Spillemyndigheden

Spillemyndighedens vejledning om forebyggelse af hvidvask og terrorfinansiering

Hvidvaskvejledning

Version 1.4 31. maj 2024

Indholdsfortegnelse

Versionshistorik

Version 1.0 af den 14. august 2019

- Første version af vejledningen.

Version 1.1 af den 10. januar 2020

- Afsnit 2.5: Indføjelse af bemærkning om, at Spillemyndigheden ikke fører tilsyn med overholdelsen af hvidvasklovens § 36.
- Afsnit 2.5.4: Indføjelse af nyt afsnit om Spillemyndighedens ret til at afvise etablering af eller fastsætte regler om særlige betingelser for datterselskaber, filialer eller repræsentationskontorer i Danmark.
- Afsnit 2.5.5: Indføjelse af nyt afsnit om Spillemyndighedens pligt til at give generel feedback til Hvidvasksekretariatet.
- Afsnit 5.1: Indføjelse af et nyt afsnit om spiludbyderens ansvar for at meddele og indlevere oplysninger til Spillemyndigheden, hvis denne ønsker at etablere en filial eller et repræsentationskontor i et højrisikotredjeland.
- Afsnit 6.2.2: Uddybende beskrivelse af, hvad der forstås ved en "pålidelig og uafhængig kilde".
- Afsnit 6.5.1.4: Indføjelse af bemærkning for landbaserede kasinoer og forhandlere af landbaserede væddemål om skærpede kundekendskabsprocedurer for kunder med hjemsted i et højrisikotredjeland.
- Afsnit 6.6.1.4: Indføjelse af bemærkning for forhandlere af landbaserede væddemål om skærpede kundekendskabsprocedurer for kunder med hjemsted i et højrisikotredjeland.
- Afsnit 8.1 og 8.2: Indføjelse af ny § 25, stk. 1 og 2. Nuværende stk. 2 og 3 bliver herefter stk. 3 og 4.

Version 1.2 af den 2. juni 2022

- Relevante lovhenvisninger er opdateret.
- Alle steder, hvor SØIK har været nævnt, er nu rettet til enten NSK eller Hvidvasksekretariatet.
- Nyt afsnit 2.1.2 om hvidvaskpakken i EU.
- Afsnit 2.5.2 om Spillemyndighedens tilsyn er opdateret.
- Afsnit 6.7.5.1 er uddybet i forhold til skærpede overvågningskrav af PEP'er, nærtstående og nære samarbejdspartnere.
- Afsnit 8.3.5 om berostillelse af transaktioner. Her er der indsat et afsnit om den nye § 26, stk. 4, i hvidvaskloven.
- Nyt afsnit 9.1.4, om i hvor lang tid oplysninger skal opbevares. De hidtidige afsnit 9.1.4 og 9.1.5 er dermed blevet til 9.1.5 og 9.1.6.
- Nyt afsnit 11.3.3. om videregivelse af oplysninger til et operativt samarbejdsforum.
- Der er indsat fodnoter i de relevante afsnit med information om, at adressekravet udgår af bekendtgørelse om onlinekasino og bekendtgørelse om online væddemål pr. 1. juli 2022.
- Enkelte andre afsnit er uddybet med henblik på at skabe en øget forståelse.

Version 1.3 af den 14. juli 2023

- Afsnit 2.2.2 om bekendtgørelser er opdateret fsva. pkt. 2, 3 og 4.
- Afsnit 2.3.1. om nationale risikovurderinger er opdateret med nyeste version.
- Afsnit 2.3.2. om supranationale risikovurderinger er opdateret med nyeste version.
- Afsnit 3.2.3 om landbaseret væddemål er uddybet fsva. egne forhandlere og eksterne forhandlere
- Afsnit 5.2 om undervisning er opdateret og uddybet.
- Afsnit 7.2.4 om outsourcing er opdateret og uddybet.
- Afsnit 8.3.3 er opdateret med den nyeste bekendtgørelse.
- Der er rettet i de relevante afsnit, hvor adressekravet er nævnt, da adressekravet er udgået fra bekendtgørelse om onlinekasino og bekendtgørelse om online væddemål pr. 1. juli 2022.

Version 1.4 af den 31. maj 2024

- Generel opdatering af sproglige formuleringer og opsætning i alle afsnit.
- Alle steder, hvor begrebet 'fast forretningsforbindelse' har været benyttet, er erstattet med begrebet 'forretningsforbindelse'.
- Alle steder, hvor begrebet 'lejlighedsvise kunder' har været benyttet, er erstattet med begrebet 'enkeltstående transaktioner'.
- Alle steder, hvor begrebet 'spiller' og 'gæst' har været benyttet, er erstattet med begrebet 'kunde'.
- Afsnit 2 om regulering er kortet ned.
- Afsnit 3 om risikovurdering er opdateret og uddybet.
- Afsnit 4 om politikker, forretningsgange og kontroller er opdateret og uddybet.
- Afsnit 6 om kundekendskabsprocedurer og opdateret og uddybet.
- Afsnit 7.3 om outsourcing er opdateret og uddybet.
- Afsnit 8 om undersøgelsesforpligtelsen er uddybet.
- Der er indsat et nyt afsnit 9, hvor underretningsforpligtelsen, som før fremgik af afsnit 8, behandles særskilt. Indholdet er samtidig opdateret. De tidligere afsnit 9-10 er derfor afsnit 10-11.
- De tidligere afsnit 2.5 om Spillemyndigheden som tilsynsmyndighed, afsnit 11.3 om Spillemyndighedens tavshedspligt og afsnit 12 om reaktioner for manglende overholdelse af hvidvaskloven, er flyttet til en ny vejledning om Spillemyndighedens hvidvasktilsyn.
- Det tidligere afsnit 11.1 og 11.2 om spiludbyderens tavshedspligt er flyttet til afsnit 13.
- Der er indsat et nyt afsnit 12, hvor finansielle sanktioner, som før fremgik af afsnit 2.5, behandles.

Spillemyndigheden gør opmærksom på, at det er den danske udgave af hvidvaskvejledningen, der har forrang, hvis der måtte opstå fortolkningstvivl i forhold til den engelske udgave.

Indledning

1

1.1 Indledning

Denne vejledning henvender sig til spiludbydere, deres medarbejdere og andre relevante interessenter. Vejledningen er et supplement til Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme (hvidvaskloven)[1], og det anbefales derfor, at spiludbydere orienterer sig i denne vejledning for uddybende oplysninger om konkrete forhold.

Reglerne på spilområdet om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme skal medvirke til bekæmpelse af kriminalitet ved at:

- begrænse mulighederne for misbrug af spilbranchen til hvidvask af penge og finansiering af terrorisme
- lette politiets efterforskning af kriminalitet, samt
- hindre tilbageførelsen af kriminelt udbytte i den legitime samfundsøkonomi.

Denne vejledning indeholder retningslinjer for og fortolkningsbidrag til, hvordan reglerne i hvidvaskloven skal opfyldes af spiludbydere. På de områder, hvor det er overladt til spiludbyderen at foretage en risikovurdering, indeholder vejledningen anvisninger på, hvordan reglerne kan opfyldes.

