forretningsgrundlaget for private virksomheder, som har muligheden for at tilbyde eller allerede i dag tilbyder lignende løsninger. Det gælder særligt i forhold til personkredsen i hvidvasklovens § 2, nr. 7, litra a, da mange af de nødvendige oplysninger kan tilgås gennem CVR. Dette betyder, at der, hvis en af de foreslåede løsninger etableres, kan opstå en situation, hvor den konkurrerer med løsninger fra private aktører.

De foreslåede løsninger vil ikke kunne benyttes til screening af udenlandske PEP'er og personkredsen i hvidvasklovens §§ 2, nr. 7, litra b og c. Det skyldes, at disse screeninger ikke kan foretages alene på baggrund af oplysninger fra offentlige registre. Der vil derfor fremover stadig være rum til private PEP-løsninger, som kan supplere den offentlige løsning. Det bør i den forbindelse også overvejes, om og i hvilket omfang private løsninger skal have adgang til PEP-løsningen. Disse overvejelser bør inddrage reglerne om bistand fra tredjemand, jf. kapital 4 i hvidvaskloven.

8. Generaliserede scenarier i transaktionsovervågningen

Finanstilsynet indstiller, at det besluttes om samarbejdet mellem myndigheder og pengeinstitutter bør udbygges med det formål at udvikle typologier for relevante scenarier (generaliserede scenarier), der bør afdækkes i transaktionsovervågningen. Et sådant arbejde vil være oplagt at placere i regi af en FEHT, hvis eller når en sådan etableres.

Manglende indsigt i kriminel adfærd begrænser pengeinstitutternes mulighed for effektivt at opdage undringsværdige forhold (mistænkelig adfærd). For det første er kriminelle aktører dygtige til at skjule deres aktivitet, bl.a. ved hele tiden at udvikle deres metoder. Eksempelvis var momskarruseller tidligere særligt forbundet med køb og salg af hardware. I dag bruges andre produkter også i denne type svindel – eksempelvis frossen kylling. For det andet er det ikke blandt pengeinstitutternes kernekompetencer at forstå kriminel adfærd. Det er omvendt kernekompetencer hos en række myndigheder, særligt Hvidvasksekretariatet og andre politimyndigheder. I og med at pengeinstitutterne pålægges et stort ansvar i forhold til at identificere mistænkelig adfærd, er det derfor helt afgørende for en effektiv indsats, at den viden, der er i myndighederne, så vidt muligt også deles med pengeinstitutterne for at understøtte dem i deres arbejde.

Der eksisterer allerede i dag en række initiativer, der bl.a. har til formål at løfte denne opgave. Etableringen af HVF+, hvor Finanstilsynet er formand, var fra 2018 en del af regeringens strategi til bekæmpelse af hvidvask og terrorfinansiering. Formålet med dette forum er at sikre, at myndighederne og sektoren udveksler relevant information om udviklingen på området, og ikke mindst at understøtte samarbejdet på området.

Hvidvasksekretariatet deler desuden både kvartals- og temarapporter med pengeinstitutterne, der berører udviklingen i modtagne underretninger og særligt relevante fokusområder. Kvartalsrapporterne indeholder bl.a. oplysninger om tendenser i underretningerne, samt mere overordnede eksempler på områder, som de underretningspligtige skal have særligt eller yderligere fokus på. Temarapporterne indeholder mere dybdegående analyser af specifikke trends og risici, som de underretningspligtige bør være opmærksomme på. Hvidvasksekretariatet er desuden begyndt at konkretisere information om kriminel adfærd og give konkrete eksempler på undringsværdige forhold, der kan være relevante at inddrage i transaktionsovervågningen, i løbende orienteringer til de underretningspligtige.

Anbefalingerne fra Finans Danmarks Hvidvask Task Force fremhævede et behov for at kunne gå mere i dybden med udviklingstendenserne. Motivet var i højere grad at nyttiggøre de informationer, som myndighederne har, og derigennem effektivisere pengeinstitutternes arbejde. Task Forcen foreslog derfor bl.a. etablering af et såkaldt Bankforum, som eksempelvis kan arbejde mere indgående med underretningerne fra pengeinstitutterne til Hvidvasksekretariatet og derigennem sikre en vis standardisering og kvalificering af underretningerne. Det skulle bl.a. også skabe bedre grundlag for Hvidvasksekretariatets analysearbejde. Samtidig vil et sådant forum kunne understøtte en bedre uddannelse af pengeinstitutterne.

Task Forcen foreslog desuden, at man med inspiration fra England og det pågående samarbejde mellem myndighederne og den finansielle sektor i en *Joint Money Laundering Intelligence Taskforce (JMLIT)* etablerer en *Fælles Efterretningsenhed for Hvidvask og Terrorfi-*

nansiering (FEHT) i Danmark[44]. Formålet med oprettelse af FEHT er at muliggøre, at personfølsomme oplysninger om konkrete sager kan deles med henblik på at sikre en effektiv forebyggelse og opklaring af sager om alvorlig kriminalitet, særligt hvidvask.

Finanstilsynet vurderer, at en måde at understøtte pengeinstitutternes arbejde på er, at understøtte et øget samarbejde mellem myndigheder og pengeinstitutter fokuseret på løbende at konkretisere, hvilke scenarier pengeinstitutterne skal være opmærksomme på i deres transaktionsovervågning. Potentialet understøttes blandt andet af Finanstilsynets undersøgelse af regeloverholdensen for transaktionsovervågningen, jf. afsnit 10.4. Samtidig indikerer resultater i regi af Nationalbankens POC[45], der bl.a. gør brug af tre konkrete scenarier opstillet i samarbejde med Hvidvasksekretariatet, at denne form for samarbejde kan bidrage til at effektivisere transaktionsovervågningen, fordi:

1. mistænkelig adfærd kan identificeres langt tidligere, end det sker i dag. Helt konkret ses det, at brugen af de opstillede scenarier medfører, at et faktisk rejst risikoflag i 84 pct. af tilfældene kunne være rejst tidligere.

2. mistænkelig adfærd, der i dag ikke opdages, opdages i højere grad ved brug af de opstillede scenarier. Helt konkret blev 1.482 tilfælde af "nye" mistænkelige transaktioner flaget.

Finanstilsynet vurderer på den baggrund, at der med fordel kan igangsættes et arbejde med det formål at afklare, under hvilket betingelser denne form for samarbejde kan understøttes. Et forum som FEHT vurderes umiddelbart at kunne bære denne opgave bedst, da etableringen af et fortroligt rum vil medvirke til at underbygge den tillid, der er nødvendig for at drøfte og dele relevante observationer på tværs af pengeinstitutterne og myndighederne. Det er som udgangspunkt ikke nødvendigt at dele personhenførbare oplysninger for at udvikle generaliserede scenarier for, hvornår der bør rejses et risikoflag for en given kunde eller transaktion. Øvelsen kræver dog gensidig tillid, idet alle vil skulle bidrage med konkrete erfaringer fra det daglige arbejde.

Udmeldinger fra JMLIT understøtter også, at et udvidet samarbejde mellem myndigheder og de forpligtede enheder kan medvirke til at øge effektiviteten af indsatsen[46]:

> *"Partnerships have contributed to: improvements in the quantity and quality of reports of suspicion related to particular economic crime threats; and to the timeliness and relevance of such reporting to active investigations or live incidents."*

Det skal dog understreges, at generaliserede scenarier på intet tidspunkt bør betragtes som en best practise for transaktionsovervågning, men nærmere som et bidrag til, hvordan pengeinstitutterne indretter deres transaktionsovervågning bedst muligt, jf. afsnit 10.2. Samtidig er der en risiko for, at kriminelle aktører bliver vidende om, hvilke scenarier der bruges i

[44] FIDA foreslår, at en sådan enhed skal placeres i regi af det offentlige og have deltagere fra både sektoren og myndighederne. Deltagerne fra myndighederne kunne være SØIK, Hvidvasksekretariatet, Politiet, Politiets Efterretningstjeneste, Forsvarets Efterretningstjenesten, Skattestyrelsen mv.
[45] Nationalbanken har i et Proof Of Concept (POC) i løbet af første halvår 2020 undersøgt, om oplysninger fra pengeinstitutternes transaktionsdata sammenholdt med forskellige myndighedsoplysninger vil kunne understøtte en mere effektiv indsats mod finansiel kriminalitet.
[46] FFIS (Nick J. Maxwell) – Expanding the Capability of Financial Information-Sharing Partnerships, Marts 2019

transaktionsovervågningen, og derfor finder på nye måder, hvorpå de kan undgå at blive udtaget til kontrol. Fordelene ved, at pengeinstitutterne i højere grad bliver opmærksomme på konkret adfærd udvist af kriminelle, vil dog alt andet lige begrænse de kriminelles muligheder.

8.1. Juridiske overvejelser

De juridiske overvejelser med hensyn til øget vidensdeling mellem myndigheder og pengeinstitutter afhænger navnlig af den valgte model. Ovenstående forslag vedrører alene bedre fælles forståelse af mistænkelig (kriminel) adfærd, og udveksling af personhenførbare oplysninger er ikke en forudsætning.

Samarbejde om udviklingen af generelle scenarier

Oplysninger om risikoindikatorer, risikoscenarier og mere generelle oplysninger om, hvilke risikofaktorer der bør overvåges af pengeinstitutter med henblik på at bekæmpe hvidvask og terrorfinansiering, vil kunne udveksles både mellem pengeinstitutterne og med myndighederne uden juridiske udfordringer. Der er dermed intet juridisk til hinder for at oprette et forum, hvor både den private sektor og de kompetente myndigheder er repræsenteret og kan udveksle oplysninger i summarisk eller abstrakt form. Det har i den forbindelse ingen betydning, om det oprettes som en underarbejdsgruppe til et eksisterende forum eller tilknyttes en nyoprettet enhed. Effektiviteten af et sådant forum vil formentlig stige i takt med voksende tillid og forståelse parterne imellem. Finanstilsynet finder det derfor naturligt og mest hensigtsmæssigt at oprette forummet i tilknytning til eksempelvis det foreslåede FEHT.

Udvekslingen af oplysninger bør ikke få en karakter, som vil kunne afsløre myndighedernes efterforskningsmetoder eller lignende. Der vil i den forbindelse være tale om en konkret vurdering og en hensynsafvejning, som den enkelte myndighed bør foretage, inden den deler oplysninger.

Oprettelse af FEHT eller lignende

Oprettelsen af en enhed eller et forum, som kan behandle oplysninger om konkrete enkeltpersoner, herunder eksempelvis oplysninger om underretninger, mistanker om kriminalitet eller lignende, vil navnligt stille krav til behandlingshjemmel, tavshedspligt og retsvirkning for kunderne[47].

Den politiske aftale af 19. september 2018 om yderligere initiativer til styrkelse af indsatsen mod hvidvask og terrorfinansiering indeholder, under aftalens pkt. 2 om samarbejde med private aktører, et initiativ om oprettelse af en sådan enhed:

> *"De retshåndhævende myndigheder skal vurdere, om der er behov for oprettelse af en stående arbejdsgruppe, hvor konkrete efterforskningssager bl.a. kan drøftes med udvalgte private aktører, samt hvorvidt dette kan indeholdes inden for gældende lovgivningsramme."*

Initiativet behandles i Justitsministeriets søjle, der vil vurdere de juridiske aspekter. Selve oprettelsen af et sådant forum med henblik på at dele personhenførbare oplysninger beskrives derfor ikke yderligere her.

[47] https://www.regeringen.dk/aktuelt/publikationer-og-aftaletekster/hvidvaskaftale/

9. Øget adgang til myndighedernes data

Finanstilsynet indstiller, at det besluttes, om der skal igangsættes et arbejde fokuseret på muligheden for, at pengeinstitutter får adgang til sammenstillede virksomhedsdata eller vurderinger i regi af Erhvervsstyrelsen. Beslutningen bør suppleres med overvejelser om, hvorvidt et sådant arbejde også bør berøre muligheder for en bredere adgang til andre myndigheders data.

