



# Politik for risikostyring på hvidvask- og terrorområdet

# Politik for risikostyring på hvidvask- og terrorområdet

## 1. Indledning

I medfør af lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme § 8, stk. 1 har bestyrelsen for Sparekassen Sjælland-Fyn A/S (sparekassen) vedtaget følgende politik for risikostyring på hvidvask- og terrorområdet.

Politikken fastlægger sparekassens fokus på hvidvask- og terrorområdet med henblik på effektiv forebyggelse, begrænsning og styring af risici på området. Sparekassens risikoprofil (sandsynlighed for at blive misbrugt) er fastsat i sparekassens risikovurdering.

Politikken for risikostyring på hvidvask- og terrorområdet fastsætter de overordnede strategiske mål i relation til forebyggelse af hvidvask og finansiering af terrorisme med udgangspunkt i risikovurderingen af sparekassens forretningsmodel.

Banken har i den eksterne politik, for at mindske risikoen for at blive misbrugt til hvidvask og/eller afsløre aktuel forretningsstrategi, i forhold til den interne politik undtaget visse former for aktiviteter fra sparekassens risikovurdering og bankens forretningsmodel. Den interne politik er imidlertid altid tilgængelig for relevante myndigheder og relevante interessenter.

## 2. Risici reguleret af denne politik

Ved iboende risiko på hvidvask- og terrorområdet menes den iboende sandsynlighed for, at sparekassen kan blive misbrugt til hvidvask og terrorfinansiering. Denne iboende generelle sandsynlighed for at blive misbrugt, er baseret på både den nationale risikovurdering og den supranationale risikovurdering.

Politikken tager primært udgangspunkt i følgende risikofaktorer, der er forbundet med sparekassens forretningsmodel og hovedelementerne i sparekassens vurdering af den iboende sandsynlighed for at blive misbrugt til hvidvask og terrorfinansiering: kunder, produkter, tjenesteydelser, transaktioner samt leveringskanaler og lande eller geografiske områder. Herudover vurderes øvrige faktorer som påvirker sandsynligheden for at blive misbrugt til hvidvask eller terrorfinansiering.

## 3. Sparekassens risikoprofil (iboende sandsynlighed for misbrug) på hvidvask- og terrorområdet

Det er sparekassens pligt at minimere risikoen for, at sparekassen bliver misbrugt til hvidvask og finansiering af terrorisme. Dette sker via overholdelse af de regler, der er udstedt i medfør af hvidvaskloven, Europa-Parlamentets og Rådets forordning om oplysninger, der skal medsendes om betalere ved pengeoverførsler

samt EU-forordninger indeholdende regler om finansielle sanktioner.

Sparekassens iboende sandsynlighed for at blive misbrugt til hvidvask eller terrorfinansiering er fastsat ud fra risikovurderingen til at være middel/høj for hvidvask og middel for terrorfinansiering.

Delvurderingerne af den iboende sandsynlighed på de enkelte risikofaktorer i risikovurderingen – kunder, produkter, leveringskanaler og geografiske områder – er grundlaget for de udarbejdede arbejdsgange, forretningsgange og de opstillede overvågningsscenarier i systemet til overvågning af kundernes transaktioner.

### 3.1 Kunder

Da sparekassens kunder også består af kundetyper, der ud fra en hvidvask og terrormæssig vurdering kan udgøre en risiko samt det forhold, at sparekassen har enkelte kunder af de typer, der udgør en forøget hvidvaskrisiko, vurderes sparekassens kundesammensætning at give en høj sandsynlighed for både misbrug til hvidvask og terrorfinansiering.

Sparekassen kræver derfor at have kendskab til kunderne, herunder identitet og fyldestgørende information om kundens formål med sparekassen samt tilsigtet beskaffenhed (midlernes

oprindelse mv.) og har derfor stor fokus på Kend din Kunde (KDK) aktiviteter.

Delvurderingerne af den iboende sandsynlighed på de enkelte risikofaktorer i risikovurderingen er sammen med resultatet af sparekassens KDK-aktiviteter – og ud fra kundernes transaktioner – basis for de relevante parametre i sparekassens overvågningssystem til løbende overvågning af kundernes aktiviteter.