Reglerne om forebyggende foranstaltninger mod hvidvask og terrorfinansiering er risikobaserede. Den risikobaserede regulering i hvidvaskloven sikrer grundlaget for, at spiludbyderen målrettet og effektivt kan fokusere sin indsats på områder, hvor risikoen for hvidvask og terrorfinansiering er størst.

En risikobaseret tilgang kræver, at spiludbyderen har en god forståelse for de risici, der er ved spiludbyderens virksomhed, og at spiludbyderen er i stand til at udøve sund dømmekraft. Dette kræver opbygning af ekspertise, fx gennem uddannelse, vejledning, professionel rådgivning og "learning by doing".

Denne vejledning er opdelt i emner og følger systematikken fra hvidvaskloven. Reglerne i hvidvaskloven gælder for alle typer af udbud af spil, der er fuldt ud omfattet af hvidvaskloven. Der kan dog være tilfælde, hvor der gælder noget særligt for et specifikt udbud, fx landbaserede væddemål. I sådanne tilfælde, vil der være indsat et afsnit, der udelukkende relaterer sig til dette udbud.

1.2 Hvad er hvidvask?

Hvidvasklovens § 3 indeholder en definition af, hvad der forstås ved hvidvask:

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

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

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

[1] Finanstilsynet – Regler for hvidvask – nr. 2

§ 290

For hæleri straffes med bøde eller fængsel indtil 1 år og 6 måneder den, som uberettiget modtager eller skaffer sig eller andre del i udbytte, der er opnået ved en strafbar lovovertrædelse, og den, der uberettiget ved at skjule, opbevare, transportere, hjælpe til afhændelse eller på lignende måde efterfølgende virker til at sikre en anden udbyttet af en strafbar lovovertrædelse.

Stk. 2. Straffen kan stige til fængsel i 6 år, når hæleriet er af særligt grov beskaffenhed navnlig på grund af forbrydelsens erhvervsmæssige eller professionelle karakter eller som følge af den opnåede eller tilsigtede vinding, eller når et større antal forbrydelser er begået.

Stk. 3. Straf efter denne bestemmelse kan ikke pålægges den, som modtager udbytte til sædvanligt underhold fra familiemedlemmer eller samlever, eller den, der modtager udbytte som normalt vederlag for sædvanlige forbrugsvarer, brugsting eller tjenester.

§ 290 a

For hvidvask straffes med bøde eller fængsel indtil 1 år og 6 måneder den, der konverterer eller overfører penge, som direkte eller indirekte er udbytte af en strafbar lovovertrædelse, for at skjule eller tilsløre den ulovlige oprindelse.

Stk. 2. Straffen kan stige til fængsel i 8 år, når hvidvasken er af særligt grov beskaffenhed navnlig på grund af forbrydelsens erhvervsmæssige eller professionelle karakter eller som følge af den opnåede eller tilsigtede vinding, eller når et større antal forbrydelser er begået.

1.3 Hvad er terrorfinansiering?

Finansiering af terrorisme defineres ligeledes i hvidvaskloven.

Hvidvasklovens § 4 indeholder en definition af, hvad der forstås ved finansiering af terrorisme

1. Ved finansiering af terrorisme forstås i denne lov finansiering af terrorisme som defineret i straffelovens § 114 b, for så vidt angår handlinger omfattet af straffelovens § 114.

Definitionen er overensstemmende med definitionen af terrorisme i straffelovens § 114 b, for så vidt angår handlinger, der er omfattet af straffelovens § 114.

§ 114 b

Med fængsel indtil 12 år straffes den, som

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

Regulering

2

2.1 Financial Action Task Force

Financial Action Task Force (FATF) er en verdensomspændende organisation bestående af mere end 200 lande og jurisdiktioner, der har forpligtet sig til at lade deres respektive indsats mod hvidvask, terrorfinansiering og proliferationsfinansiering blive evalueret af assessorer understøttet af FATF's sekretariat, som er beliggende i Paris. Danmark har været medlem siden 1991.

FATF har vedtaget 40 anbefalinger om forebyggelse og bekæmpelse af hvidvask og terrorfinansiering. Som medlemsland er Danmark forpligtet til at efterleve FATF's 40 anbefalinger.

2.2 EU-regler

2.2.1 Hvidvaskdirektiver

EU-Kommissionen er særskilt medlem af FATF. Det medfører indirekte, at alle EU-lande skal gennemføre FATF's anbefalinger.

Reglerne om forebyggelse af hvidvask og terrorfinansiering er løbende udvidet og revideret siden fremsættelsen af det 1. hvidvaskdirektiv i 1991.

Hvidvaskdirektiver indtil nu

1. hvidvaskdirektiv af 10. juni 1991
2. hvidvaskdirektiv af 4. december 2001
3. hvidvaskdirektiv af 26. oktober 2005
4. hvidvaskdirektiv af 20. maj 2015
5. hvidvaskdirektiv af 30. maj 2018

For flere informationer om fremtidige EU-lovgivning henvises til Finanstilsynets hjemmeside.

2.3 Lovgrundlag

2.3.1 Hvidvaskloven

Denne vejledning bygger på lovbekendtgørelse nr. 316 af 11. marts 2022 om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme (hvidvaskloven) med senere ændringer.

Loven er en gennemførelse af 4. og 5. hvidvaskdirektiv. Loven gennemfører også dele af de internationale standarder fra Financial Action Task Force (FATF) fra 2012 med senere ændringer.

2.3.2 Bekendtgørelser

I medfør af hvidvaskloven er der blandt andet udstedt følgende bekendtgørelser:

1. Bekendtgørelse nr. 727 af 9. juni 2017 om delvis undtagelse af visse spil fra hvidvaskloven. Se nærmere i afsnit 2.6 om delvis undtagelse af visse spil.
2. Bekendtgørelsen nr. 657 af 26. maj 2023 om indsendelse af underretninger m.v. til Hvidvasksekretariatet. Se nærmere i afsnit 9 om underretningspligt.

3. Bekendtgørelse nr. 658 af 30. maj 2023 om indberetning og offentliggørelse af oplysninger om indenlandske politisk eksponerede personer. Se nærmere i afsnit 6.5.3 om politisk eksponerede personer (PEP'er).
4. Bekendtgørelse nr. 431 af 11. april 2023 om transaktioner omfattet af fast track-ordningen fra hvidvaskunderretninger.

2.4 Nationale og supranationale risikovurderinger

Der bliver udgivet både nationale og supranationale risikovurderinger. Spiludbyderen skal inddrage disse i den risikovurdering, som spiludbyderen skal udarbejde med udgangspunkt i virksomhedens forretningsmodel.

2.4.1 Nationale risikovurderinger

Hvidvasksekretariatet udgiver en national risikovurdering i relation til hvidvask. Vurderingen beskæftiger sig med og udpeger særlig risikobetonede områder i alle forpligtede sektorer. Den seneste risikovurdering findes som et link på Spillemyndighedens hjemmeside under afsnittet om "Bekæmpelse af hvidvask".

Politiets Efterretningstjeneste (PET) udarbejder tilsvarende en national risikovurdering i relation til terrorfinansiering. Den seneste risikovurdering er ligeledes tilgængelig som et link fra Spillemyndighedens hjemmeside under afsnittet "Bekæmpelse af hvidvask".

