Politik til forebyggelse af hvidvask og terrorfinansiering
For
Secure Spectrum MidtVest ApS
(Selskabet)

17. februar 2023

Version: nr. 1

1. Indledning og formål

Secure Spectrum MidtVest ApS ("Selskabet") er underlagt forpligtelser om kundekendskab, monitorering og underretning af mistænkelige transaktioner i Lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme. For at sikre efterlevelse heraf har Selskabet godkendt nærværende politik. For at sikre overholdelse af politikken, er der udarbejdet en underliggende forretningsgang på området, som løbende justeres i forhold til det aktuelle risikobillede og eventuelle ændringer af relevant lovgivning.

Denne politik er udarbejdet for at mitigere de risici, som er identificeret i den årlige vurdering af risikoen for, at Selskabet via udbudte produkter kan blive misbrugt i forbindelse med hvidvask samt finansiering af terror ('Risikovurdering - hvidvask og finansiering af terror'). Derudover er den supranationale risikovurdering for hvidvask og terrorfinansiering, den nationale risikovurdering for hvidvask 2022, samt den nationale risikovurdering for terrorfinansiering 2019 også inddraget som baggrund for nogle af de tiltag, der er foretaget.

Denne politik vil, sammen med risikovurderingen og de underliggende procedurer, blive evalueret, når der sker ændringer i udbuddet af produkter, kundesammensætningen, ændringer i ekstern regulering, eller der på andre måder opstår behov for en revurdering af Selskabets arbejde med foranstaltninger mod hvidvask og terrorfinansiering. Dog vil politikken som minimum blive godkendt af direktionen én gang om året sammen med en opdateret risikovurdering.

Det er formålet med denne politik at opstille Selskabets overordnede retningslinjer til at forebygge hvidvask og terrorfinansiering. Politikken afspejler de tiltag, der foretages for at nedbringe den iboende risiko som Selskabet er eksponeret for i relation til hvidvask og terrorfinansiering. Dette gælder blandt andet de muligheder, der foreligger for overvågning af kunders adfærd for at kunne identificere mistænkelig adfærd.

2. Definitioner

I hvidvaskloven er begreberne defineret som følger (lovens §§ 3 og 4):

Ved *'hvidvask'* skal forstås:

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

Ved *'finansieringen af terrorisme'* skal forstås finansiering af terrorisme som defineret i straffelovens § 114b, for så vidt angår handlinger omfattet af § 114 (terrorisme). Det vil sige, hvis en person

4) direkte eller indirekte yder økonomisk støtte til,
5) direkte eller indirekte tilvejebringer eller indsamler midler til eller
6) direkte eller indirekte stiller penge, andre formuegoder eller finansielle eller andre lignende ydelser til rådighed for

en person, en gruppe eller sammenslutning, der begår eller har til hensigt at begå handlinger omfattet af §114 eller §114 a.

Ved *'aktuelt risikobillede'* og *'iboende risiko'* menes den risiko, der er for, at Selskabet kan blive misbrugt til hvidvask eller terrorfinansiering, før foranstaltninger (skriftlige arbejdsprocesbeskrivelser, interne kontroller og organisatorisk ansvarsfordeling) til imødegåelse heraf er implementeret.

3. Overordnet strategisk mål

Direktionens overordnede strategiske mål er at nedbringe Selskabets risiko for at blive misbrugt til Hvidvask og terrorfinansiering.

Dette indebærer, at Selskabet skal:

- Kende sin kunde,
- Opbevare kundens oplysninger, og
- Overvåge kundens aktiviteter

4. Risikostyring for forebyggelse af hvidvask og terrorfinansiering

Selskabet arbejder aktivt med risikostyring, og risikovurderingen opdateres løbende, så den til enhver tid afspejler Selskabets aktuelle risikoprofil. Dog skal risikovurderingen som minimum opdateres én gang om året.