En generel udfordring i dag er, at en manglende tilgængelighed af verificerede kundeinformationer kan begrænse og besværliggøre pengeinstitutternes mulighed for at opnå et tilstrækkeligt kundekendskab. Det skyldes delvist, at kundekendskabet er fragmenteret på tværs af sektoren, jf. afsnit 10. Det kan også skyldes, at oplysninger i offentlige registre ikke er tilgængelige i tilstrækkelig grad. Uanset årsag, kan begrænset adgang til verificerede kundeinformationer have konsekvenser for effektiviteten af pengeinstitutternes indsats mod hvidvask og terrorfinansiering.

Anbefalingerne fra Finans Danmarks Hvidvask Task Force understøtter også denne vurdering. Task Forcen nævner bl.a. en række myndigheder med viden og data, der kunne skabe værdi for pengeinstitutterne i bekæmpelsen af hvidvask og terrorfinansiering.

Finanstilsynets analyse tager udgangspunkt i værdien ved øget adgang til sammenstillede data i regi af Erhvervsstyrelsen. Det skyldes bl.a., at en positiv effekt af at inddrage denne data i transaktionsovervågningen allerede er delvist dokumenteret for pengeinstitutterne i regi af Nationalbankens POC[48].

I dag offentliggør Erhvervsstyrelsen en række virksomhedsdata i CVR. Erhvervsstyrelsen har etableret et betydeligt mere avanceret internt register over virksomhederne, herunder bl.a. over relationer virksomhederne imellem. Registeret kaldes grafdatabasen. Kort fortalt skaber grafdatabasen et meget nuanceret overblik over alle virksomheder i Danmark på baggrund af Erhvervsstyrelsens samlede datagrundlag. Grafdatabasen bygger på registerdata[49], herunder data om relationer såsom virksomhedernes tilknyttede fysiske personer og de indbyrdes relationer mellem personerne samt forskellige beregninger på registerdata (metadata). Mere nuancerede metadata indgår desuden, eksempelvis vurderinger gennemført ved brug af maskinlæringsmodeller på baggrund af register- og anden indberettet data (årsrapporter mv.). At få adgang til grafdatabasen er en oplagt måde, hvorpå pengeinstitutterne kan få et bedre kendskab til deres virksomhedskunder.

Resultaterne af Nationalbankens POC indikerer, at pengeinstitutter kan forbedre deres processer for transaktionsovervågning, hvis datagrundlaget beriges med bl.a. data fra grafdatabasen. Resultaterne er baseret på en maskinlæringsmodel (algoritme), og sammenlignings-grundlaget er den eksisterende proces for transaktionsovervågning. Ved at træne algoritmen på det berigede datasæt[50] viste det sig, at der blev rejst betydeligt flere risikoflag, end hvad

[48] Nationalbankens POC introduceres kort i en fodnote i afsnit 8.
[49] Indebærer også registerdata fra andre myndigheder, grundet Erhvervsstyrelsen relativt brede hjemmel til indsamling af data, jf. lov om Erhvervsstyrelsens behandling af data af den 8. maj 2018.
[50] Primært beriget med data i Erhvervsstyrelsen grafdatabase.

den eksisterende proces lykkedes med[51]. Algoritmen var desuden i stand til at bortsortere en betydelig mængde sager, der under den eksisterende proces fejlagtigt blev videregivet til manuel undersøgelse (såkaldte false-positives). Berigelsen af data med grafdatabasen viste sig at være afgørende for begge resultater, bl.a. ved at være den direkte årsag til 35 pct. af de bortsorterede false-positives.

Nationalbankens resultater forudsætter maskinlæringsteknikker til at optimere processerne for transaktionsovervågning. Det skaber en usikkerhed om, hvorvidt man vil se en lignende effekt af, at pengeinstitutter får adgang til grafdatabasen under eksisterende processer, jf. afsnit 10.1. Hvad angår infrastruktur, vil der sandsynligvis være nogle udfordringer ved at give alle pengeinstitutter adgang til grafdatabasen. Der er tale om en meget stort datasæt, som løbende vokser, kombineret med en IT-infrastruktur, der ikke nødvendigvis er gearet til at dele så store mængder data i realtid.

Et samarbejde med Erhvervsstyrelsen kan alternativt afdække muligheden for at udvikle maskinlæringsmodeller, der kan forestå konkrete vurderinger af risikoen (sandsynligheden) for, at en given virksomhed bruges til hvidvask eller terrorfinansiering. Resultaterne af disse modeller kunne deles med pengeinstitutterne, eksempelvis i form af en sammenlagt risikoscore suppleret med en beskrivelse af, hvilke forhold der driver risikoscoren. Det vil alt andet lige være mindre belastende for den eksisterende IT-infrastruktur end delingen af den fulde grafdatabase. Samtidig har Erhvervsstyrelsen både kompetencerne og den nødvendige erfaring med at bruge maskinlæring. Finanstilsynet er eksempelvis blevet præsenteret for en model baseret på samme teknik, der angiver sandsynligheden for, at en given virksomhed vil begå skatte- og momssvig. SKAT bruger i dag modellen, som har medvirket til, at SKAT mere præcist kan udvælge de rette virksomheder til manuelle undersøgelser.

Finanstilsynet vurderer, at pengeinstitutterne bør kunne forbedre deres kundekendskabsprocedurer, hvis deres datagrundlag beriges med data fra eller vurderinger foretaget på baggrund af grafdatabasen. Et næste skridt kan derfor være, at Finanstilsynet i samarbejde med Erhvervsstyrelsen vurderer mulighederne for enten en direkte adgang til grafdatabasen eller udarbejdelsen af de omtalte maskinlæringsmodeller, og i hvilket omfang data kan deles og ønskes delt. På den baggrund kan det afklares, om der vil være værdi i at gå videre med et sådant tiltag, og hvilke andre aktører der i så fald bør involveres.

Andre myndighederes data kan også give værdi

En bredere adgang til andre myndigheders data vil også kunne give værdi. Det gælder eksempelvis data fra Skattestyrelsen, Udbetaling Danmark, en udvidet adgang til CPR, adgang til pas- og kørekortsregistre samt udlændingestyrelsens registre[52]. Sådanne datakilder kan bruges i forskelligt omfang. Adgangen til disse er i dag også i nogle tilfælde betinget af virksomhedstypen[53]. Eksempelvis har Finans og Leasing forelagt Finanstilsynet et ønske om at kunne verificere udenlandske låneansøgeres oprindelsesland og opholdsgrundlag i Danmark via adgang til udlændingestyrelsens registre. Et andet ønske er at kunne sammenholde pas eller kørekort med Rigspolitiets registre for at se, om de er meldt stjålet eller er udløbet.

[51] Bemærk, at dette ikke nødvendigvis forudsætter, at transaktionsovervågningen bliver bedre, jf. afsnit 3. Det kan dog sagtens være tilfældet.
[52] Bl.a. udtrykt gennem Hvidvask Task Forcens anbefalinger samt dialog med Finans og Leasing.
[53] Finans og Leasing har eksempelvis udtrykt, at leasingselskaber ikke samme adgang til E-skat-data i regi af Skattestyrelsen, som billånsudbydere og pengeinstitutter generelt har gennem fuldmagt fra kunden.

9.1. Juridiske overvejelser

Udgangspunktet for Erhvervsstyrelsens grafdatabase er data fra forskellige offentlige registre, som efterfølgende sammenstilles med henblik på beregning af bl.a. risikoscorer (vurderinger) for at prioritere tilsyn mv. Databasen beriges løbende med resultaterne af de beregnede vurderinger. De sammenstillede data vedrører som hovedregel juridiske personer og i mindre grad fysiske personer. Data indeholder dog i nogen grad oplysninger om fysiske personer, eksempelvis direktører, såvel som enkeltmandsvirksomheder, der er omfattet af databeskyttelsesreglerne.

Udveksling af sammenstillet objektiv data fra Erhvervsstyrelsens grafdatabase

Udveksling af sammenstillede data i grafdatabasen mellem Erhvervsstyrelsen og pengeinstitutterne til brug for pengeinstitutternes kundekendskabsprocedurer vil ikke være omfattet af de samme juridiske udfordringer, som udveksling af de vurderinger, der efterfølgende foretages af systemet.

I det omfang, der er tale om oplysninger, som virksomhederne efter lovgivningen er forpligtet til at indberette til Erhvervsstyrelsen, vurderer Finanstilsynet, at pengeinstitutterne vil kunne få adgang til disse, hvis virksomhederne gøres bekendt med, at Erhvervsstyrelsen vil kunne videregive oplysningerne til pengeinstitutterne i forbindelse med gennemførelsen af kundekendskabsprocedurer.

Det kræver dog, at pengeinstitutterne har en behandlingshjemmel efter persondataforordningen. Pengeinstitutterne er i medfør af hvidvasklovens kapitel 3 forpligtet til at kende deres kunder, herunder til at indsamle og opbevare oplysninger, der kan danne grundlag for at vurdere kundernes risikoprofil mv. Pengeinstitutterne har dermed allerede nu hjemmel til at indhente og behandle oplysninger om deres kunder.

Det skal i forlængelse heraf vurderes, om Erhvervsstyrelsens formål med at indsamle de pågældende oplysninger også kan rumme, at styrelsen videregiver oplysningerne til pengeinstitutterne til brug for deres forebyggende indsats mod hvidvask og terrorfinansiering.

Lovgrundlaget for Erhvervsstyrelsens indsamling og behandling af data er ikke gennemgået nærmere i denne analyse. Der vil dog være tale om objektive data, som kan understøtte den samfundsvigtige rolle, som hvidvaskloven pålægger pengeinstitutterne. Desuden vil kunderne være bekendt med, hvilke oplysninger Erhvervsstyrelsen kan videregive, ligesom der er tale om data vedrørende faktiske forhold.

Finanstilsynet vurderer den baggrund, at det vil være muligt, eventuelt med en justerende lovændring til Erhvervsstyrelsens lov om behandling af data, at skabe en hjemmel til videregivelse af oplysninger til brug for pengeinstitutternes løbende overholdelse af hvidvasklovens regler.

Udveksling af vurderinger foretaget af Erhvervsstyrelsen

Finanstilsynet vurderer samtidig, at det vil være forbundet med juridiske udfordringer at give pengeinstitutterne adgang til sammenstillet data i form af vurderinger og analyser foretaget i Erhvervsstyrelsen grafdatabase.

En model, hvor pengeinstitutternes kundekendskabsprocedurer tilføres vurderinger foretaget i Erhvervsstyrelsens database, eksempelvis om en forventet hvidvaskrisiko for virksomheder, vurderes navnlig at indebære overvejelser om, hvad retsmidlerne overfor en sådan vurdering er. Det gælder eksempelvis, om kunder kan påklage vurderingen eller indbringe spørgsmålet for retten.

Indgår en sådan vurdering i pengeinstitutternes kundekendskabsprocedurer, bør den enkelte kunde have adgang til at blive bekendt med oplysningerne. Denne adgang vil navnlig skulle tjene til at sikre, at Erhvervsstyrelsens vurdering er baseret på korrekte faktiske oplysninger, så styrelsen ikke vurderer på et forkert eller ufuldstændigt grundlag. Det bør overvejes, om og hvordan kunderne kan få adgang til oplysninger og elementer i vurderingen, eksempelvis de oplysninger, som indgår i Erhvervsstyrelsens grafdatabase og beregningsmetoderne (algoritmer mv.). Det vil være forbundet med retssikkerhedsmæssige betænkeligheder, hvis kunderne ikke kan få kendskab til Erhvervsstyrelsens vurdering og dermed ikke har lejlighed til at kende grundlaget, hvorpå de bliver vurderet af pengeinstitutterne, eller mulighed for at gå i rette med vurdering eller lignende.