2.4.2 Supranationale risikovurderinger

EU-Kommissionen udgiver en supranational risikovurdering. Risikovurderingen identificerer, analyserer og evaluerer hvidvask- og terrorfinansieringsrisici, som påvirker det indre marked og relaterer sig til grænseoverskridende aktiviteter på panunionsniveau. Risikovurderingen indeholder de vigtigste risici for det indre marked inden for en bred vifte af sektorer og de horisontale sårbarheder, som kan påvirke sådanne sektorer. På baggrund heraf giver dokumentet et bud på de mitigerende foranstaltninger, der skal følges på EU-plan og nationalt plan for at imødegå disse risici og fremsætter en række anbefalinger til de forskellige forpligtede enheder og myndigheder. Den seneste supranationale risikovurdering er tilgængelig som et link på Spillemyndighedens hjemmeside under afsnittet om "Bekæmpelse af hvidvask".

Se mere om inddragelse af nationale og supranationale risikovurderinger under afsnit 3 om risikovurdering.

2.5 Spil omfattet af hvidvaskloven

Hvidvasklovens § 1, stk. 1, nr. 19, angiver, at udbydere af spil er omfattet af loven, når udbuddet sker erhvervsmæssigt. Det betyder, at alle spil udbudt som følge af spilleloven som udgangspunkt er omfattet.

Forudsætningen om, at spillet skal være udbudt erhvervsmæssigt, betyder, at fx poker udbudt efter lov om offentligt hasardspil i turneringsform (pokerloven) ikke er omfattet af hvidvaskloven.

Det er tillige et krav, at udbyderen er etableret i Danmark for at være omfattet af loven. Spiludbydere med en dansk tilladelse til at udbyde spil anses for at være etableret her i landet og er dermed omfattet af hvidvaskloven[2].

Følgende tilladelsestyper efter spilleloven (spil udbudt i Danmark) er omfattet af hvidvaskloven:

- Væddemål, både landbaseret og online, jf. § 11.
- Landbaserede kasinoer, jf. § 14.
- Onlinekasinoer, jf. § 18.
- Onlinekasino, jf. § 42, stk. 4, jf. § 18 (indtægtsbegrænset tilladelse).
- Væddemål, jf. § 42, stk. 4, jf. § 11 (indtægtsbegrænset tilladelse).

Ligeledes omfattes personer og virksomheder etableret her i landet, som udbyder spil svarende til de spil, som er omfattet af spillelovens § 11, § 14, § 18 og § 42, stk. 4, men hvor udbuddet ikke er rettet imod Danmark.

2.6 Delvis undtagelse af visse spil

Hvidvasklovens § 1, stk. 7

Hvidvasklovens § 1, stk. 7, indeholder en mulighed for, at skatteministeren kan undtage spil, enten helt eller delvist fra hvidvaskloven, hvis spillet er vurderet til at udgøre en begrænset risiko for at blive misbrugt til hvidvask eller finansiering af terrorisme. Muligheden kan dog ikke anvendes til at undtage kasinoer fra hvidvaskloven.

Hjemlen er udnyttet[3] til delvist at undtage følgende spil i spilleloven:

- Lotterier udbudt i henhold til § 6.
- Klasselotterier udbudt i henhold til § 8.
- Almennyttige lotterier udbudt i henhold til § 10.
- Lokale puljevæddemål udbudt i henhold til § 13.
- Gevinstgivende spilleautomater udbudt i henhold til § 19.
- Managerspil udbudt i henhold til § 11 og § 42, stk. 4 og 5.
- Spil udbudt i henhold til §§ 9-15 i bekendtgørelse om offentlige forlystelser.
- Konkurrencer, hvor deltagelse sker ved afsendelse af SMS eller lignende.
- Onlinebingo udbudt via fjernsyn.

Ovenstående spil, som er delvist undtaget fra hvidvaskloven, er dermed ikke omfattet af en lang række af hvidvasklovens forpligtelser. Spiludbyderen er dog omfattet af underretningsforpligtelsen efter hvidvasklovens § 26, stk. 1, stk. 3, 1. og 3 pkt., stk. 4-6, samt § 36, stk. 2-4, § 37 og § 38, stk. 1 og 2.

Selvom langt de fleste krav i hvidvaskloven om fx kundekendskabsprocedurer, undersøgelses- og noteringspligt ikke gælder for disse udbud af spil, er spiludbyderen stadig forpligtet til at underrette Hvidvasksekretariatet, hvis spiludbyderen i forbindelse med udbud af spil får viden eller mistanke om hvidvask eller terrorfinansiering.

Det betyder, at Spillemyndigheden også kan føre tilsyn med disse spiludbyderes overholdelse af de forpligtelser, som de er underlagt i henhold til loven.

Se nærmere om Spillemyndighedens tilsynskompetence i vejledning om Spillemyndighedens hvidvasktilsyn.
Der henvises derudover til afsnit 9 for nærmere oplysninger om spiludbyderens underretningsforpligtelse.

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

[3] Se bekendtgørelse nr. 727 af 9. juni 2017 om delvis undtagelse af visse spil fra hvidvaskloven

Risikovurdering

3

3.1 Introduktion

Hvidvasklovens § 7

Spiludbyderen skal identificere og vurdere risikoen for, at spiludbyderens virksomhed kan blive misbrugt til hvidvask og terrorfinansiering. Spiludbyderens risikovurdering skal foretages med udgangspunkt i spiludbyderens konkrete forretningsmodel. Det fremgår af hvidvasklovens § 7, stk. 1.

Formålet med risikovurderingen er, at spiludbyderen skal have et anvendeligt værktøj, der giver spiludbyderen et overblik over og en forståelse for, hvor og i hvilket omfang spiludbyderen er udsat for at blive misbrugt til hvidvask eller finansiering af terrorisme, og hvilke tiltag der er nødvendige for at begrænse risiciene herfor.

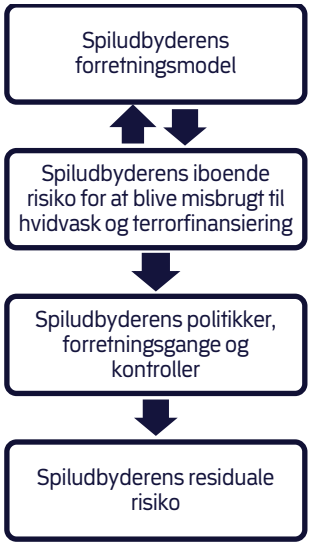
Det bemærkes, at spiludbyderens risikovurdering er en forudsætning for, at spiludbyderens politikker, forretningsgange og kontroller, som er omtalt i kapitel 4, kan anses for at være tilstrækkelige.

I Finanstilsynets hvidvaskvejledning er der anført en model, der illustrerer processen fra konstateringen af spiludbyderens iboende risiko til konstateringen af den risiko, der er tilbage, når spiludbyderen har udarbejdet politikker, forretningsgange og kontroller.[4] Risikoen , der er tilbage, betegnes som den residuale risiko.