Risikovurderingen foretages med udgangspunkt i Selskabets forretningsmodel og skal klarlægge, hvilke forretningsområder i Selskabet, som er eksponeret for hvidvask- og/eller terrorfinansieringsrisici, hvor store disse risici er, og hvordan de kan manifestere sig.

Med en forretningsmodel menes i denne forbindelse en kombination af:

1) Kundetyper
2) Produkter, tjenesteydelser og transaktioner, som Selskabet udbyder
3) Geografiske områder, hvor forretningsaktiviteterne udøves
4) Leveringskanaler
5) Selskabets organisation

4.1 Risikoappetit

Selskabet ønsker som udgangspunkt kunder med lav og mellem risiko.

For at begrænse Selskabets risiko for at blive misbrugt til hvidvask og terrorfinansiering ønskes der kun højrisikokunder i et begrænset omfang, og sådanne skal altid godkendes af direktøren, forud for indgåelse af kundeforholdet.

Selskabets kunder er privatpersoner såvel som juridiske enheder.

Nedenstående er en negativ afgræsning af, hvilke kunder Selskabet som udgangspunkt ikke ønsker. Listen er ikke udtømmende:

- Udenlandske kunder
- Kunder, hvormed kundeforholdet kræver andre ydelser, der ikke kan relateres til Selskabets kerneydelse i form af investeringsrådgivning og formueforvaltning.
- Kunder, der forud for kundeforholdets indgåelse, ikke vil udlevere de oplysninger, der efterspørges, som en del af kundekendskabsproceduren.
- Kunder, der ikke kan redegøre for oprindelsen af deres formue og midler.
- Kunder, der har nær tilknytning til lande, der fremgår af FATF's grå eller sorte liste.
- Kunder, der optræder på EU's sanktionsliste.

Ovenstående negative afgrænsning er ved etablering af kundeforhold. En situation, hvor en eksisterende kunde, i løbet af kundeforholdet, bliver en af ovenstående er behandlet i afsnit 4.2.2.

4.2 Foranstaltninger

Med udgangspunkt i risikovurderingen skal Selskabet indføre følgende foranstaltninger til forebyggelse af risikoen for hvidvask og terrorfinansiering:

- Skriftlige interne procedurer, herunder kundekendskabsprocedurer
- Overvågning af kundeforhold
- Organisatorisk ansvarsfordeling
- Interne kontroller

4.2.1 Skriftlige interne procedurer

Selskabets direktion har besluttet denne politik med udgangspunkt i risikovurderingen. Selskabets direktion er ansvarlig for, at principperne i denne politik udmøntes i konkrete forretningsgange til brug for Selskabet, for derved at begrænse risikoen for hvidvask og terrorfinansiering. Det indebærer, at Selskabet har udarbejdet en forretningsgang, der fastsætter krav og behandler følgende områder:

- Hvidvaskprocedurer ved etablering af kundeforhold
- Hvidvaskprocedurer ved løbende overvågning
- Politisk eksponeret person
- Midlernes oprindelse
- Underretning ved mistanke om hvidvask

4.2.2 Kundekendskab

Selskabets kundekendskabsprocedure skal basere sig på en risikobaseret tilgang, hvor alle kunder risikoklassificeres, sådan at selskabet bliver yderligere oplyst om kundeforholdet i takt med, at risikoen vurderes højere.

Selskabet skal **identificere** og **legitimere** samtlige af selskabets kunder for at begrænse risikoen for, at der anvendes forfalsket legitimation, og i sidste ende at kunderne ikke er dem, som de giver sig ud for. Derudover skal Selskabet løbende **klarlægge formålet med kundeforholdet** og kundeforholdets forventede forretningsomfang, herunder oplysninger om midlernes oprindelse.

For kunder, der er juridiske enheder, indebærer det, at Selskabet skal klarlægge ejer- og kontrolstrukturen og den juridiske enheds reelle ejere. Reelle ejere skal legitimeres i samme omfang som kunden. Hvis kunden identificeres som en politisk eksponeret person (PEP) eller er nærtstående med en sådan, skal Selskabets hvidvaskansvarlige, samt Selskabets direktør godkende kundeforholdet forud for etablering.