Udvekslingen af de beskrevne vurderinger giver også anledning til overvejelser om, hvordan data verificeres, hvem der er ansvarlig for vurderingerne, og hvordan de efterfølgende bliver brugt. Der vil desuden være spørgsmål om, hvorvidt kunderne har ret til at få vurderingerne ændret eller slettet.

Det bør i den forbindelse overvejes, om kunderne vil kunne påklage Erhvervsstyrelsens risikovurdering til en anden myndighed, eller om Erhvervsstyrelsen vil kunne indbringes for domstolene, eksempelvis i forbindelse med spørgsmål om erstatningsansvar ved økonomisk tab opstået på baggrund af pengeinstitutternes brug af vurderingerne fra grafdatabasen. En løsning, hvor Erhvervsstyrelsen deler sine vurderinger, eksempelvis i form af indikationer af risiko ved hjælp af kategorisering i farver, med pengeinstitutterne, vil kræve nærmere undersøgelser af det ønskede setup, algoritmernes funktioner og den forventede merværdi. På samme måde vil der skulle tages stilling til ovenstående juridiske udfordringer. Det er ikke muligt på nuværende tidspunkt at afgøre, om det reelt vil være muligt at dele vurderinger foretaget i offentligt regi.

Adgang til registerdata vedrørende fysiske personer

Sektoren har som nævnt ovenfor udtrykt ønske om adgang til en række registre, som vil kunne styrke og effektivisere deres kundekendskab. Der er i den forbindelse peget på registre, som i stor grad indeholder oplysninger om fysiske personer, herunder registre i regi af Skattestyrelsen og Rigspolitiet.

Adgang til registre med oplysninger om fysiske personer vil kræve, at der bliver taget højde for kravene i databeskyttelsesforordningen. Det skyldes, at brug af adgangen vil være en behandling af personoplysninger.

En personoplysning er enhver form for information, der kan henføres til en bestemt person. Det gælder også, selvom informationen kun i kombination med andre oplysninger kan bruges til at identificere en person.

Databeskyttelsesforordningen opdeler personoplysninger i tre typer:

- Almindelige oplysninger, eksempelvis navn, adresse og økonomiske forhold
- Følsomme oplysninger, eksempelvis race, religion og politisk overbevisning

- Oplysninger om strafbare forhold, eksempelvis strafferetlige afgørelser og rettighedsfrakendelse.

Opdelingen knytter sig til forskellige betingelser og procedurer for behandling af personoplysninger afhængig af oplysningernes følsomhed.

Der vil dermed ved vurderingen af, hvilke registre der kan gives hel eller delvis adgang til, indledningsvist skulle foretages en kategorisering af de data, der er indeholdt i det enkelte register. Herefter vil behovet for samtykke og kravene om lovlighed, rimelighed og gennemsigtighed skulle vurderes. Indsamlede data må desuden som udgangspunkt kun bruges til det konkrete formål, som de er indsamlet til (formålsbegrænsningen).

Det vil dermed altid kræve et retsgrundlag for at de forpligtede enheder eller offentlige myndigheder kan behandle personoplysninger, eksempelvis som led i kundekendskabsprocedurer.

Behandling af personoplysninger på grundlag af reglerne i hvidvaskdirektiverne anses som værende i samfundets interesse, og udgør derfor en lovlig behandlingshjemmel efter persondataforordningen, jf. afsnit 2. Det betyder, at der vil kunne gives hjemmel til, at de forpligtede enheder i forbindelse med deres kundekendskabsprocedurer, som har til formål at forebygge hvidvask og terrorfinansiering, kan få adgang til konkrete registre, der er egnet til at opfylde formålet. Det vil i den forbindelse være afgørende, hvilke type data der er tale om, og de offentlige myndigheder vil skulle vurdere proportionaliteten i hensyn hertil (egnethed, nødvendighed og forholdsmæssighed).

Som ovenfor anført indeholder databeskyttelsesreglerne tre kategorier af personoplysninger. Almindelige, som har de laveste beskyttelseskrav, følsomme, som har skærpede krav til behandling, og endeligt oplysninger om strafbare forhold, som er omfattet af særlige regler.

Det betyder, at det er muligt at give adgang til oplysninger om bopæl i CPR, da disse er kategoriseret som almindelige oplysninger. Omvendt vil der formentlig ikke kunne gives adgang til det Centrale Kriminalregisters oplysninger om strafbare forhold[54].

De offentlige myndigheder vil derfor skulle vurdere proportionalitet i forhold til de enkelte registre. Uanset hvilke registre myndighederne giver adgang til, skal de sikre, at der er en klar hjemmel til udveksling mellem offentlige myndigheder og de forpligtede enheder. Oplysningerne i nogle registre vil formentlig kunne udveksles under de gældende regler i hvidvaskloven, mens andre registre vil kræve nye lovhjemler, hvis data skal deles.

[54] Det Centrale Kriminalregister (Kriminalregisteret) indeholder oplysninger om de lovovertrædelser, der bl.a. bliver brugt til at udarbejde straffeattester.

10. Deling af risikoflag rejst i transaktionsovervågningen

Finanstilsynet indstiller, at det besluttes, om der skal igangsættes arbejde fokuseret på at muliggøre delingen af risikoflag mellem pengeinstitutter. Som led i beslutningen bør der tages stilling til, om der skal arbejdes for, at pengeinstitutterne indbyrdes skal kunne dele risikoflag, og hermed for en ændring af tavshedsbestemmelserne i hvidvaskdirektivet, eller om det videre arbejde skal fokuseres på, at delingen udelukkende sker gennem en offentlig myndighed.

Muligheden for at foretage en retvisende risikoklassificering, når et pengeinstitut etablerer et kundeforhold, kan begrænses af, at pengeinstitutter som udgangspunkt ikke må dele kundeoplysninger. Eksempelvis kan en kunde, som et pengeinstitut har afviklet kundeforholdet med grundet en mistanke om hvidvask eller terrorfinansiering, i dag uden større problemer etablere et kundeforhold i et andet pengeinstitut. Dette pengeinstitut vil ikke være bekendt med de bekymringer, som det foregående pengeinstitut måtte have, og det er ikke muligt for pengeinstitutterne at advare hinanden.

Finanstilsynet vurderer, at muligheden for at dele risikoflag rejst som led i transaktionsovervågningen i sektoren kan bidrage til at imødegå denne problemstilling. Det skyldes helt grundlæggende, at ansvaret for effektive kundekendskabsprocedurer fortsat vil ligge hos det enkelte pengeinstitut, samtidig med at kundekendskabsprocedurerne, særligt risikoklassificeringen og den efterfølgende overvågning af kundeforhold, kan gennemføres på et mere oplyst grundlag:

- Kvaliteten af pengeinstitutternes kundekendskabsprocedurer forventes at kunne hæves på brancheniveau, hvis kendskabet til mistænkelige kunder i højere grad deles på tværs af branchen.

- Pengeinstitutter kan hurtigere få informationer om potentielt mistænkelige kunder i deres portefølje.

- Mulighederne for at opdage kriminelle netværk forbedres, hvis delte risikoflag beriges med de rette stamdata (grunddata om eksempelvis navn, CVR-nummer, informationer om den givne transaktionen mv.).

Finans Danmarks Hvidvask Task Force har også fremhævet udfordringerne ved, at pengeinstitutter ikke kan udveksle oplysninger om risikable kundeforhold.

Pengeinstitutterne har i dag udelukkende mulighed for at dele oplysninger om kunder, hvis oplysningerne vedrører den samme kunde og samme transaktion, jf. hvidvasklovens § 38, stk. 6. Det er muligt, at en sådan datadelingsmekanisme kunne understøttes bedre, men værdien herved er begrænset i forhold til en mere generel deling af risikoflag. Det skyldes, at en sådan mekanisme udelukkende vil understøtte en mere effektiv deling af oplysninger om mistænkelige transaktioner foretaget af den samme kunde på tværs af egne konti i forskellige pengeinstitutter, men ikke vil bidrage til at gøre det nemmere at identificere andre kundeforhold med højere risiko.

Finanstilsynet har derfor analyseret værdien og kompleksiteten ved at dele risikoflag på to tidspunkter i transaktionsovervågningen. Det gælder hhv. risikoflag rejst og prioriteret automatisk (prioriterede risikoflag, der rejses tidligt i pengeinstitutternes transaktionsovervågningen, inden transaktionen er undersøgt manuelt og mistanken be- eller afkræftet), og risikoflag, der er blevet undersøgt af en sagsbehandler, og hvor mistanken ikke er afkræftet (undersøgte risikoflag). Særligt tre forhold har relevans for denne analyse:

1. **Kvalitet af transaktionsovervågningen på tværs af pengeinstitutter:** En konsekvens af lav kvalitet kan være, at mængden af delte false-positives (transaktioner, der fejlagtigt flages som mistænkelige) bliver for stor med det resultat, at delingen af risikoflag kan skabe mere støj end gavn.

2. ***Derisking* af kundeporteføljerne:** En sådan deling kan have uheldige konsekvenser, hvis pengeinstitutter eksempelvis ikke vil indlede eller afvikler kundeforhold, der er flaget af andre pengeinstitutter som mistænkelige (blacklisting).

3. **Løbende kontroller af risikoflag:** Kontrolleres validiteten af delte risikoflag ikke løbende, eksempelvis når en mistanke afkræftes, risikerer man, at delt data forstyrrer det samlede billede.

Finanstilsynet vurderer, at undersøgte risikoflag som udgangspunkt bedre vil kunne bidrage til formålet end prioriterede risikoflag. Det skyldes kvaliteten af pengeinstitutternes transaktionsovervågning, jf. afsnit 10.4. Værdien i delingen af undersøgte risikoflag er dog begrænset af, at processerne ikke kan automatiseres. Perioden fra et undringsværdigt forhold observeres, til det kan deles med andre, vil derfor afhænge af effektiviteten af det enkelte pengeinstituts interne processer. Delingen af prioriterede risikoflag kan også bidrage til formålet og har samtidig potentiale til fuld automatisering. En forudsætning er dog, at kvaliteten af pengeinstitutternes automatiserede transaktionsovervågning øges. Dette kan bl.a. ske ved, at der fastsættes generaliserede scenarier for, hvilke og hvornår risikoflag må deles. Transaktionsovervågningen vil dermed også i nogen grad ensartes på tværs af pengeinstitutterne.

Et særligt opmærksomhedspunkt i forbindelse med deling af risikoflag er at sikre, at det ikke leder til en øget derisking af kundeporteføljerne. Delte risikoflag bør udelukkende indgå som input i pengeinstitutternes kundekendskabsprocedurer og overvågning, og de må ikke alene lægges til grund for beslutninger om det specifikke kundeforhold. Det skyldes dels retssikkerhedsmæssige betænkeligheder, jf. afsnit 10.7, og dels risikeres det, at kriminelle aktører i stedet vil forsøge at operere på det sorte marked, hvorved de vil blive endnu sværere at opdage. Delingen af risikoflag indebærer derfor som minimum en forventningsafstemning mellem myndigheder og pengeinstitutter omkring udfordringerne ved derisking. Det bør eksempelvis tydeliggøres, at det ikke er en forventning fra myndighederne, herunder Finanstilsynet, at pengeinstitutter ikke har kunder med høj risiko i porteføljen, men udelukkende, at overvågningen af kundeforholdet er betinget af risikoen.