Den residuale risiko er udtryk for den risiko, der er tilbage i spiludbyderens virksomhed efter, at spiludbyderen har iværksat mitigerende foranstaltninger med henblik på at begrænse den iboende risiko for, at virksomheden kan blive misbrugt til hvidvask og terrorfinansiering. Den residuale risiko er dermed den risiko, som spiludbyderen løber for at blive misbrugt til hvidvask og terrorfinansiering

En høj iboende risiko i spiludbyderens virksomhed betyder derfor nødvendigvis ikke, at virksomhedens reelle risiko er høj, hvis spiludbyderen effektivt har iværksat begrænsende tiltag, som i sidste ende medfører, at spiludbyderens residuale risiko er lav.

Nedenfor er der angivet en tilsvarende model for ligeledes at illustrere det i denne vejledning.



[4] Finanstilsynets vejledning om lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme (hvidvaskloven), side 25.

Som modellen ovenfor illustrerer, skal spiludbyderen altså først og fremmest kende sin forretningsmodel for at kunne identificere og vurdere, hvilken iboende risiko virksomheden er udsat for i forhold til at blive misbrugt til hvidvask og terrorfinansiering.

Risikoen kan ændres, hvis spiludbyderen ændrer sin forretningsmodel, og der kan således både være tale om en øget eller mindsket risiko som følge deraf.

Spiludbyderens politikker, forretningsgange og kontroller er virksomhedens mitigerende foranstaltninger, dvs. de tiltag, som spiludbyderen iværksætter for at få en effektiv forebyggelse, begrænsning og styring af risici for hvidvask og terrorfinansiering. Spiludbyderen kan fx mitigere sin iboende risiko ved at have effektive skriftlige forretningsgange, som beskriver, hvilke tiltag spiludbyderen har iværksat med henblik på at begrænse risikoen forbundet med forskellige aspekter af spiludbyderens forretningsmodel. Det kan fx være risici forbundet med spiludbyderens kundetyper eller lignende.

3.2 Den iboende risiko

Når spiludbyderen skal risikovurdere sin forretningsmodel, indebærer det, at spiludbyderen skal identificere og vurdere den iboende risiko for, at spiludbyderen kan blive misbrugt til hvidvask og terrorfinansiering. Det betyder, at vurderingen af risikoen skal foretages uden hensyntagen til de mitigerende foranstaltninger, som spiludbyderen har iværksat for at begrænse de identificerede risici.

Spiludbyderen skal derfor i sin risikovurdering fx ikke inddrage det forhold, at spiludbyderen gennemfører kundekendskabsprocedurer eller har iværksat andre mitigerende foranstaltninger.

3.3 Identificering og vurdering af risikofaktorer

Risikovurderingen af spiludbyderens forretningsmodel består af to delelementer – identificering og vurdering af risikofaktorer.

Spiludbyderen skal derfor først og fremmest identificere alle relevante risikofaktorer, som er forbundet med spiludbyderens forretningsmodel. For at spiludbyderen kan identificere de relevante risikofaktorer, som kan have betydning for spiludbyderens risiko for at blive misbrugt til hvidvask og terrorfinansiering, forudsætter det således, at spiludbyderen har foretaget en grundig analyse af sin forretningsmodel og forstår, hvilke sårbarheder udbud af spil har i relation til hvidvask og terrorfinansiering.

Omfanget og indholdet af spiludbyderens risikofaktorer hænger sammen med spiludbyderens art og størrelse, og hvordan spiludbyderen i øvrigt har valgt at tilrettelægge sin forretningsmodel.

Når spiludbyderen skal identificere, hvilke relevante risikofaktorer der kan være forbundet med spiludbyderens forretningsmodel, skal spiludbyderen inddrage den nationale og supranationale risikovurdering og andre relevante kilder.

Det kan være udfordrende for spiludbyderen at gennemskue, hvilke aspekter af spiludbyderens konkrete forretningsmodel, som kan udgøre en risiko i relation til hvidvask og terrorfinansiering. Den nationale og supranationale risikovurdering skal i den sammenhæng understøtte spiludbyderens tilegnelse af viden om konkrete sektorspecifikke risikofaktorer. På samme måde skal andre relevante kilder, som fx denne vejledning, bidrage til, at spiludbyderen identificerer alle relevante risikofaktorer, som er forbundet med spiludbyderens virksomhed.

Når spiludbyderen har identificeret sine iboende risikofaktorer, skal spiludbyderen ud fra en holistisk tilgang vurdere, i hvilket omfang de identificerede risikofaktorer bevirker, at spiludbyderen kan blive misbrugt til hvidvask og terrorfinansiering.

Spiludbyderen har som udgangspunkt metodefrihed til selv at vælge, hvordan vurderingen af de iboende risikofaktorer kommer til udtryk. Spiludbyderen kan fx vælge at vægte de enkelte risikofaktorer for derefter at klassificere dem som enten lav, middel eller høj. Vægtningen af risikofaktorerne kan fx baseres på en vurdering af sandsynlighed og konsekvens. Det betyder, at spiludbyderen i sin vurdering af risikoen for at blive misbrugt til hvidvask og terrorfinansiering kan lægge vægt på, hvilken sandsynlighed der er for, at en bestemt risikofaktor indtræffer, og hvad konsekvensen er, hvis dette er tilfældet.

Det afgørende er, at spiludbyderen har foretaget vurderingen på en sådan måde, at spiludbyderen efterfølgende vil kunne anvende risikovurderingen som et operationelt værktøj til at få en forståelse for, hvor og i hvilket omfang spiludbyderen er udsat for at blive misbrugt til hvidvask og terrorfinansiering. Spiludbyderen kan derefter fokusere sine begrænsende tiltag på de områder, hvor risikoen er størst.

Spiludbyderen skal som nævnt vurdere risikoen ved hver enkelt iboende risikofaktor, som er forbundet med spiludbyderens forretningsmodel. Det er derfor ikke tilstrækkeligt, hvis spiludbyderen alene vurderer den samlede risiko, som fx er forbundet med flere risikofaktorer.

Ved at spiludbyderen vurderer risikoen særskilt ved hver enkelt risikofaktor, får spiludbyderen indsigt i, om spiludbyderens enkelte risikofaktorer udgør henholdsvis en begrænset eller øget risiko for, at spiludbyderen bliver misbrugt til hvidvask og terrorfinansiering.

Spiludbyderens risikovurdering skal forholde sig til risikoen for både hvidvask og terrorfinansiering. Det kan fx være, at et af spiludbyderens spilprodukter udgør en høj iboende risiko for hvidvask men en begrænset risiko for terrorfinansiering.

3.4 Risikofaktorer, der som minimum skal identificeres og vurderes

Spiludbyderens risikovurdering skal som minimum omfatte risikofaktorer, der er forbundet med spiludbyderens kunder, produkter, tjenesteydelser og transaktioner samt leveringskanaler og lande eller geografiske områder. Det fremgår af hvidvasklovens § 7, stk. 1, 2. pkt.