Kundekendskabsproceduren er afgørende for at nedbringe risikoen for, at Selskabet bliver misbrugt til hvidvask og terrorfinansiering. Selskabet ønsker ikke at etablere kundeforhold med kunder, hvor der ikke kan ske tilfredsstillende legitimering af kunden. Kundekendskabsproceduren skal være gennemført inden kundeforholdet kan begynde. Hvis der identificeres mangler i legitimering af etablerede kundeforhold, skal nødvendige oplysninger indhentes inden for 3 måneder. Er manglerne ikke udbedret inden for 3 måneder, skal kundeforholdet ophøre.

Midlernes oprindelse klarlægges og sandsynliggøres som en del af kundekendskabsproceduren, før der indgås et kundeforhold. Ønsker en eksisterende kunde at øge sit mandat, eller foretage en ny alternativ investering for midler, der ved kundeforholdets opstart ikke er sandsynliggjort, og kan kunden ikke redegøre for, hvor midlerne stammer fra, skal Selskabet afvise at forøge kundens mandat eller afvise, at kunden foretager en ny alternative investering.

Såfremt en eksisterende kunde i løbet af kundeforholdet flytter til udlandet, får en nær tilknytning til et land, der optræder på FATF's grå eller sorte liste, eller kunden pludselig optræder på EU's sanktionsliste skal kundeforholdet ophøre inden for 6 måneder.

4.2.3 Overvågning af kundeforholdet

Selskabet skal have løbende opmærksomhed på eventuelle ændringer i Selskabets kundeforhold, som giver anledning til at gennemføre en ny kundekendskabsprocedure. Sker der ændringer i kundens forhold såsom flytning til udlandet, øgning af mandat, der ikke kan sandsynliggøres, eller andre ændringer, der medfører at kundens risikoklassifikation ændres markant, skal den hvidvaskansvarlige straks underrettes.

Herudover skal der med faste intervaller foretages en ajourføring af kundekendskabet på alle Selskabets kunder. Intervallerne fastlægges ud fra en risikobaseret tilgang, så frekvensen er højere, hvor kundeforholdet vurderes at indebære en højere risiko.
Det betyder, at der ved kunder, der er vurderet som kunder med høj risiko, skal ajourføringen ske en gang hvert 1½ år. Ved kunder med mellem risiko skal ajourføringen ske hvert år, og ved kunder med høj risiko skal ajourføringen ske hvert ½ år.

For de kunder, hvor Selskabet har en kigge-fuldmagt til kundens depotkonto, skal Selskabet, hver måned, undersøge om kunden har foretaget transaktioner, der ligger udenfor kundens aftale med Selskabet.

4.3 Roller og ansvar

Selskabet skal have en effektiv organisatorisk ansvarsfordeling på hvidvask og terrorfinansieringsområdet, som skal styrke målsætningen om at nedbringe risikoen for, at Selskabet bliver misbrugt til hvidvask og terrorfinansiering. Dette skal ske ved at sikre, at

Selskabets politik, forretningsgang og interne kontroller på hvidvaskområdet er effektive og lever op til kravene i hvidvasklovgivningen, og at Selskabet har indgået aftale med en ekstern part om udførelse af kontroller på hvidvaskområdet jf. pkt. 4.3.2.

4.3.1 Den hvidvaskansvarlige

Selskabet har udpeget Selskabets direktør som Selskabets hvidvaskansvarlige.

Den hvidvaskansvarlige er ansvarlig for, at Selskabet har metoder og procedurer, som er egnet til effektiv forebyggelse, begrænsning og styring af risici for hvidvask eller finansiering af terrorisme, og dermed sikre, at Selskabet overholder hvidvasklovgivningen.