Uanset typen af risikoflag, der ønskes delt, er pengeinstitutterne i dag forpligtet til at hemmeligholde underretninger til Hvidvasksekretariatet, eller at der er eller vil blive iværksat undersøgelser efter § 25 i hvidvaskloven. Det følger af § 38, stk. 1. Det betyder, at en løsning, hvor

pengeinstitutterne generelt har adgang til delte risikoflag, ikke er mulig under det gældende regelsæt.

Finanstilsynet vurderer på den baggrund, at en sektordreven løsning med en bredere deling af risikoflag pengeinstitutterne imellem vil kræve en ændring af § 38 i hvidvaskloven. Da hvidvaskloven implementerer EU's hvidvaskdirektiv, vil en ændring kræve, at der først foretages ændringer i dette.

Et videre arbejde med denne mulighed indebærer derfor først og fremmest, at der på europæisk plan igangsættes en indsats med fokus på at tilpasse tavshedsbestemmelserne indeholdt i hvidvaskdirektivet.

I 2021 igangsættes et fælles europæiske arbejde omkring omdannelsen af hvidvaskdirektivet, hvor Danmarks bidrag kunne indeholde en sådan indsats. Den præcise form af omdannelsen er endnu ikke tydeliggjort, men Finanstilsynet forventer, at der vil være mulighed for at rejse et forslag om en tilpasning af tavshedsbestemmelserne.

Det kan dog forventes, at der vil være modstand mod et sådant forslag fra flere sider, da en række lande har den holdning, at problemet i dag ikke er hvidvaskreglerne, men snarere implementering af dem, jf. afsnit 11.

Alternativt kan det overvejes, om en datadelingsmekanisme for risikoflag kan etableres i regi af en offentlig myndighed. Pengeinstitutterne ville derigennem få adgang til relevant data for risikoklassificeringen af egne kunder. Da tavshedspligtsbestemmelserne i hvidvaskloven alene retter sig mod de underretningspligtige, er myndighederne ikke bundet af dem. Myndighederne vil derimod være omfattet af andre regelsæt, som giver anledning til andre juridiske overvejelser, bl.a. fordi der som udgangspunkt vil være tale om deling af oplysninger om mulige strafbare forhold, jf. afsnit 10.7.

En centralisering af datadelingsmekanismen, uanset om det er i offentligt eller privat regi, vil sandsynligvis være nødvendig af tekniske årsager, jf. afsnit 10.6. Den bør bl.a. kunne understøtte et kontrolmiljø, der så vidt muligt sikrer, at delte risikoflag repræsenterer en reel mistanke, samt understøtte yderligere analyse af delte risikoflag.

Uanset valget af model vil proportionaliteten i forhold til persondatareglerne skulle vurderes i forhold til de tre elementer: Egnethed, nødvendighed og forholdsmæssighed, jf. afsnit 10.7.

10.1. Effektiv transaktionsovervågning i praksis

Finanstilsynet har i samarbejde med eksterne konsulenter undersøgt regeloverholdelsen for transaktionsovervågning på tværs af en række større danske pengeinstitutter. Undersøgelsen har bl.a. dannet grundlag for en generaliseret metodologi for de enkelte elementer i en effektiv proces. Analysen tager udgangspunkt i denne metodologi.

Figur 10.1 illustrerer de enkelte elementer i en generaliseret proces for transaktionsovervågningen. Første skridt er, at relevante data for pengeinstitutternes kunder samles til et datasæt. Det indebærer som minimum:

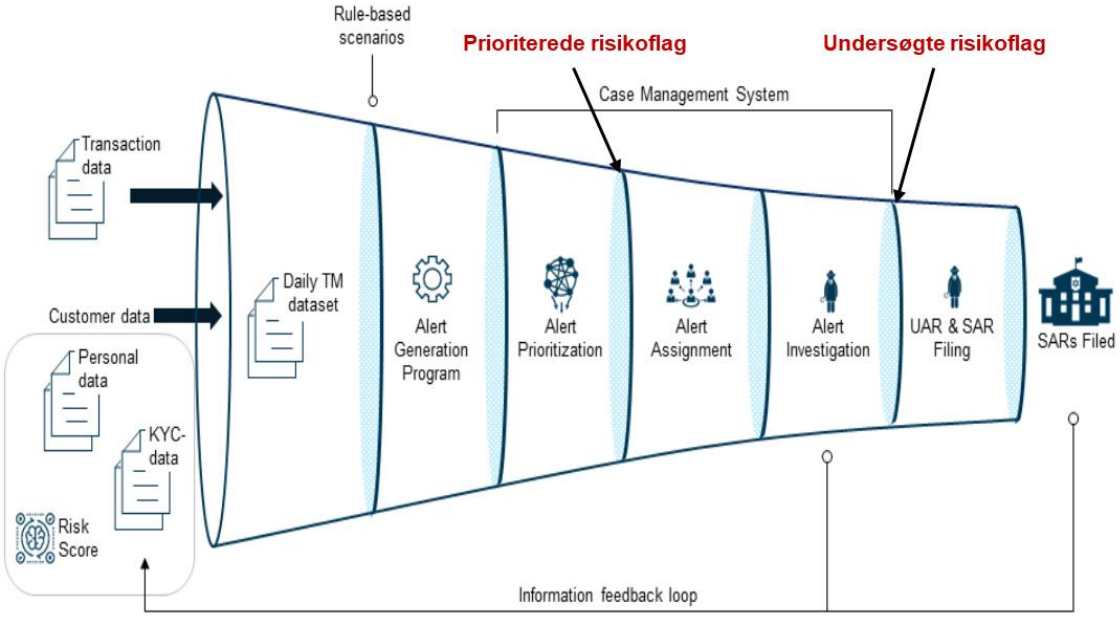
- **Kundeoplysninger:** Identitetsoplysninger, formål, tilsigtet beskaffenhed og risikoklassificering, jf. § 11 i hvidvaskloven

- **Transaktionsdata:** Det fulde overblik over kundens transaktioner og aktiviteter.

Dette konsoliderede datasæt udgør grundlaget for pengeinstitutternes transaktionsovervågning. Kvaliteten og omfanget af datasættet er derfor afgørende for effektiviteten af pengeinstitutternes indsats.

En effektiv transaktionsovervågning bør have automatiserede processer, der hhv. flager undringsværdige forhold (risikoflag) og prioriterer dem i forhold til den efterfølgende undersøgelse. Risikoflag rejses i dag primært ved brug af såkaldte regelbaserede scenarier (scenariemetoden). Scenarierne repræsenterer undringsværdige forhold, som identificeres ud fra prædefinerede betingelser, der er opstillet som indikatorer på potentiel hvidvask eller terrorfinansiering. Det er derfor afgørende for en effektiv transaktionsovervågning, at de opstillede scenarier er effektive, jf. afsnit 10.2.

Figur 10.1 – Generaliseret arkitektur for transaktionsovervågningen



Kilde: Finanstilsynet undersøgelse af regeloverholdelse for transaktionsovervågningen.

Den automatiserede prioritering af de genererede alarmer i forhold til den efterfølgende undersøgelse skal sikre, at de mest kritiske forhold undersøges først. Det skal eksempelvis ske ved at prioritere analysen af specifikke kundeforhold ud fra antallet og ikke mindst karakteren af rejste alarmer og ved frasortering af kendte false-positives[55]. Der kan eksempelvis opstå situationer, hvor en alarm rejses igen, selvom den tidligere er blevet rejst, vurderet og frasorteret.

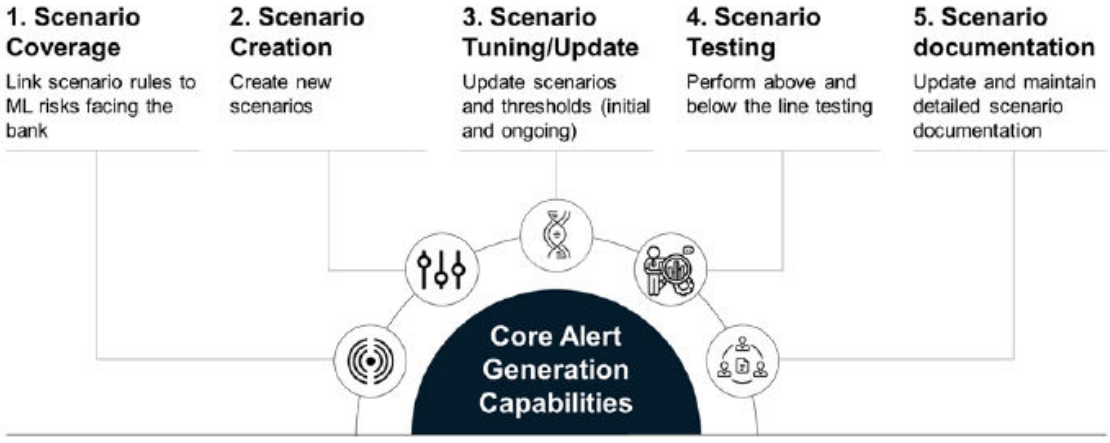
[55] False-positives kan også opstå, hvis et givent scenarie medfører, at der rejses en række risikoflag på et ikke materielt grundlag. Dette vil dog være svært at frasortere automatisk, da problematikken relaterer sig til kvaliteten af det specifikke scenarie.

Efter prioriteringen undersøges et givent risikoflag af en sagsbehandler. Denne undersøgelse kan eventuelt lede til, at der sendes en underretning til Hvidvasksekretariatet. En effektiv sagsbehandling indebærer, at sager håndteres ud fra en risikobaseret tilgang, og at der er etableret systemer til at sikre, at alle relevante observationer om en given kunde inddrages i undersøgelsen. Det indebærer bl.a. stamdata, KYC-informationer og tidligere rejste risikoflag. Samtidig bør der være opstillet retningslinjer for, hvilke faktorer sagsbehandleren skal lægge vægt på i en given undersøgelse, eksempelvis scenariespecifikke retningslinjer. Til sidst er det vigtigt med dokumentation for undersøgelsens resultater[56]. Det er både nødvendigt, hvis en undersøgelse leder til en underretning af Hvidvasksekretariatet, og for at sikre et tilstrækkeligt kundekendskab i de tilfælde, hvor det ikke leder til en underretning.

10.2. Effektive scenarier

Effektive scenarier karakteriseres ved, at de dækker de iboende risici ved pengeinstitutternes forretningsmodel, er dynamiske i forhold til kundens risikoklassificering, og at formålet med det enkelte scenarie er dokumenteret og fyldestgørende. En effektiv overvågning på tværs af pengeinstitutter er derfor ikke nødvendigvis det samme som, at alle bruger de samme scenarier og grænseværdier[57]. Pengeinstitutternes transaktionsovervågning vil derfor ikke kunne harmoniseres, selvom der ofte vil være overlap mellem de risikokategorier, der bør afdækkes. Effektivitetsforbedringer bør derfor også deles på tværs. Forskellene mellem pengeinstitutterne vil sandsynligvis være større end forskellene mellem andre virksomheder i andre brancher. Pengeinstitutterne misbruges nemlig på mange forskellige måder, eksempelvis ved at midlerne føres igennem et bredt netværk at konti.

Figur 10.2 – Udgangspunkt for etableringen af effektive scenarier



Kilde: Finanstilsynets undersøgelse af regeloverholdelse for transaktionsovervågning.