Det betyder, at spiludbyderens risikovurdering ikke kun skal forholde sig til de oplistede områder i bestemmelsen, da risikovurderingen skal afspejle og dække alle dele af spiludbyderens forretningsmodel. Spiludbyderen skal fx også identificere og vurdere den iboende risiko, som kan være forbundet med virksomhedens organisation. Spiludbyderen kan i den forbindelse identificere og vurdere risikoen for, at spiludbyderens egne ansatte medvirker til hvidvask og terrorfinansiering. Det kan også være risici forbundet med fx brug af tredjemandsbistand eller outsourcing.

Omfanget af risikovurderingen afhænger af spiludbyderens konkrete forretningsmodel. Hvis spiludbyderen har en omfattende forretningsmodel, fordi spiludbyderen fx udbyder et stort udvalg af forskellige spilprodukter både online og landbaseret, vil det stille større krav til risikovurderingens indhold og omfang. Spiludbyderens forretningsmodel vil i de tilfælde omfatte flere risikofaktorer, som spiludbyderen skal forholde sig til i relation til hvidvask og terrorfinansiering. Omvendt vil en spiludbyder med en komprimeret og begrænset forretningsmodel være eksponeret for færre risici. Spiludbyderen er uanset størrelse og omfang forpligtet til at foretage en grundig analyse af, hvordan den konkrete forretningsmodel kan blive misbrugt til hvidvask og terrorfinansiering.

3.4.1 Kunder

Risikofaktorer, som er forbundet med spiludbyderens kunder, er en analyse af, hvilke kundetyper spiludbyderen har eller i øvrigt er eksponeret for. Det kan fx være, at spiludbyderen har kunder, som kommer fra et land, der er opført på Europa-Kommissionens liste over højrisikotredjelande, eller som er en politisk eksponeret person (PEP'er). Læs mere om kunder fra højrisikotredjelande og PEP'er under afsnit 6.5.2 og 6.5.3.

Det er spiludbyderens konkrete forretningsmodel, som dikterer, hvilke kundetyper spiludbyderen skal risikovurdere. Hvis spiludbyderen har indrettet sin forretningsmodel på en sådan måde, at spiludbyderen alene accepterer kunder, som har en adresse registreret i Danmark og et dansk cpr-nummer, er spiludbyderen således ikke forpligtet til at identificere og vurdere risikoen forbundet med udenlandske kunder. Spiludbyderen skal dog være opmærksom på, at selvom spiludbyderen alene tillader kunder fra Danmark, så er der stadig en risiko for, at udenlandske kunder forsøger at omgå spiludbyderens begrænsende tiltag. Det kan fx være ved brug af falske dokumenter eller VPN.

Efter dansk spillelovgivning må spiludbyderen alene have fysiske kunder. Spiludbyderens risikovurdering af sine kundetyper skal derfor ikke omfatte virksomheder og reelle ejere.
Når spiludbyderen har identificeret alle sine relevante kundetyper, skal spiludbyderen vurdere risikoen for, at de enkelte kundegrupper misbruger virksomheden til hvidvask og terrorfinansiering.

Risikovurderingen af spiludbyderens kunder efter hvidvasklovens § 7, stk. 1, betyder ikke, at spiludbyderen skal foretage en vurdering af spiludbyderens enkelte kunde. Der er efter hvidvasklovens § 7, stk. 1, alene tale om en vurdering af i hvilket omfang spiludbyderens generelle kundetyper påvirker spiludbyderens iboende risiko for at blive misbrugt til hvidvask og terrorfinansiering. Risikovurderingen af den enkelte kunde hører til den vurdering, som spiludbyderen skal foretage efter hvidvasklovens § 11, som du kan læse mere om under afsnit 6.3.

Når spiludbyderen skal identificere, hvilke kundetyper spiludbyderen har og efterfølgende vurdere risikoen i relation til hvidvask og terrorfinansiering, må spiludbyderen gerne inddrage overordnede oplysninger og erfaringer fra konkrete kunder. Ved at kigge på spiludbyderens konkrete kunder, kan spiludbyderen danne sig et overblik over, hvilke typer af kunder virksomheden har, og om kundernes generelle adfærd har betydning for en bestemt kundegruppes indflydelse på spiludbyderens iboende risiko for at blive misbrugt til hvidvask og terrorfinansiering.

3.4.2 Produkter

Spiludbyderen skal identificere og vurdere risikofaktorer, som er forbundet med spiludbyderens produkter. Spilprodukter, hvor der fx kan foretages store indskud, eller hvor hastigheden af spilproduktets afvikling er høj, kan udgøre faktorer, som kan inddrages i spiludbyderens vurdering.

Spiludbyderen kan også kigge på, om spilproduktet alene beror på tilfældighed, eller om spilproduktet har et element af færdighed, som kan have betydning for spilproduktets tilbagebetalingsprocent. Spilproduktets tilbagebetalingsprocent kan være en faktor, som spiludbyderen kan inddrage i sin risikovurdering.

Spiludbyderen kan derudover kigge på, om spilproduktet giver mulighed for, at kunderne kan spille mod hinanden, og om kunderne også kan spille mod udenlandske kunder. Disse spilprodukter kaldes ofte for peer-to-peer-produkter (P2P-produkter) og kan være en risikofaktor, som spiludbyderen kan inddrage.

Når spiludbyderen har vurderet sine enkelte risikofaktorer, som er forbundet med et specifikt spilprodukt, skal spiludbyderen på baggrund af vurderingen af de enkelte risikofaktorer også vurdere risikoen ved selve produktet.

Eksempel

En spiludbyder udbyder P2P-poker til sine kunder. Spiludbyderen skal først identificere alle de risikofaktorer, som er forbundet med P2P-poker. Spiludbyderen identificerer, at P2P-poker udgør en risiko i relation til hvidvask og terrorfinansiering, da produktet bl.a. muliggør, at der kan ske overførsel af midler mellem kunder. Den omstændig, at der ved P2P-poker sker overførsel af midler, er en risikofaktor, der er forbundet med P2P-poker, og som spiludbyderen skal vurdere risikoen ved. En anden risikofaktor kan fx være, at kunden via P2P-poker kan spille mod kunder fra andre jurisdiktioner. Spiludbyderen skal herefter vurdere de forskellige risikofaktorer enkeltvist. På baggrund af spiludbyderens identificering og vurdering af de forskellige risikofaktorer, der er forbundet med P2P-poker, skal spiludbyderen herefter også foretage en samlet vurdering af risikoen ved P2P-poker som et produkt.

Spiludbyderen skal som udgangspunkt identificere og vurdere risikofaktorer ved alle sine spilprodukter. Hvis spiludbyderen udbyder flere forskellige varianter af et spilprodukt, fx roulette, så skal disse risikovurderes enkeltvist, hvis spilvarianten væsentligt adskiller sig fra spiludbyderens andre spilprodukter. Spiludbyderens forskellige typer af et bestemt produkt adskiller sig væsentligt, hvis varianten fx udbydes live med brug af spiludbyderens personale, varianten giver mulighed for væsentlig større indskud, eller hvis hastigheden af spillets afvikling adskiller sig markant fra spiludbyderens andre typer af produktet. Hvis spiludbyderens forskellige typer af samme produkt alene adskiller sig af kosmetiske grunde, skal spiludbyderen ikke foretage en særskilt risikovurdering.