Denne overvågning (og løbende opfølgning) sikrer, sammen med konkrete fravalg/afgrænsninger i forretningsmodellen, at sparekassens sandsynlighed for misbrug til hvidvask og terrorfinansiering, sænkes markant og kun efterlader en residualrisiko, der kan accepteres.

### 3.2 Produkter, tjenesteydelser og transaktioner

Identifikation og afgrænsning af risikofaktorer ved sparekassens produkter:

Sparekassens produktpalette består bl.a. af helt traditionelle indlånsprodukter, der både nationalt og supranationalt vurderes samlet at give en middel sandsynlighed for misbrug til hvidvask- og terrorfinansiering. Samtidig sigter sparekassen efter langvarige kunderelationer med helkunder, hvilket er med til at mindske hvidvask- og terrorrisikoen.

Enkelte af standardprodukterne og -tjenesteydelserne – som f.eks. håndtering af kontanter i ATM (sparekassen har ikke kassefunktioner i filialerne) og Private Banking – vurderes dog at give høj sandsynlighed, men denne sandsynlighed imødegås via opsætningen af parametre i det IT baserede transaktionsovervågnings-system og via en øget fokus hos rådgiverne på at sikre, at relevant dokumentation altid er tilstrækkelig ved transaktionerne i hverdagen.

I den nationale og den supranationale risikovurdering vurderes muligheden for anonymitet – både i forhold til hvad der har genereret/ frembragt midlerne og i forhold til hvad midlerne skal bruges til – at være en væsentlig årsag til en øget sandsynlighed for misbrug til hvidvask eller terrorfinansiering og derfor er dette et fokusområde hos rådgiverne i hverdagen.

Det vurderes derfor, at sparekassens produkttyper, tjenesteydelser og transaktioner giver en middel sandsynlighed for at blive misbrugt til både hvidvask og terrorfinansiering.

### 3.3 Leveringskanaler

Identifikation og afgrænsning af risikofaktorer ved sparekassens leveringskanaler:

Det vurderes i sparekassens risikovurdering, at sparekassens leveringskanaler giver øget sandsynlighed for udnyttelse til hvidvask- og terrorfinansiering – især bidrager kundernes mere udbredte brug af selvbetjeningssystemer til denne vurdering. Sparekassen har dog fortsat høj grad af kontakt med kunderne, og dermed mindskes risikoen for misbrug af leveringskanalerne.

Primært vurderes to leveringskanaler – ”Mulighed for distance onboarding” og ”Mulighed for indbetaling via ATM” – i den Nationale og Supranationale risikovurdering at give en høj sandsynlighed for misbrug.

I sparekassen er det imidlertid kun muligt at blive distance onboardet som absolut basiskunde med behørig legitimation, men uden nogen former for produkter eller ydelser, bortset fra det juridiske krav om en basiskonto. Hvis engagementet udvides, kræves den normale kontakt med en rådgiver. Transaktionerne på basiskontoen er samtidigt øjeblikkeligt overvåget af sparekassens IT baserede transaktionsovervågnings-system og som standard, bliver alle nye kunder overvåget skærpet i starten af et kundeforhold.

”Mulighed for indbetaling via ATM” sker under opsyn, da alle ATM’ere er videoovervåget og også her gælder, at transaktionerne er overvåget af sparekassens IT baserede transaktionsovervågnings-system med øget fokus ved kontanthåndtering over en vis størrelse.

Det vurderes i Risikovurderingen, at sparekassens leveringskanaler giver en middel/høj sandsynlighed for misbrug – både i forhold til hvidvask- og terrorfinansiering.

### 3.4 Geografiske områder

Identifikation og afgrænsning af risikofaktorer ved sparekassens geografiske område:

Sparekassens geografiske område for aktivitet vurderes ikke i sig selv at påvirke sparekassens sandsynlighed for udnyttelse til hvidvask- og terrorfinansiering væsentligt.

Dette underbygges af, at sparekassens kunder primært bor i Danmark og i de geografiske områder, hvor sparekassen har filialer. Det vurderes derfor, at sparekassens geografiske område kun giver lav/middel sandsynlighed for udnyttelse til hvidvask- og terrorfinansiering.