Som illustreret i figur 10.2 bør udarbejdelsen og brugen af scenarierne i bedste fald bygge på fem kriterier. Pengeinstitutterne skal sikre, at scenarierne afspejler de relevante risikofaktorer relateret til produkt- og kundetyper, geografiske forhold mv. Derudover bør alle benyttede scenarier løbende vedligeholdes og de benyttede grænseværdier tilpasses både i forhold til pengeinstituttets risikoprofil og den enkelte kundes risikoklassificering. Det bør gøres

[56] En undersøgelse skal dokumenteres gennem et narrativ, der beskriver undersøgerens argumentation for en given vurdering, og ved at inkludere alle benyttede observationer og kilder.
[57] Grænseværdien er den værdi, der skal overskrides for, at der rejses et risikoflag. Den kan både fastsættes ud fra specifikke informationer indhentet om kunden, såsom forventede størrelser på overførsler, og på baggrund af en mere generel betragtning af, hvornår et forhold bør karakterisere som mistænkeligt.

på baggrund af løbende test af scenariets effektivitet. Dette skyldes bl.a. en forventning om, at de kriminelles adfærd ændrer sig i takt med, at deres metoder bliver afsløret.

Muligheden for generaliserede scenarier

Finanstilsynet har i undersøgelsen af regeloverholdelsen for transaktionsovervågningen observeret, at der er et vist overlap mellem de risici, der afdækkes gennem transaktionsovervågningen, og en vis lighed mellem de tilhørende scenarier. Overlappene er størst for de pengeinstitutter, der har outsourcet transaktionsovervågningen til de samme datacentraler, men ses også for andre pengeinstitutter. Finanstilsynet har kategoriseret de benyttede scenarier under 13 overordnede risikokategorier, der kan indikere, at en kundes aktiviteter er undringsværdige og bør undersøges. Eksempler er:

- **Grænseoverskridende aktiviteter:** Scenarier, der er fokuseret på at fange usædvanlige aktiviteter relateret til grænseoverskridende transaktioner. Det kan eksempelvis være i forbindelse med samarbejde med korrespondentbanker, hvor kundekendskabet vedrører korrespondentbanken eller respondenten og ikke kunden, der rent faktisk udfører transaktionerne

- **Afvigelser fra kundens KYC-profil:** Scenarier, der identificerer aktiviteter, der afviger fra kundeprofilen. Det kan eksempelvis være, hvis kunden foretager eller modtager en betydeligt højere overførsel, end hvad der er angivet som maksimum under etablering af kundeforholdet.

- **Aktiviteter med kontanter:** Scenarier fokuseret på udsædvanlige aktiviteter med kontanter. Det kan eksempelvis dreje sig om store indskud eller hævninger.

Andre eksempler på, at scenarierne kan generaliseres, er FATF's guidance fra september 2020 omkring risikoflag for virtuelle aktiver[58] og Egmonts gennemgang af indikatorer på terrorfinansiering[59].

10.3. Fokus på to modeller for deling af risikoflag

Det er afgørende for kvaliteten af en datadelingsmekanisme for risikoflag, at delt information kan prioriteres. Det vil bl.a. kræve, at pengeinstitutter, der inddrager den delte information, i højere grad kan opstille processer for dette og sikre mindre "støj" som følge af false-positives i det delte datasæt, jf. afsnit 10.1.

Samtidig er det afgørende for en effektiv datadelingsmekanisme, at der kan fastsættes klare retningslinjer for delingen af risikoflag. Det skyldes, at pengeinstitutter kun vil kunne inddrage delte risikoflag effektivt i egne kundekendskabsprocedurer, hvis der er fuld transparens omkring årsagen til en mistanke. En tilgang er at fokusere sådanne retningslinjer på, hvornår et delt risikoflag er tilstrækkeligt dokumenteret. Med tilstrækkelig dokumentation menes, at bevæggrunden bag det rejste risikoflag skal belyses i en sådan grad, at andre pengeinstitutter kan inddrage mistanken effektivt i egne kundekendskabsprocedurer[60].

[58] FATF Report – Red flag indicators of Money Laundering and Terrorist Financing.
[59] FIUs and Terrorist Financing Analysis - A review by the Egmont Group. Egmont Group er et organ bestående af deltagere fra 166 FIU'er. Formålet med organet er at udveksle ekspertise og derigennem understøtte en fælles international indsats mod hvidvask og terrorfinansiering.
[60] Det kunne eksempelvis indebære en begrundelse i form af et narrativ og informationer om det underliggende scenarie og de benyttede grænseværdier for kunden.

En alternativ tilgang er, at risikoflag kun må deles på baggrund af generaliserede scenarier. I så fald vil fastsættelsen og den løbende udvikling af scenarierne og prioriteringsmekanismerne skulle tillægges et ansvarligt organ. Ansvaret for dette kunne eksempelvis placeres i det forum, FEHT, som sektoren har foreslået, jf. afsnit 8. Det bør i så fald kommunikeres klart, at ansvaret for tilstrækkeligt at afdække alle relevante risici i transaktionsovervågningen fortsat ligger hos det enkelte pengeinstitut.

Finanstilsynet vurderer derfor, at delingen af risikoflag vil kunne gennemføres på to tidspunkter i transaktionsovervågningen, nemlig hhv. efter, at risikoflagene er blevet prioriteret automatisk (model 1), eller efter, at de er blevet undersøgt af en sagsbehandler (model 2).

Model 1: Deling af prioriterede risikoflag
En fordel ved at dele prioriterede risikoflag er, at automatiseringspotentialet er højt. Det skyldes, at scenariemetoden som udgangspunkt er automatiseret, og det samme bør en effektiv prioritering af risikoflag være.

Delingen af prioriterede risikoflag forudsætter, at pengeinstitutternes processer for transaktionsovervågning er effektive. Er det ikke tilfældet, er der en betydelig risiko for, at delingen af prioriterede risikoflag vil skabe "støj" i andre pengeinstitutters kundekendskabsprocedurer. Omvendt vil behovet for dokumentation være af mere teknisk karakter. Det gælder eksempelvis oplysninger om scenariet og kundens individuelle grænseværdi.

En anden fordel ved delingen af prioriterede risikoflag er, at det er muligt at lægge generaliserede scenarier direkte til grund for, hvornår et risikoflag kan deles. Det kan mindske kompleksiteten for andre pengeinstitutter i forhold til at inddrage risikoflagene i egne kundekendskabsprocedurer, da det vil skabe fuld gennemsigtighed omkring bevæggrunden bag delingen. En konsekvens af dette er dog, at nuancegraden vil være mindre, end hvis risikoflag kan deles frit. Det skyldes primært, at der ikke vil kunne opstilles en ramme for alle scenarier, der bør indgå i pengeinstitutternes transaktionsovervågning, jf. afsnit 10.2.

Model 2: Deling af undersøgte risikoflag
Alternativt kan man forestille sig en mekanisme, hvor pengeinstitutterne får mulighed for at dele resultaterne af sagsbehandlernes undersøgelser af risikoflagene. Denne model kan skabe værdi i to typer af tilfælde:

1. Undersøgelsen medfører en mistanke om kriminelle aktiviteter, og mistanken vurderes tilstrækkelig til, at Hvidvasksekretariatet underrettes.

2. Undersøgelsen medfører en mistanke, men mistanken vurderes ikke tilstrækkelig til, at den videregives til Hvidvasksekretariatet. Det kan eksempelvis være i tilfælde, hvor kommunikationen med kunden om det specifikke forhold endnu ikke har afkræftet mistanken tilstrækkeligt. En direkte konsekvens af en sådan mistanke kan være en justering af risikovurderingen af kunden.

Finanstilsynet vurderer, at delingen af undersøgte risikoflag har nogle fordele i forhold til at dele prioriterede risikoflag:

- **Færre videregivne false-positives:** De rejste risikoflag vil både have gennemgået en automatisk bortsortering af false-positives og en manuel undersøgelse.

- **Mere effektiv brug:** Undersøgte risikoflag gennemgår "checks and balances" via den manuelle sagsbehandling. Det vil alt andet lige betyde, at mistanken omkring hvidvask eller terrorfinansiering vil være mere konkret end ved delingen af prioriterede risikoflag.

- **Samlet pakke:** Den manuelle undersøgelse vil basere sig på det fulde kundekendskab og dermed ikke enkelte risikoflag. Derfor vil delingen i de fleste tilfælde tage form af en samlet pakke af alle risikoinformationer for en given kunde og transaktion.

Denne model forudsætter ikke i samme omfang som den forrige, at pengeinstitutternes processer for transaktionsovervågning er effektive.

Omvendt vil automatiseringspotentialet for delingen af undersøgte risikoflag være mere begrænset. Det skyldes, at undersøgelsen per definition indebærer manuel håndtering af en sagsbehandler. Derudover vil dokumentationskravene være mere omfattende end for prioriterede risikoflag, da der eksempelvis også bør indgå en kvalitativ begrundelse for den samlede vurdering.

10.4. Værdien af datadeling er betinget af kvaliteten af transaktionsovervågningen

Finanstilsynets vurdering af, om kvaliteten af danske pengeinstitutters transaktionsovervågning er tilstrækkelig til at dele risikoflag, baseres på Finanstilsynets undersøgelse af regeloverholdelsen for transaktionsovervågningen i de største pengeinstitutter. Det skyldes forventningen om, at de største pengeinstitutter er længst fremme i forhold til indretningen af en effektiv transaktionsovervågning. Fælles for de undersøgte pengeinstitutter er, at datacentraler helt eller delvist håndterer den tekniske infrastruktur.

Den overordnede konklusion på undersøgelsen er, at transaktionsovervågningen ikke har været tilstrækkeligt effektiv. Det skyldes særligt, at processerne hverken er tilstrækkeligt dokumenteret eller fyldestgørende afdækker alle elementer af pengeinstitutternes risikovurdering eller de enkelte kunders risikoklassificering. Finanstilsynet gav derfor en række påbud, og visse af påbuddene var af så fundamental karakter, at en efterlevelse kræver ændringer hos datacentralerne.

Finanstilsynet vurderer derfor, at værdien ved at dele risikoflag er betinget af, hvilken model der bruges, og hvilket tidsperspektiv man ønsker for implementeringen af løsningen.

Nødvendigheden af objektive kriterier for prioriterede risikoflag

Finanstilsynet vurderer, at de danske pengeinstitutters udfordringer især relaterer sig til dels at opstille tilstrækkelige scenarier, dels at dokumentere hvilke specifikke risici hvert scenarie enkeltvis søger at mitigere. Det medfører en risiko for, at et betydeligt omfang af de undringsværdige forhold i dag slet ikke flages, og at de faktisk flagede aktiviteter i mange tilfælde er false-positives.

Finanstilsynet vurderer derfor, at fri deling af prioriterede risikoflag er forbundet med en betydelig risiko for, at:

1. kunder risikerer at blive afvist af et pengeinstitut på et fejlagtigt grundlag

2. pengeinstitutterne ikke kan styre de risici, der er forbundet med kunderne. Fejlagtige data kan forurene kundekendskabet og dermed risikoklassifikation af kunden i de pengeinstitutter, der gør brug af de delte risikoflag. Dette er desuden et problem, fordi pengeinstitutterne, på grund af et mangelfuldt revisionsspor, ikke kan foretage fornyede vurderinger af årsagen til, at et risikoflag er rejst hos et andet pengeinstitut

3. værdien ikke retfærdiggør omkostninger ved at etablere en datadelingsmekanisme, da der kun vil deles en (mindre) delmængde af de risikoflag, der kunne skabe værdi på tværs af branchen.

Finanstilsynets undersøgelse viste eksempelvis, at der i perioden fra den 1. oktober 2018 til den 30. september 2019 i gennemsnit blev rejst 4.450 risikoflag om måneden på tværs af de undersøgte pengeinstitutter, men kun 5 pct. af disse risikoflag ledte til en underretning til Hvidvasksekretariatet. En af forklaringerne er sandsynligvis, at flere af pengeinstitutterne ikke har implementeret processer for prioritering af risikoflag. Undersøgelsen viste nemlig også, at det pengeinstitut, der havde automatiserede processer for prioritering af risikoflag, frasorterede knap 60 pct. af de rejste risikoflag, før de blev sendt videre til manuel undersøgelse. For dette pengeinstitut ledte godt 40 pct. af de prioriterede risikoflag til en underretning til Hvidvasksekretariatet.