3.4.3 Transaktioner

Ved risikovurdering af spiludbyderens transaktioner forstås, at spiludbyderen blandt andet skal identificere og vurdere risikofaktorer, som er forbundet med spiludbyderens anvendte betalingsløsninger. Det indebærer, at spiludbyderen skal danne sig et overblik over, hvilke betalingsløsninger kunderne har mulighed for at anvende, når de spiller hos spiludbyderens virksomhed.

Når spiludbyderen skal identificere og vurdere risikofaktorer forbundet med de enkelte betalingsløsninger, kan spiludbyderen fx inddrage det forhold, om betalingsmidlet er egnet til at sløre, hvor midlerne stammer fra, og i hvor høj grad betalingsløsningen kan misbruges af en anden person. Hvis spiludbyderen fx tillader, at kunden kan foretage ind- og udbetalinger til og fra spilkontoen ved brug af betalingskort, som er udstedt af et pengeinstitut, kan spiludbyderne identificere og vurdere risikoen ved, at kunden muligvis anvender et betalingskort, som er stjålet.

Spiludbyderen kan også kigge på, om betalingsløsningen giver mulighed for at gennemføre hurtige og store transaktioner.

Når spiludbyderen har vurderet sine enkelte risikofaktorer, som er forbundet med en specifik betalingsløsning, skal spiludbyderen på baggrund af vurderingen af de enkelte risikofaktorer også vurdere risikoen ved selve betalingsløsningen.

Spiludbyderen skal som udgangspunkt vurdere risikoen ved hver enkelt betalingsløsning, som spiludbyderen anvender. Hvis spiludbyderen anvender flere forskellige e-wallets eller typer af betalingskort, som alle overordnet har de samme karakteristika og ikke i væsentlig grad adskiller sig fra hinanden, behøver spiludbyderen ikke at vurdere risikoen ved hver enkel variant af betalingsløsningen særskilt. I det tilfælde er det tilstrækkeligt, hvis spiludbyderen samlet vurderer risikoen, som er forbundet med typen af betalingsløsning.

3.4.4 Leveringskanaler

Spiludbyderen skal identificere og vurdere risikofaktorer, som er forbundet med spiludbyderens leveringskanaler. Det betyder, at spiludbyderen skal foretage en risikovurdering af den måde, som spiludbyderen vælger at stille sine spilprodukter til rådighed for sine kunder på, og den måde som spiludbyderen i øvrigt har sin kontakt med kunden på.

Det kan fx være, at spiludbyderen stiller sine spilprodukter til rådighed online, eller at spiludbyderen sælger sine spilprodukter fysisk via et landbaseret kasino. Det kan også være, at spiludbyderen sælger sine spilprodukter fysisk ved brug af eksterne og interne forhandlere eller det forhold, at spiludbyderens produkter tilknyttes eller faciliteres via en spilkonto eller en selvbetalingsterminal.

Uanset hvilken forretningsmodel spiludbyderen har, skal spiludbyderen risikovurdere, i hvilket omfang spiludbyderens leveringskanaler har indflydelse på, at spiludbyderens virksomhed misbruges til hvidvask og terrorfinansiering.

3.4.5 Lande og geografiske områder

Spiludbyderen skal identificere og vurdere risikofaktorer, som er forbundet med lande og geografiske områder. De geografiske risici skal blandt andet ses i sammenhæng med spiludbyderens kunder, idet kundetypens tilknytning til en bestemt geografisk lokation kan have indflydelse på kundetypens iboende risiko. Spiludbyderen skal derfor foretage en vurdering af, hvilken risiko forskellige lande udgør i relation til hvidvask og terrorfinansiering.

Til brug for vurderingen kan spiludbyderen fx inddrage, om landet har strategiske mangler i forhold til forebyggelse af hvidvask og terrorfinansiering. I den forbindelse kan det være relevant at inddrage, om landet er på Europa-Kommissionens liste over højrisikotredjelande eller er opført på FATF's grå og sorte lister.

3.5 Dokumentation og brug af relevante kilder

Spiludbyderens risikovurdering skal dokumenteres. Det følger af hvidvasklovens § 7, stk. 1, 3 pkt.

Dokumentationskravet indebærer, at spiludbyderens risikovurdering skal være saglig underbygget ved brug af relevante kilder og data, og at den altså ikke må været baseret på antagelser. De relevante kilder skal dokumentere og understøtte, hvordan spiludbyderen er kommet frem til, at virksomheden har en bestemt iboende risiko for at blive misbrugt til hvidvask og terrorfinansiering.

Det er et krav, at risikovurderingen som minimum skal tage udgangspunkt i den nationale og supranationale risikovurdering. Det er derfor vigtigt, at spiludbyderen har et indgående kendskab til disse. Læs mere herom under afsnit 2.3.1 og 2.3.2. Den nationale og supranationale risikovurdering skal samtidig hjælpe spiludbyderen med at få en forståelse af, hvilke risikofaktorer der fx kan være til stede i spiludbyderens virksomhed. Ved brug af både den nationale og supranationale risikovurdering vil det derfor også være lettere for spiludbyderen at identificere, hvilke risikofaktorer der kan være forbundet med spiludbyderens forretningsmodel.

Spiludbyderens risikovurdering kan også tage udgangspunkt i andre former for dokumentation på området, herunder fx relevante rapporter og typologier, som er udsendt af FATF eller Europa-Kommissionen.

Derudover kan spiludbyderens egne erfaringer og indsamlet data anvendes som dokumentation til risikovurderingen.

Når spiludbyderen fx skal identificere og vurdere risikofaktorer ved et bestemt spilprodukt, skal spiludbyderen således kunne dokumentere, hvorfor spiludbyderen har identificeret forskellige risikofaktorer ved det bestemte produkt, og hvorfor spiludbyderen har tildelt de enkelte risikofaktorer en bestemt vægtning. Spiludbyderen kan fx henvise til, at der i den seneste nationale risikovurdering af hvidvask er anført, at fastoddsvæddemål udgør en risiko i relation til hvidvask, idet kunden kan spille på lave odds. Spiludbyderen kan derefter dokumentere vurderingen af risikoen ved spil til lave odds ved fx at inddrage oplysninger om, hvor mange af spiludbyderens kunder som indgår væddemål på lave odds, og om der fx er foretaget underretning på kunderne. På den måde kan spiludbyderens dokumentere, hvilken indflydelse spil til lave odds har af indflydelse på virksomhedens iboende risiko for at blive misbrugt til hvidvask og terrorfinansiering. Der kan være situationer, hvor spiludbyderen ikke har mulighed for at dokumentere den iboende risiko ved flere forskellige aspekter af sin forretningsmodel. Det kan fx være tilfældet, hvis spiludbyderen lancerer et nyt spilprodukt eller anvender en ny teknologi, som spiludbyderen ikke tidligere har haft erfaring med, og hvor der ikke findes relevante kilder, som kan underbygge risikovurderingen.

Følgende er eksempler på relevante kilder, der med fordel kan inddrages til brug for risikovurderingen:

- FATF's Vulnerabilities of Casinos and Gaming Sector - Rapport om kasinosektoren, hvori risikofaktorer i kasinosektoren specificeres.
- Risk-Based Approach Guidance for prepaid cards, mobile payments and Internet-based payment services – Rapport om risici forbundet med forudbetalte kort, mobile betalinger og internetbaserede betalingsmetoder.