## 4. Risikobegrænsende tiltag i forhold til den iboende sandsynlighed for at blive misbrugt til hvidvask og terrorfinansiering

På baggrund af sparekassens risikovurdering – der er baseret på både den nationale og supranationale risikovurdering – og egen intern læring, har sparekassen indført følgende tiltag for at minimere sandsynligheden for udnyttelse til hvidvask- og terrorfinansiering:

### 4.1 Regler, retningslinjer og fravalg i forretningsmodellen

Forretningsgange, der beskriver hvad vi gør – og hvad vi ikke gør (med basis i hvad der øger/mindsker sandsynligheden for misbrug til hvidvask eller terrorfinansiering).

Arbejdsgange, der beskriver hvordan vi gør tingene – processer, instrukser og værktøjer (med basis i hvad der øger/mindsker sandsynligheden for misbrug til hvidvask eller terrorfinansiering).

Desuden har sparekassen fravalgt specifikke brancher og er forbeholdende med at påbegynde kundeforhold med udvalgte brancher, som skal godkendes af Hvidvaskteamet.

### 4.2 Øvrige skriftlige interne forretningsgange

Sparekassen har desuden indført skriftlige interne regler om:

- Kundekendskab
- Opmærksomheds-, undersøgelses- samt noteringspligt
- Underretning til hvidvasksekretariatet
- Opbevaring af registreringer
- Intern kontrol
- Risikovurdering (der er basis for denne politik)
- Risikostyring (der sker på baggrund af denne politik)
- Ledelseskontrol og kommunikation
- Uddannelses- og instruktionsprogrammer for medarbejderne

Disse interne regler er udarbejdet for yderligere at understøtte, at sparekassens iboende sandsynlighed for at blive misbrugt til hvidvask- og terrorfinansiering (fra sparekassens udarbejdede risikovurdering) bliver begrænset/minimeret.

### 4.3 Løbende aktivering af medarbejdernes årvågenhed i hverdagen

Et vigtigt led i sparekassens foranstaltninger for at begrænse/undgå at blive misbrugt til hvidvask eller terrorfinansiering, er medarbejdernes løbende opmærksomhed omkring kunderne og de transaktioner, som kunderne foretager.

Der er tale om en pligt til at være opmærksom, som alle medarbejdere løbende skal iagttage i deres daglige arbejde i forhold til alle kunderne – og denne pligt understøttes løbende, og relevant, af information og uddannelse af medarbejdere.

Information til og uddannelse af medarbejderne foregår både direkte til den enkelte medarbejder i forbindelse med tilbagemelding på kontroller (f.eks. i forbindelse med KDK arbejdet)

og via større møder eller udsendelse af generel information (hvis f.eks. ny læring eller indsigt kræver dette).

Derudover er det et krav for alle medarbejdere, at de regelmæssigt gennemfører sparekassens IT baserede kursusmoduler (er samtidigt en vigtig brik i vedligeholdelsen af medarbejdernes kompetencer på området), der er opdateret med fokus på aktuel viden om begrænsning af sandsynligheden for at blive misbrugt til hvidvask eller terrorfinansiering.

#### 4.4 Løbende overvågning af transaktioner

Grundpillen i sparekassens dedikerede arbejde med at begrænse sandsynligheden for at blive misbrugt til hvidvask og terrorfinansiering er, sammen med medarbejdernes årvågenhed, den løbende monitorering af kundernes transaktioner.

De opstillede overvågningsscenarier i systemet til overvågning af kundernes transaktioner er baseret på informationer fra sparekassens risikovurdering.

Grundlaget for overvågningsscenarierne i overvågningssystemet er imidlertid afvigelser fra normal adfærd, der er beskrevet og i overensstemmelse med det aftalte kundeforhold, og derfor er "Kend din Kunde" processen helt afgørende for at overvågningssystemet leverer relevante alarmer rettidigt.

Det basale KDK-arbejde er derfor standardiseret, optimeret og konstant i fokus i hverdagen – og udsat for løbende kontrol og opfølgning.

#### 4.5 Kontroller

Der er afsat faste ressourcer til kontrol og opfølgning i forhold til KDK arbejdet – og nødvendige korrektioner rapporteres både til den enkelte rådgiver og dennes direkte leder, med regelmæssigt summerede resultatoverblik til områdeledelsen. Disse resultatoverblik er basis for korrigerende handlinger som f.eks. totalkontrol på områder med utilstrækkelig performance.