Finanstilsynet vurderer på den baggrund, at værdien ved frit at dele prioriterede risikoflag på baggrund af tilstrækkelig dokumentation i dag er meget begrænset. Værdien i en sådan model kræver, at den generelle kvalitet af transaktionsaktionsovervågning løftes betydeligt på brancheniveau, hvilket bør sikres, men også vil være forbundet med et længere tidsperspektiv.

Fastsættes der generaliserede scenarier for, hvilke prioriterede risikoflag der kan deles, vurderes der at være en merværdi. Tidsperspektivet i en sådan datadelingsmekanisme vil dog også være betinget af den tid, det vil tage at fastsætte generaliserede scenarier.

Deling af undersøgte risikoflag forbundet med størst værdi i dag
Finanstilsynet vurderer derimod, at undersøgte risikoflag, der enten leder til en underretning af Hvidvasksekretariatet eller en tilpasning af risikoklassificeringen af kundeforholdet, i mange tilfælde repræsenterer en reel mistanke. Derfor vil der også være en merværdi ved fri deling af undersøgte risikoflag i forhold til prioriterede risikoflag i dag.

Det skyldes primært, at pengeinstitutternes udfordringer især relaterer sig til den automatiserede del af transaktionsovervågningen fremfor den manuelle sagsbehandling af de rejste risikoflag.

Finanstilsynets undersøgelse viste dog, at pengeinstitutterne fortsat også har en række udfordringer i forhold til praksis for den manuelle sagsbehandling, herunder:

- Mangel på klar og detaljeret vejledning (arbejdsgange) for hvordan risikoflag rejst fra specifikke adfærdsscenarier bør undersøges af en sagsbehandler

- Manglende systematik i fordelingen af alarmer til den rigtige sagsbehandler. Risikoflagene afspejler i høj grad forskellige risici, og kompetencerne for vurdering af en specifik risiko vil i mange tilfælde være fordelt på tværs af sagsbehandlere

- Begrænset omfang af kvalitetskontroller og -vurderinger af sagsbehandleres undersøgelser af de rejste risikoflag.

En konsekvens af dette kan både være, at de faktisk foretagne underretninger er misvisende, og at pengeinstitutterne ikke underretter om alle relevante forhold til Hvidvasksekretariatet. I praksis vil den primære konsekvens af de manglende processer sandsynligvis være, at pengeinstitutterne bruger flere ressourcer end nødvendigt, når rejste risikoflag undersøges manuelt[61]. Eksempelvis har en direktør for en SIFI-bank udtalt til Finanstilsynet, at den økonomiske gevinst ved en sædvanlig privatkunde forsvinder, hvis denne kunde bare én gang udtages til manuel undersøgelse i forbindelse med transaktionsovervågningen.

Derudover kan en ineffektiv kalibrering af den automatiserede transaktionsovervågning have afledte effekter på kvaliteten af den manuelle sagsbehandling. Eksempelvis ved at:

1. der sendes så mange risikoflag til manuel behandling, at der opstår en backlog i forbindelse med den manuelle behandling, og Hvidvasksekretariatet derved ikke underrettes rettidigt.

2. alle relevante risikoflag ikke rejses.

Finanstilsynet vurderer derfor også, at værdien ved deling af undersøgte risikoflag kan forstærkes, hvis der fastsættes generaliserede scenarier. Det skyldes, at pengeinstitutterne sandsynligvis vil rejse og videregive færre false-positives til manuel undersøgelse, og sagsbehandlerne derfor i højere grad vil rette deres indsats mod faktisk undringsværdige forhold.

Delingen af risikoflag indebærer omkostninger for pengeinstitutterne
Pengeinstitutterne har i dag ikke mulighed for at dele risikoflag med hinanden. Delingen af risikoflag vil derfor medføre, at de hver især skal investere i deres tekniske infrastruktur, hvis de vil tage del i udvekslingen. Det vil sandsynligvis være forbundet med betydelige omkostninger, særligt for større og ældre pengeinstitutter, hvis IT-systemer ofte er mere omfattende og komplekse at udvikle.

Fælles for de undersøgte pengeinstitutter er, at de hver især har outsourcet dele af eller hele den tekniske infrastruktur for transaktionsovervågningen til en datacentral. Datacentralerne er delvist ejet af pengeinstitutterne og løfter en helt central rolle i implementeringen og vedligeholdelsen af den tekniske infrastruktur. Pengeinstitutterne er aktivt involverede i deres arbejde, bl.a. gennem styregrupper, og i nogle tilfælde også ved, at der allokeres ressourcer

[61] Det skyldes bl.a., at de undersøgte pengeinstitutter har implementeret systemer, der gør det muligt for sagsbehandlere systematisk at indsamle anden relevant information, der er afgørende for en retvisende vurdering.

til datacentralerne i forbindelse med gennemførelsen af forskellige projekter. Det gælder eksempelvis inddragelsen af ny data i transaktionsovervågningen.

Finanstilsynet vurderer, at pengeinstitutterne i fællesskab vil kunne bære en del af omkostningerne ved at udvikle infrastrukturen. Samtidig må den kunne udvikles hurtigere i takt med, at den skal udvikles færre steder. Det må dog fortsat forventes, at udviklingen af IT-systemerne tager tid.

En anden konsekvens af at gennemføre et initiativ, der tillader delingen af risikoflag, er, at pengeinstitutterne skal allokere flere ressourcer til både at dokumentere og sætte sig ind i bevæggrunden bag delte risikoflag. Det skyldes, at processen for transaktionsovervågning ikke kan harmoniseres, og at det vil være svært at retfærdiggøre ikke at forholde sig til et delt og indhentet risikoflag for en given kunde.

Finanstilsynet vurderer, at delingen af prioriterede risikoflag på baggrund af generaliserede scenarier vil være forbundet med færre omkostninger i forbindelse med dokumentation for et delt risikoflag. Samtidig vil gennemsigtigheden bag formålet med sådanne scenarier mindske mængden af ressourcer, der skal allokeres til at forstå bevæggrunden bag et prioriteret risikoflag. Pengeinstitutternes omkostninger ved at implementere en sådan model vurderes derfor primært at være af teknisk karakter. Det gælder eksempelvis for implementeringen af de forskellige scenarier i transaktionsovervågningen.

De ressourcemæssige omkostninger vil derimod sandsynligvis være større ved delingen af undersøgte risikoflag. Det gælder både i forhold til at dokumentere bevæggrunden bag delte risikoflag og for andre pengeinstitutter i forhold til at inddrage oplysningerne i egne kundekendskabsprocedurer. Nye omkostninger i relation til dokumentation bør dog være begrænsede, da pengeinstitutterne i dag allerede bør have processer for dokumentationen af deres arbejde med at undersøge risikoflag.

10.5. Muligheden for bredere netværksanalyser

Udgangspunktet for pengeinstitutternes transaktionsovervågning er som sagt scenariemetoden. En effektiv transaktionsovervågning bør også indebære såkaldte netværksanalyser, enten som led i den automatiserede overvågning eller som et redskab, sagsbehandlere har adgang til. Sådanne analyser er i dag kun muligt internt i pengeinstituttet eller i koncernen, eksempelvis ved at kortlægge mistænkelige transaktionsnetværk internt i pengeinstituttet. Analyser kan også gennemføres i form af en mere helhedsorienteret betragtning af outliers på tværs af det samlede kundegrundlag. Denne type overvågning er dog ikke særligt udbredt blandt danske pengeinstitutter i dag, og i de tilfælde, den bruges, driver den kun en lille andel af de samlede rejste risikoflag[62].

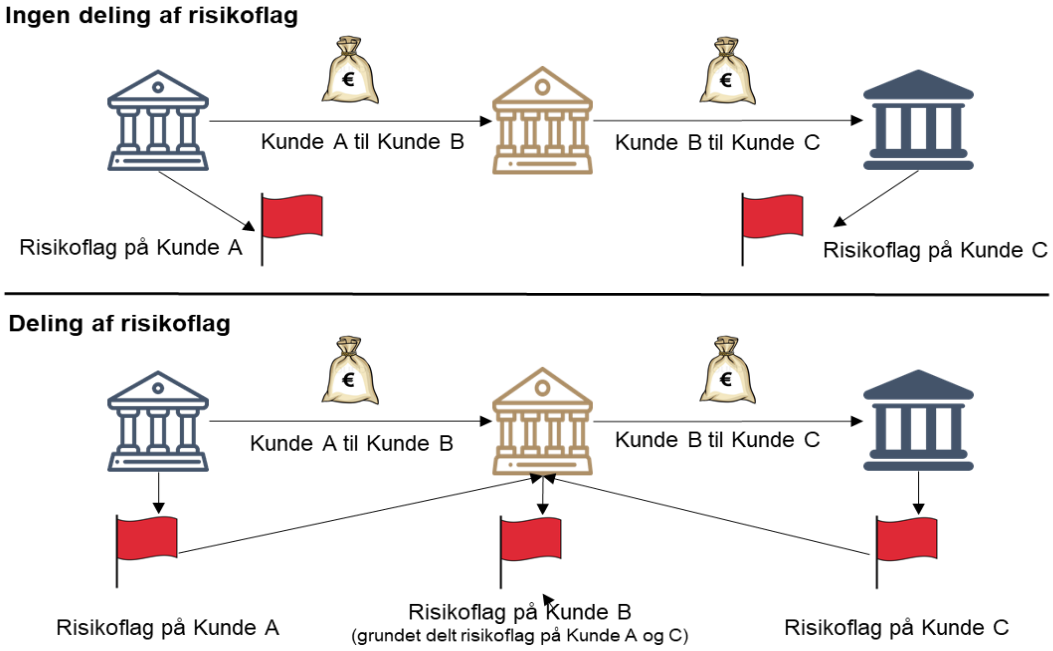
En generel udfordring er dog, at kriminelle aktører ofte slører deres aktiviteter gennem et netværk af transaktioner, virksomheder og konti på tværs af mange finansielle virksomheder, nationalt og globalt. Pengeinstitutternes indsigt i sådanne netværk starter i dag, når midler overføres til en konto hos det enkelte pengeinstitut, og stopper i det øjeblik, midlerne føres ud af pengeinstituttet igen. Det er altså ikke muligt for de enkelte pengeinstitutter at følge

[62] Baseret på observationer i Finanstilsynets undersøgelse af regeloverholdelse for transaktionsovervågningen.

pengenes rejse på tværs af den finansielle sektor, hvilket med stor sandsynlighed begrænser deres mulighed for at opdage alle undringsværdige forhold.

Delingen af risikoflag på tværs af sektoren har, hvis det bliver gjort rigtigt, også potentiale til at understøtte denne type netværksanalyser. Beriges delte risikoflag med de rette stamdata, bl.a. informationer om afsender, modtager og anden information om transaktionen, vil det i højere grad være muligt at identificere et netværk af mistænkelige kunder. Det gælder eksempelvis, hvis der overføres penge gennem en række identificerede gennemstrømningskonti på tværs af pengeinstitutter, jf. figur 10.3.

Figur 10.3 – Eksempel på muligheden for netværksanalyser



Kilde: Finanstilsynet.

10.6. Værdien i en centraliseret datadelingsmekanisme

Det bør under alle omstændigheder overvejes, om deling af risikoflag mest hensigtsmæssigt skal ske via en central funktion, og om det bør høre under eller administreres af en offentlig myndighed. En centralisering af datadelingsmekanismen er forbundet med både tekniske og potentielt analytiske fordele:

1. Der kan både fastsættes et standardiseret dataformat og en standardiseret adgang til at dele og hente risikoflag. Pengeinstitutterne vil kun skulle tale med én aktør fremfor hele branchen.