Den hvidvaskansvarlige er ansvarlig for følgende opgaver:

- Godkendelse af forretningsgange
- Godkendelse af etablering eller videreførelse af forretningsforbindelser med PEP'ere

4.3.2 Compliance

Selskabet har ikke en selvstændig intern compliancefunktion. Selskabet har uddelegeret compliancekontroller til Secure Spectrum Administration ApS, der ansvarlig for uafhængigt at kontrollere og vurdere, om Selskabets forretningsgang, kontroller og foranstaltninger på området for hvidvask og terrorfinansiering er effektive.

Secure Spectrum Administration ApS er ansvarlig for, at der rapporteres til Selskabet om resultatet af ovenstående kontroller og vurderinger af området for hvidvask og terrorfinansiering.

5. Undersøgelsespligt

Selskabet er forpligtet til at undersøge alle usædvanlige transaktionsmønstre og aktiviteter, der ikke har et klart økonomisk eller påviseligt lovligt formål, f.eks. hvor en transaktion ikke svarer til kundens normale adfærdsmønster, eller hvor Selskabet ikke har viden om, hvorfra kundens midler stammer.

Selskabet har implementeret en række arbejdsprocedurer, der sikrer løbende overvågning af om en kundes adfærd kan betegnes som normal for den konkrete kunde. Dette gøres blandt andet ved at sammenholde den aktuelle adfærd med den for kunden normale adfærd, der er dannet på baggrund af oplysninger om kundens formueforhold, beskæftigelse og boligsituation samt tidligere adfærdsmønstre.

Såfremt Selskabets undersøgelse ikke kan afkræfte en mistanke om et kriminelt forhold, skal der ske underretning jf. afsnit 6.

6. Underretning

Den hvidvaskansvarlige er ansvarlig for, at alle mistænkelige transaktioner bliver underrettet korrekt og umiddelbart efter endt undersøgelse.

Hvis en mistanke om hvidvask og/eller terrorfinansiering ikke kan afkræftes, skal den hvidvaskansvarlige straks underrettes. Den hvidvaskansvarlige skal foretage underretningen til NSK straks efter, at den hvidvaskansvarlige er blevet bekendt med mistanken.

Indberetter den hvidvaskansvarlige ikke en mistænkelig transaktion, skal Direktionen underrettes og foretage indberetningen.

Selskabet fører statistik over, hvornår der indberettes til NSK, herunder hvor mange og hvilke forhold der er tale om. Dette indgår i den løbende rapportering til bestyrelsen.

7. Opbevaringspligt

Selskabet opbevarer kundekendskabsdokumenter i fem år efter ophør af kundeforholdet i henhold til hvidvaskloven § 30.

Transaktionsdata gemmes i 5 år, medmindre kunden har haft en eller flere transaktioner, som har været underrettet til NSK. I disse tilfælde opbevarer Selskabet data i 10 år.

Dokumentationen opbevares med respekt for krav om behandling af persondata.

8. Videregivelse af oplysninger om mistænkelige transaktioner til tredjepart

Videregivelse til tredjemand om oplysninger om mistænkelige transaktioner, hvor der er sket underretning til NSK, må kun ske mellem Selskabet og andre virksomheder, som Selskabet har et fælles kundeforhold med.

Det er en forudsætning, at der mellem Selskabet og virksomheden som oplysningerne videregives til, foreligger en skriftlig samarbejdsaftale, hvori der indgår en forpligtelse om videregivelsen.

9. Kontrol og rapportering

Compliancefunktionen vil stikprøvevis kontrollere, at Selskabets medarbejdere efterlever nærværende politik.
Kontrollens resultater skal indgå i rapporteringen fra compliancefunktionen til direktionen.

10. Opdatering

Direktionen skal mindst én gang årligt, i overensstemmelse med årsplanen, vurdere og eventuelt opdatere nærværende politik.

Alle opdateringer skal godkendes af direktionen.

Godkendt af direktionen i Secure Spectrum MidtVest ApS, den 17. februar 2023.