Alle alarmer fra overvågningssystemet resulterer i vurderinger og evt. nødvendige kontroller af transaktioner og/eller informationer. Ud over dette udføres også andre relevante kontroller på vigtige områder, der fremgår af de enkelte forretningsgange. Når ny viden eller resultatet af den løbende overvågning tilsiger dette, udvælges områder, som gennemgås i en temaundersøgelse.

Det vurderes, at de risikobegrænsende tiltag, der er beskrevet i denne politik (og tager udgangspunkt i sparekassens Risikovurdering), markant har begrænset den iboende risiko for, at sparekassen kan blive misbrugt til hvidvask og finansiering af terrorisme.

#### 5. Residual risiko for sparekassen ved misbrug til hvidvask og terrorfinansiering

Selv om de beskrevne tiltag i afsnit 4 ovenfor vurderes at sænke sandsynligheden for at sparekassen vil blive misbrugt til hvidvask eller terrorfinansiering markant, vil der altid være en resterende residual risiko.

Den residuale risiko skal være mindst mulig i forhold til sparekassens forretningsmodel og samtidigt på et acceptabelt niveau for sparekassen – den risiko vurderes hvert år af

Compliance og Risikostyringsfunktionen på baggrund af sparekassens interne risikomodel, der både inddrager sandsynligheden for at blive misbrugt og et estimat for evt. konsekvenser i risikovurderingen.

Den residuale risiko rapporteres årligt til Direktion og Bestyrelse. Herefter vurderes om den residuale risiko er acceptabel for sparekassen. Konstateres det at niveauet er for højt, skal de begrænsende tiltag, som ovenfor beskrevet, revurderes eller nytænkes.

#### 6. Principper for organisatorisk ansvarsfordeling på hvidvask- og terrorområdet

Det overordnede ansvar for forebyggelse og bekæmpelse af hvidvask og terrorfinansiering samt efterlevelse af finansielle sanktioner er forankret i Hvidvaskteamet. Sparekassens hvidvaskansvarlige jf. hvidvasklovens §7, stk. 2, Susanne Bouman, leder Hvidvaskteamet og refererer til sparekassedirektør Jan Kolbye Jensen.

Jan Kolbye Jensen refererer til direktionsmedlem og adm. direktør Lars Petersson, der ligeledes er hvidvaskansvarligt direktionsmedlem, jf. § 8, stk. 5 i hvidvaskloven.

Den hvidvaskansvarlige har dermed direkte adgang til direktionen, herunder det hvidvaskansvarlige direktionsmedlem og har ligeledes adgang til bestyrelsen.

#### 7. Medarbejderkompetencer

Medarbejderne besidder en faglighed, som sætter den enkelte medarbejder i stand til på kvalificeret vis at håndtere det aktive arbejde med at begrænse sparekassens sandsynlighed

for at blive misbrugt til hvidvask eller terrorfinansiering inden for deres faglige områder.

Kvalifikationerne afspejler indholdet af den konkrete jobfunktion og kan hidrøre fra uddannelse, særligt branchekendskab og erhvervs erfaring i øvrigt.

Dette område udvikler sig imidlertid konstant og derfor modtager sparekassens medarbejdere regelmæssigt undervisning i både kravene i hvidvaskloven og aktuel ny viden på området. Dermed arbejdes der aktivt på at fastholde kompetencerne, så de modsvarer aktuelle trusler på området.

#### 8. Rapportering

Hvidvask afdelingen rapporterer til direktion, bestyrelse og finanstilsyn mindst en gang om året eller når det kræves/er relevant ved identificerede nye hvidvaskrisici, advarsler og/eller andre betæneligheder, hvor hvidvaskrisikoen vurderes at være meget høj.

#### 9. Opfølgning og godkendelse

Den hvidvaskansvarlige vurderer politikken mindst en gang årligt og foretager de nødvendige tilpasninger, hvorefter politikken forelægges direktionen inden endelig godkendelse af bestyrelsen. Tilpasningerne kan ske oftere hvis relevant – f.eks. ved markante konsekvenser af ændringer i den nationale eller supranationale risikovurdering.

Godkendt af bestyrelsen.

**For mere information besøg venligst [spks.dk](http://spks.dk)**