2. Adgangsmekanismen vil kunne struktureres, så kun pengeinstitutternes særlige complianceansvarlige får adgang til oplysninger – og udelukkende oplysninger, der er relevante for egne kundeforhold[63].

[63] Se eksempelvis overvejelser om videregivelse af informationer i forslaget til en udvidet PEP-løsning, jf. afsnit 5.

3. Der vil blive skabt et konsolideret datagrundlag for risikoobservationer på tværs af sektoren, der kan bruges til analyseformål, eksempelvis til bedre at forstå kriminel adfærd, eller hvilke alarmer der kan klassificeres som false-positives. Samtidig kan det understøtte netværksanalyser på tværs af alle delte risikoflag[64].

Registreringen af risikoflag i et centralt register skal dog indebære overvejelser om håndteringen og adgangen til persondata, særligt da der i vid udstrækning vil være tale om oplysninger om mulige strafbare forhold. Samtidig skal der tages stilling til, hvilket ansvar denne centrale enhed er underlagt med hensyn til fejlregistrering og kontrol af de oplysninger, som pengeinstitutterne indberetter. Det skal eksempelvis sikres, at delte risikoflag fjernes, hvis den bagvedliggende mistanke er blevet afkræftet.

10.7. Juridiske overvejelser

Deling af risikoflag vurderes navnlig at indebære juridiske spørgsmål i forhold til hvidvasklovens regler om undersøgelsespligt og tavshedspligt, jf. §§ 25 og 38. Bestemmelserne gennemfører henholdsvis artikel 40 og 39 i hvidvaskdirektivet. Hvidvasklovens § 25 har følgende ordlyd:

> *"**§ 25.**[65] Virksomheder og personer skal undersøge baggrunden for og formålet med:*
> ***1.** Alle transaktioner, der*
> ***a.** er komplekse,*
> ***b.** er usædvanlig store*
> ***c.** der foretages i et usædvanligt mønster, eller*
> ***d.** ikke har et åbenbart økonomisk eller lovligt formål.*
> ***2.** Alle aktiviteter, der ikke har et åbenbart økonomisk eller lovligt formål.*
> *Stk. 2. Virksomheder og personer skal, hvor det er relevant, udvide overvågningen af kunden med det formål at afgøre, om transaktionerne eller aktiviteterne forekommer mistænkelige.*
> *Stk. 3. Resultaterne af en undersøgelse skal noteres og opbevares, jf. § 30.*
> *Stk. 4. En registreret person har ikke ret til indsigt i personoplysninger, der vedrører den pågældende selv, der er eller vil blive behandlet efter stk. 1-3."*

Bestemmelsen indebærer, at de forpligtede enheder skal undersøge, om forhold, der er vurderet som værende usædvanlige, giver grundlag for mistanke eller formodning om hvidvask eller finansiering af terrorisme, eller om en mulig mistanke kan afkræftes. Undersøgelsen efter § 25 vil efter omstændighederne kunne indebære en pligt til at underrette, jf. hvidvasklovens § 26.

Hvidvasklovens § 38, stk. 1, har følgende ordlyd;

> *"**§ 38.** Virksomheder og personer omfattet af denne lov, ledelse og ansatte i disse virksomheder og hos disse personer samt revisorer eller andre, der udfører eller har udført særlige hverv for virksomheden eller personen, har pligt til at hemmeligholde,*

[64] Se eksempelvis Swedish Bankers' Associations overvejelser om deling af risikoflag mellem pengeinstitutter og myndigheder (side 16-18): https://www.swedishbankers.se/media/4425/sammanslutning-mot-finansiell-brottslighet_vf.pdf
[65] Angivet som nyaffattet i forbindelse med specialsamleloven OKT 2020, der forventes vedtaget i indeværende periode. Justeret henset til KOM's begrundede udtalelse.

at der er givet underretning efter § 26, stk. 1 og 2, eller at dette overvejes, eller at der er eller vil blive iværksat en undersøgelse efter § 25, stk. 1."

De forpligtede enheder er dermed forpligtet til at hemmeligholde, at de har underrettet Hvidvasksekretariatet, eller at der er eller vil blive iværksat en undersøgelse efter § 25. Bestemmelsen giver dog mulighed for, at de forpligtede enheder kan udlevere oplysningerne til myndigheder og organisationer, der fører tilsyn med overholdelsen af hvidvaskloven, dvs. Finanstilsynet, Erhvervsstyrelsen og Advokatrådet. Oplysningerne kan også deles indenfor virksomheden eller med virksomheder i koncernen.

Der er endelig i lovens § 38, stk. 6, mulighed for at dele oplysningerne med andre forpligtede enheder, herunder pengeinstitutter (§ 1, stk. 1, nr. 1), hvis:

1. oplysningerne vedrører samme kunde og samme transaktion,

2. modtageren af oplysningerne er underlagt krav til bekæmpelse af hvidvask og finansiering af terrorisme, der svarer til kravene i hvidvaskdirektivet, og

3. modtageren er underlagt forpligtelser med hensyn til tavshedspligt og beskyttelse af personoplysninger.

Pengeinstitutternes mulighed for at dele oplysninger om deres kunder i dag
Hvidvasklovens § 38, stk. 6, muliggør altså, at pengeinstitutter kan dele oplysninger om de ovennævnte forhold, hvis oplysningerne vedrører den samme kunde og samme transaktion. Pengeinstitutterne kan derfor allerede dele denne type oplysninger, når oplysningerne konkret er relevante for deres opgaver i forbindelse med forebyggelse og bekæmpelse af hvidvask og finansiering af terrorisme. Så længe pengeinstitutterne iagttager de almindelige regler for databehandling, eksempelvis databehandleransvar, og overholder de objektive kriterier (kun oplysninger om egne kunder og fælles transaktioner), så er der ikke umiddelbart noget til hinder for, at de kan foretager en sådan deling ved hjælp af en central mekanisme.

Tavshedsbestemmelserne understøtter ikke deling af risikoflag
En model med generel deling af undersøgte risikoflag og oplysninger om kunderne mellem pengeinstitutterne vil være i strid med den nuværende tavshedspligtsbestemmelse i hvidvaskloven, idet de er omfattet af undersøgelsen i § 25.

Prioriterede risikoflag vurderes umiddelbart også at være omfattet af tavshedspligtsbestemmelsen, da § 38 pålægger tavshedspligt i forbindelse med, "at der er eller *vil blive iværksat* undersøgelse". Pengeinstitutternes overvågningssystemer er indrettet til at finde de mistænkelige forhold, som kræver undersøgelse. Risikoflagene vurderes dermed at være en del af denne proces, formentlig på stadiet, hvor der *vil blive iværksat* en undersøgelse enten for at af- eller bekræfte, at der er tale om et mistænkeligt forhold (aktivitet eller transaktion).

Løsningen med generel deling af undersøgte såvel som prioriterede risikoflag kræver dermed, at der foretages ændringer i hvidvasklovens § 38, som er en implementering af hvidvaskdirektivets art. 39, der har følgende ordlyd:

"Forpligtede enheder samt deres ledelse og ansatte må ikke oplyse den pågældende kunde eller tredjemand om, at der sendes, vil blive sendt eller er blevet sendt oplysninger i henhold til artikel 33 eller 34, eller at der er blevet eller eventuelt vil blive iværksat en analyse vedrørende hvidvask af penge eller finansiering af terrorisme."

Ændringer af hvidvaskdirektivets bestemmelser må antages at være en mere omfattende proces, der i sidste ende kræver, at der er enighed blandt EU's medlemslande, jf. afsnit 11.

Indgrebets proportionalitet – undersøgte og prioriterede risikoflag
Inden der arbejdes videre med en løsning, som vil kræve ændring af hvidvasklovens regler og dermed forhandlinger på EU-niveau, bør en række forhold tages i betragtning.

Formålet med at dele risikoflag mellem pengeinstitutter er at styrke samfundets muligheder for at bekæmpe hvidvask og terrorfinansiering. Ved bedre at kunne dele oplysninger om kunders adfærd, transaktioner og aktiviteter, kan pengeinstitutterne og dermed samfundet i højere grad undgå, at kriminelle kan fortsætte kriminaliteten. Det kan i dag eksempelvis ske ved at den kriminelle aktør skifter pengeinstitut, hvormed det nye pengeinstitut skal opbygge kendskabet til kunden efter skiftet på ny, eller ved at der benyttes et netværk af konti i forskellige pengeinstitutter, hvor det enkelte pengeinstitut alene får kendskab til en delmængde af de samlede transaktioner. Finanstilsynet vurderer derfor, at en mulighed for deling af risikoflag eller andre typer af oplysninger vil være egnet til at opnå det forfulgte formål.

En bred deling af risikoflag eller andre oplysninger om mistænkelige transaktioner, aktiviteter eller adfærd vil formentlig være værktøjer, der kan sikre en styrket indsats mod hvidvask og terrorfinansiering, navnlig i forhold til kriminalitet, der går på tværs af flere forpligtede enheder. Finanstilsynet vurderer umiddelbart, at en model indeholdende generel deling af risikoflag og lignende oplysninger har størst potentiale.

Hvad angår modellens forholdsmæssighed, må den anses for at opfylde et påtrængende samfundsbehov, idet bekæmpelse af hvidvask og terrorfinansiering er en væsentlig samfundsopgave. De forpligtede enheder skal efter de gældende regler allerede rejse og undersøge risikoflag baseret på en kundes adfærd, transaktioner mv. Der er altså ikke tale om at registrere nye oplysninger om kunderne, men at oplysninger, som pengeinstitutterne allerede registrerer, gøres tilgængelige for andre pengeinstitutter og til samme formål, som de indsamles til.

Bemærk dog, at jo lavere grad af vurdering og undersøgelse, det enkelte pengeinstitut har foretaget, des større et indgreb vil det være overfor kunderne. Risikoklassificeringen af den enkelte kunde danner bl.a. grundlag for de parametre (tærskelværdier), der er sat op for, hvornår systemerne skal generere et risikoflag. Det bør derfor bl.a. overvejes, i hvilket omfang kunder med høj risiko, eksempelvis PEP'er og PEP'ers nærmeste, i højere grad vil slå ud med et risikoflag, selvom der ved nærmere undersøgelse ikke er noget mistænkeligt ved en transaktion eller aktivitet.

Det taler for, at en løsning vil skulle opbygges med en høj grad af sikkerhed for, at mistanken har en vis styrke. Det kunne eksempelvis være i form af objektive kriterier for prioriterede risikoflag, hvis andre pengeinstitutter skal dele og bruge dem. Proportionalitetsafvejningen

vil også kunne variere, afhængig af hvor mange og hvilke medarbejdere i pengeinstitutterne der har adgang til oplysninger, og af hvorvidt man alene kan få adgang til oplysninger om egne kunder eller om alle kunder i systemet.

Jo færre medarbejdere, der har adgang til oplysningerne, og jo færre oplysninger, der gives adgang til, eksempelvis alene for pengeinstituttets egne kunder, des mindre indgribende vil modellen være. En model, hvor der alene deles oplysninger om pengeinstitutternes egne kunder vedrørende transaktioner i pengeinstituttet, vil som udgangspunkt kunne rummes af muligheden i hvidvasklovens § 38.

En sådan model kræver dog, at der oprettes en mekanisme, som er tilstrækkelig til at håndtere disse kriterier, ligesom der vil skulle opstilles kriterier for sletning, opdatering mv.

Derisking
Uanset hvilken model der overvejes, er det vigtigt at undgå derisking og blacklisting. Det vil bl.a. være retssikkerhedsmæssigt betænkeligt, hvis oplysninger om undersøgelser eller underretninger til Hvidvasksekretariatet foretaget af andre pengeinstitutter automatisk fører til, at øvrige pengeinstitutter afviser kunden, eller at der automatisk foretages en underretning til Hvidvasksekretariatet, jf. afsnit 2.