Der er links til ovenstående rapporter på Spillemyndighedens hjemmeside under afsnittet "Bekæmpelse af hvidvask".

3.6 Revision af risikovurdering

Spiludbyderen skal løbende opdatere sin risikovurdering. Det følger af hvidvasklovens § 7, stk. 1, 3 pkt.

For at sikre at risikovurderingen til enhver tid afspejler spiludbyderens aktuelle risikoprofil, skal risikovurderingen som udgangspunkt revideres mindst én gang årligt eller i forbindelse med væsentlige ændringer i spiludbyderens forretningsmodel eller ændringer i lovgivningen.

Spiludbyderen skal også genbesøge sin risikovurdering, hvis der er ændringer i nye nationale og supranationale risikovurderinger, som kan have betydning for spiludbyderens iboende risiko.

En ændring kan være:

- Introduktion af et nyt spilprodukt eller betalingsløsning
- Introduktion af nye leveringskanaler, fx at spiludbyderen vælger at anvende eksterne forhandlere til salg af sine produkter.
- Ændring af hvidvaskloven
- Ny national risikovurdering eller temarapporter fra Hvidvasksekretariatet, som angiver en ændring i risikoen for eksempelvis et bestemt spilprodukt eller kundetype.

3.7 Risikofaktorer

Spiludbyderen er som nævnt forpligtet til at identificere og vurdere samtlige relevante risikofaktorer, som er forbundet med spiludbyderens forretningsmodel.

Nedenfor er der oplistet en række eksempler på risikofaktorer, som kan være iboende i de forskellige typer udbud af spil, herunder for onlinespil, landbaseret kasino og landbaseret væddemål. Det bemærkes, at da der kan være forskel på risikofaktorerne for de enkelte områder, er afsnittene opdelt efter type af udbud: online spil (kasino og væddemål), landbaseret væddemål og landbaseret kasino.

Spiludbyderen skal altid tage udgangspunkt i sin egen konkrete forretningsmodel, når spiludbyderen skal identificere og vurdere risikoen for, at spiludbyderen kan blive misbrugt til hvidvask og terrorfinansiering. Oplistningen skal derfor ikke ses som en facitliste over, hvilke obligatoriske risikofaktorer spiludbyderen altid skal inddrage, da forretningsmodellen kan variere fra virksomhed til virksomhed.

3.7.1 Onlinespil

3.7.1.1 Identifikation af risikofaktorer
Nedenfor er oplistet eksempler på nogle af de risikofaktorer, der kan være til stede ved onlinespil.

Virksomhedens kundetyper

- Politisk eksponerede personer (PEP'er), nærtstående til PEP eller nære samarbejdspartnere til PEP, både indenlandske og udenlandske.
- Kunder fra lande på EU-Kommissionens liste over højrisikotredjelande.
- Kunder fra lande på FATF's sorte og grå lister.
- Kunder, som ikke har fået deres identitet kontrolleret.

Kundeadfærd

- Kunden er tilbageholdende med oplysninger.
- Kunden spiller på væddemål til lave odds.
- Kunden spiller på alle udfald af en begivenhed (hedging).
- Flere forskellige kunder placerer samtidig flere indskud på alle udfald af en bestemt begivenhed.
- Kunden benytter sig ofte af Cash-Out.

Spilprodukter

- Spiludbyderens produktportefølje, fx fastoddsvæddemål og gevinstgivende spilleautomater.
- Spilproduktet udbydes live med brug af spiludbyderens personale, fx live-roulette.
- Spilproduktets afviklingshastighed.
- Spilproduktets tilbagebetalingsprocent.
- Spilproduktet giver mulighed for, at kunder kan spille mod hinanden (P2P-produkter fx udbud af væddemålsbørs og poker.)
- Spilproduktets indskudsgrænse.
- Spilproduktet giver mulighed for Cash-Out.

Leveringskanaler

- Onlineudbud via webdomæne.
- Onlineudbud via app.
- Udbud af spil ved brug af flere webdomæner.

- Ingen fysisk kontakt med kunden ved oprettelse af spilkontoen.
- Ingen fysisk kontakt med kunden ved ind- og udbetalinger til spilkontoen.
- Ingen fysisk kontakt med kunden ved indskud på spilprodukter.

Transaktioner

- Ændring i kundens sædvanlige forbrugsmønster.
- Ind- og udbetaling af store beløb til og fra kundens spilkonto.
- Ind- og udbetaling af en række sammenhængende småbeløb, som til sammen udgør store transaktioner (structuring).
- Ind- og udbetaling af beløb til og fra spilkontoen uden væsentlig spilaktivitet.
- Oprettelse af flere spilkonti inden for et kort tidsrum og fra samme IP-adresse.
- Oprettelse af flere midlertidige spilkonti.
- Opbevaring af store beløb på spilkontoen uden spilaktivitet.

Betalingsløsninger

- Spiludbyderens forskellige betalingsløsninger, fx betalingskort, e-wallets og forudbetalte kort.
- Betalingsløsninger, som i mindre grad er sporbare.
- Betalingsløsninger, som er egnet til at sløre, hvor midlerne stammer fra.
- Betalingsløsninger, som kan misbruges.
- Betalingsløsninger, som kan finansieres med kontanter.
- Betalingsløsninger, som giver mulighed for at gennemføre hurtige og store ind- og udbetalinger til og fra spilkontoen.
- Flere betalingskort tilknyttet samme spilkonto.
- Brug af flere forskellige betalingskort til ind- og udbetalinger til og fra spilkontoen.
- Hyppige skift i brugen af betalingsløsninger.

Geografiske risici

- Usædvanligt skift af IP-adresse ved log-in på spilkonto.
- Log-in via IP-adresse, som er tilknyttet lande, som udgør en øget risiko.

Andre relevante risikofaktorer

- Spiludbyderens ansatte medvirker til hvidvask.
- Spiludbyderens ansatte følger bevidst ikke spiludbyderens forretningsgange.
- Spiludbyderens ansatte er ikke i tilstrækkelig grad uddannet i hvidvasklovens krav.
- Spiludbyderens væddemål misbruges til hvidvask forbundet med matchfixing

Nedenfor er en uddybning af nogle af de ovenstående risikofaktorer.

Bemærk, at nogle af de oplistede risikofaktorer er behandlet samlet.

3.7.1.2 Politisk eksponerede personer, nærtstående og nære samarbejdspartnere

Politisk eksponerede personer (PEP'er) er personer, som bestrider et særligt offentligt tillidshverv. På grund af PEP'ens særlige position og indflydelse i samfundet er der en risiko for, at

persongruppens embede kan misbruges til hvidvask af kriminelt udbytte. Der er derudover en øget risiko for, at PEP'ens midler stammer fra enten korruption eller bestikkelse, og som gennem spil kan komme til at fremstå som legale spilgevinster.