Overvejelser om et centraliseret offentligt register med personoplysninger
Fordelen ved en central datadelingsmekanisme hos en offentlig myndighed vil bl.a. være, at det vil være tydeligt, hvilke oplysninger de enkelte pengeinstitutter deler om deres kunder, og at de eksempelvis ikke deler oplysninger, som ikke relaterer sig til hvidvaskbekæmpelse eller lignende. Desuden har offentlige myndigheder generelt god erfaring med at etablere en sikker og let tilgængelig infrastruktur, eksempelvis i forbindelse med håndtering af persondata.

Registrering af oplysninger og deling af disse i et offentligt register vil indebære overvejelser om håndteringen og adgangen til persondata. Det skyldes, at risikoflag, undersøgelser og underretninger til Hvidvasksekretariatet bygger på mistanke om eller tilknytning til hvidvask eller terrorfinansiering. Sådanne oplysninger vil som udgangspunkt karakteriseres som oplysninger om mulige strafbare forhold begået af fysiske personer. Det betyder, at persondataforordningens regler skal iagttages, med mindre der er tale om behandlinger, som er omfattet af retshåndhævelsesloven[66].

Tavshedspligtsbestemmelsen i hvidvasklovens § 38 er alene rettet mod de virksomheder og personer, som er underlagt hvidvaskloven, og omfatter ikke de myndigheder, der modtager oplysninger om kundeforhold, undersøgelser og underretninger som led i deres myndighedsudøvelse. Muligheden for at dele risikoflag vil dermed ikke nødvendigvis være betinget af en ændring i hvidvaskdirektivet. Offentlige myndigheder er derimod underlagt andre regelsæt om tavshedspligt og videregivelse.

Oprettelse af registeret i offentligt regi giver også anledning til en lang række andre juridiske overvejelser, eksempelvis i forbindelse med:

[66] Lov om retshåndhævende myndigheders behandling af personoplysninger, lov nr. 410 af 27. april 2017.

- hvem der har ansvaret for data, verificering, kontrol mv.

- sletning, retten til indsigt og spørgsmålet om muligt erstatningsansvar i tilfælde af, at der er delt fejlbehæftede oplysninger, eller hvor delte oplysninger har været brugt i strid med formålet og eksempelvis har haft indflydelse på en kundes mulighed for at opnå erhvervslån – med økonomisk tab til følge

- administrative og økonomiske omkostninger for det offentlige, som vil skulle afvejes i forhold til den forventede effekt på forebyggelse og opklaring af hvidvask og finansiering af terrorisme.

En endelig juridisk vurdering af muligheden for at oprette et sådant register i offentligt regi kræver, at der tages konkret stilling til registerets indretning og de forventede kriterier, der skal bruges ved deling mv.

11. Processen for videre internationalt arbejde

Finanstilsynet indstiller, at der i forbindelse med beslutningen omkring det videre arbejde med de identificerede forslag i rapportens øvrige afsnit træffes beslutning om samtidig at iværksætte en prioriteret dansk indsats i EU-regi for at realisere og styrke effekten af disse forslag. Det drejer sig især om øget harmonisering af hvidvaskdirektivets nuværende bestemmelser om kundekendskabsprocedurer og identifikation af reelle ejere, målrettede ændringer af tavshedsbestemmelserne og en øget brug af ny teknologi. Disse aspekter skal ses som et samlet hele. En dansk indsats vil kunne iværksættes op til eller i forbindelse med, at EU-reglerne forventes revideret som led i Kommissionens kommende forslag på området i andet kvartal af 2021. Det må dog forventes, at en dansk indsats vil strække sig over længere tid, grundet både det politiske og tekniske omfang af EU-forhandlingerne, ligesom visse ændringer vil kunne være svære at skabe fornøden opbakning til blandt andre EU-lande, Europa-Parlamentet og Kommissionen.

For en række af de konkrete forslag nævnt i rapportens øvrige afsnit, herunder særligt afsnit 4 og 10, vil det enten være nødvendigt eller hensigtsmæssigt med en indsats i internationalt regi, særligt i EU, for at fjerne potentielle hindringer i eksisterende EU-regulering eller for at styrke den fulde effekt af forslagene.

EU arbejder aktuelt på at forberede nye tiltag til at bekæmpe hvidvask og terrorfinansiering. Kommissionen offentliggjorde primo maj 2020 en handlingsplan for nye EU-tiltag, og det forventes, at Kommissionen vil fremlægge konkrete lovforslag i andet kvartal af 2021. Lovforslagene vil dog formentlig blive drøftet på overordnet niveau i Kommissionens ekspertgruppe for bekæmpelse af hvidvask og terrorfinansiering (EGMLTF) inden da. De forventede tiltag er bl.a. mere harmoniserede EU-regler på hvidvaskområdet gennem et forslag til ændring af hvidvaskdirektivet, bl.a. om at flytte dele af direktivet til en forordning.

Danmark har dermed et vindue til at bidrage med særlige synspunkter og rejse problemstillinger enten forud for eller i forbindelse med disse EU-forhandlinger. Ændringer af hvidvaskdirektivets bestemmelser må dog antages at være en mere omfattende proces, der i sidste ende kræver kvalificeret flertal blandt EU's medlemslande og støtte fra Europa-Parlamentet, der er medlovgiver. I praksis bør også Kommissionen bakke op om ændringerne for at sikre en bred opbakning og legitimitet.

En prioriteret dansk indsats i EU-regi er særlig relevant i forhold til to centrale dele af det nuværende hvidvaskdirektiv, hvis det videre arbejde skal fremmes: Mere harmoniserede regler vedrørende bl.a. kundekendskabsprocedurer og identifikation af reelle ejere (afsnit 11.1) samt målrettede lempelser af tavshedsbestemmelserne (afsnit 11.2).

11.1. Mere harmoniserede regler

En øget harmonisering af reglerne for kundekendskabsprocedurer og identifikation af reelle ejere vil kunne føre til en mere effektiv bekæmpelse af hvidvask og åbne for nye og mere effektive muligheder for sektoren, jf. afsnit 4.

ECOFIN vedtog i november 2020 rådskonklusioner om bekæmpelse af hvidvask og terrorfinansiering[67], som udgør Rådets strategiske og prioriterede indspil til Kommissionens kommende pakke af forslag på området. I rådskonklusionerne fremgår det bl.a., at Rådet opfordrer Kommissionen til at flytte specifikt omtalte dele af hvidvaskdirektivet til en forordning:

> *17. OPFORDRER Kommissionen TIL at forelægge et lovgivningsforslag til en forordning på grundlag af en vurdering af de relevante risici og konsekvenser med henblik på yderligere harmonisering af den materielle ret under hensyntagen til følgende områder: […] kundekendskabskrav – herunder passende fjernløsninger inden for kendskabsprocedurer samt elektronisk identifikation og verifikation –; bestemmelser om kendskabsprocedurer for inden- og udenrigspolitisk udsatte personer; […] bestemmelser om fastlæggelse af reelt ejerskab […]*

Der er derfor som udgangspunkt bred opbakning til en yderligere harmonisering af disse bestemmelser i hvidvaskdirektivet ved at flytte dem til en forordning. Det er dog på nuværende tidspunkt uklart, om den konkrete udformning af bestemmelserne i en forordning vil være tilstrækkeligt til at kunne levere den ønskede merværdi. Dette er dog noget, som Danmark vil kunne lægge vægt på at forsøge at sikre. Udover dette har Danmark en række øvrige prioriteter i forhold til omdannelsen af hvidvaskdirektivet til en forordning, som bl.a. indebærer, at det nuværende høje niveau for de danske nationale hvidvaskregler ikke svækkes under processen.

11.2. Lempelser af tavshedsbestemmelserne

En lempelse af tavshedsbestemmelserne i hvidvaskdirektivet vil være en forudsætning for at kunne gå videre med forslaget om deling af risikoflag mellem pengeinstitutter, jf. afsnit 10. Som det fremgår af afsnittet, er der modsatrettede hensyn, som begge tillægges stor politisk vægt.

På den ene side er der i EU i såvel som på internationalt plan stort fokus på bekæmpelsen af hvidvask og terrorfinansiering, og særligt samarbejdet på tværs af myndigheder og sektoren ses som en mulighed for at effektivisere indsatsen markant. Det kan dermed ikke afvises, at et forslag, der indebærer en mulighed for deling af oplysninger i sektoren med henblik på at understøtte denne dagsorden, vil kunne vinde indpas i EU-forhandlingerne under den forventede revision af EU-hvidvaskreglerne og lede til beslutninger, der kan muliggøre brugbare løsninger i forhold til en mulig lempelse af tavshedsbestemmelserne.

På den anden side må det også antages at være meget svært at skabe den fornødne opbakning fra andre medlemslande i Rådet og fra Europa-Parlamentet, herunder også i praksis Kommissionen, til ændringer af tavshedsbestemmelserne, hvis det indebærer en risiko for at komme i konflikt med det afgørende hensyn til, at mistænkelige kunder ikke (direkte eller indirekte) bliver informeret om, at pengeinstituttet har en mistanke til dem (det såkaldte tipping-off ban). Der kan også være tale om modstand mod at dele oplysninger om kunderne, idet der fra både Kommissionen, Europa-Parlamentet og nogle EU-landes side er et udtalt ønske om at prioritere databeskyttelse meget højt. Hertil kommer en måske ikke helt ube-

[67] https://data.consilium.europa.eu/doc/document/ST-12608-2020-INIT/da/pdf

grundet frygt for, at det kan føre til yderligere derisking. Et forsøg på at ændre tavshedsbestemmelserne vil derfor kræve en målrettet og skarpt formuleret undtagelsesmulighed med tilstrækkelig beskyttelse af kunderne.

I de tidligere omtalte ECOFIN-rådskonklusioner er problemstillingen og spændingen mellem de forskellige hensyn også adresseret:

> *20. OPFORDRER Kommissionen TIL at udvide anvendelsesområdet for anvendelsen af data inden for de grænser, der er fastsat i databeskyttelsesbestemmelserne, også ved at gøre bedre brug af digitalisering. OPFORDRER Kommissionen TIL – idet forbuddet mod advarsler opretholdes, og der ydes tilstrækkelige sikkerhedsforanstaltninger til beskyttelse af information – at overveje en udvidelse af mulighederne for udveksling af oplysninger inden for koncerner og mellem andre forpligtede enheder, der ikke tilhører samme koncern eller samme sektor, med henblik på bedre overvågning og efterlevelse af krav.*
>
> *21. OPFORDRER INDTRÆNGENDE Kommissionen og Det Europæiske Databeskyttelsesråd TIL at redegøre for, hvordan AML/CFT-rammen kan bringes i overensstemmelse med den gældende databeskyttelseslovgivning, navnlig med den generelle forordning om databeskyttelse, for at skabe større klarhed om, hvilke oplysninger der kan deles mellem forpligtede enheder samt mellem forpligtede enheder og kompetente myndigheder, og sikre et højt niveau af databeskyttelse og løse for eksempel uoverensstemmelser mellem databeskyttelsesbestemmelserne og forbuddet mod advarsler. Desuden bør enhver eventuel synergi med andre EU-retsakter tages i betragtning.*

Rådet bakker dermed umiddelbart op om at overveje øget deling af data på tværs af forpligtede enheder, men med tilstrækkelige sikkerhedsforanstaltninger og uden at underminere forbuddet mod advarsler. Besluttes det at gå videre med forslaget, foreligger et videre arbejde med at forsøge at formulere en sådan målrettet og snæver lempelse, der kan styrke informationsdelingen uden at gå på kompromis med andre hensyn.