Kategorien PEP'er omfatter flere forskellige kundetyper, som hver især kan udgøre en særskilt iboende risiko for hvidvask og terrorfinansiering. Udenlandske PEP'er fra lande, som fx har et højt korruptionsniveau, eller som har strategiske mangler i forhold til forebyggelse af hvidvask og terrorfinansiering, vil ofte udgøre en højere iboende risiko sammenlignet med en indenlandsk PEP, hvor virksomhedens forretningsmodel i mindre grad vil være eksponeret for hvidvask og terrorfinansiering.

For nærmere information og definition af PEP, nærtstående og nære samarbejdspartnere henvises til afsnit 6.5.3.

3.7.1.3 Kunder, som ikke har fået deres identitet kontrolleret
Hvis spiludbyderen har indrettet sin forretningsmodel på en sådan måde, at der er mulighed for, at kundens identitetsoplysninger først bliver kontrolleret op til 30 dage efter oprettelsen af en spilkonto, udgør denne kundetype en risiko. Kunder, som ikke har fået deres identitet kontrolleret, udgør en risiko, idet spiludbyderen ikke har fysisk kontakt med kunden og kan som udgangspunkt derfor ikke være sikker på, at kunden er, hvem kunden udgiver sig for at være.

Der skal imidlertid tilføjes, at en kunde, som ikke er blevet verificeret, maksimalt kan indbetale 10.000 kr. til sin midlertidige spilkonto, og at kunden heller ikke kan få udbetalt midler. Det er dog vigtigt, at spiludbyderen er opmærksom på, at kunden kan overføre sine midler på anden vis, fx ved tab af indskud til andre kunder gennem spilprodukter, hvor kunder kan spille mod hinanden (peer-to-peer produkter).

3.7.1.4 Kunden er tilbageholdende med oplysninger
Det er et grundlæggende krav i hvidvaskloven, at spiludbyderen skal have kendskab til sine kunder. Spiludbyderen vil oftest være forpligtet til blandt andet at indhente relevante oplysninger fra kunden selv. Det kan fx ske, hvis spiludbyderen anmoder kunden om at indsende dokumentation for, hvordan kunden finansierer sit spilforbrug, eller hvis spiludbyderen skal have verificeret identitetsoplysninger på en kunde, som udgør en øget risiko.

Hvis spiludbyderen konstaterer, at kunden i de nævnte eksempler er tilbageholdende med at afgive de anmodede oplysninger, eller hvis kunden helt ignorerer anmodningen, er der en risiko for, at kundens intention er at misbruge spiludbyderens virksomhed til hvidvask. Kundens afvisende eller tilbageholdende adfærd i forbindelse med spiludbyderens kundekendskabsprocedurer eller undersøgelser kan indikere, at kunden prøver at skjule sin sande identitet, og at kundens midler eksempelvis er kriminelt udbytte.

Hvis kunden først efter et stykke tid fremsender de anmodede oplysninger eller dokumentation, kan det ligeledes indikere, at kunden bruger anmodningsfristen til at skaffe eller fabrikere de påkrævede oplysninger.

3.7.1.5 Ændring i kundens sædvanlige forbrugsmønster
Når spiludbyderens kunder har haft en spilkonto hos spiludbyderen over en længere periode, har spiludbyderen muligvis fået et godt kendskab til kundens sædvanlige forbrugsmønster. Hvis spiludbyderen på et tidspunkt kan konstatere, at der sker ændringer i kundens sædvanlige forbrugsmønster, er der en risiko for, at kunden er begyndt at udnytte sin spilkonto til hvidvask. Der er også en risiko for, at en anden end den identificerede kunde er begyndt at ind- og udbetale midler til og fra spilkontoen.

Ændringer i kundens sædvanlige forbrugsmønster kan fx være, at kunden som noget nyt begynder at foretage indbetalinger til spilkontoen ved brug af en betalingsløsning, som kunden hidtil ikke har anvendt. Ændringerne kan også ske i form af, at kunden begynder at gøre brug af nye spilprodukter, eller hvis kunden begynder at foretage betydelig større indbetalinger til spilkontoen.

3.7.1.6 Risikofaktorer forbundet med kundens spiladfærd

Hvis spiludbyderen fx udbyder fastoddsvæddemål, har kunden ofte mulighed for at gøre indskud på væddemål til lave odds. Ved spil på lave odds er der en relativ stor sandsynlighed for, at kunden modtager en gevinst for sit indskud. Ved at gennemspille midlerne kan kunden muligvis omgå spiludbyderens alarmer i relation til ind- og udbetalinger af midler til og fra spilkontoen uden spilaktivitet. Ved at gennemspille midler på spilkontoen via spilprodukter med høj tilbagebetalingsprocent har kunden således forsøgt at eliminere risikoen for tab.

Det samme gør sig gældende, hvis kunden fx ofte benytter sig af Cash-Out, eller hvis kunden placerer indskud på alle udfald af en begivenhed. På tilsvarende måde udgør den konkrete spiladfærd en risiko for, at kunden misbruger spiludbyderens spilprodukter med høj tilbagebetalingsprocent til at gennemspille kriminelt udbytte uden at risikere for store tab. Når kundens midler er gennemspillet, vil kunden nemmere have mulighed for at få gennemført udbetalinger til sin bankkonto uden, at spiludbyderen får mistanke om hvidvask. Udbetalingen af kundens midler fra spiludbyderen vil efterfølgende fremstå som spilgevinster over for pengeinstituttet.

Spiludbyderen skal være opmærksom på, at vurderingen af de risikofaktorer, der er forbundet med kundens spiladfærd, kan blive påvirket eller være under indflydelse af andre risikofaktorer, der er forbundet med spiludbyderens forretningsmodel. Spiludbyderens vurdering af den iboende risiko, der fx er forbundet med spil på lave odds, kan se anderledes ud, hvis risikofaktoren fx ses i sammenhæng med, at kunden foretager store indskud på væddemålet, eller hvis kunden ofte spiller på lave odds.

3.7.1.7 Ind- og udbetaling af store beløb til og fra kundens spilkonto

Der er en risiko for, at kunder, som ind- og udbetaler betydelige beløb til og fra deres spilkonto, ikke kan godtgøre over for spiludbyderen, hvor kunden har sine midler fra.

Hvis kunden ikke kan dokumentere, at midlerne stammer fra legale økonomiske aktiviteter, er der en risiko for, at kundens midler i stedet stammer fra en strafbar lovovertrædelse, og at kunden derfor forsøger at misbruge spiludbyderens virksomhed til hvidvask. Det er op til spiludbyderen selv at vurdere, hvornår kundens ind- og udbetalinger har et så betydeligt omfang, at der er en risiko for, at kunden ikke kan dokumentere midlernes oprindelse.

Det afgørende er, at spiludbyderen er opmærksom på, at ind- og udbetaling af store beløb til og fra kundens spilkonto kan have indflydelse på spiludbyderens iboende risiko for at blive misbrugt til hvidvask.

3.7.1.8 Spilprodukter, hvor kunder kan spille mod hinanden (peer-to-peer-produkter)

P2P-produkter er karakteriseret ved, at spiludbyderens kunder har mulighed for at spille mod hinanden. Udbuddet sker ofte ved, at spiludbyderen faciliterer eller stiller en online netværksplatform til rådighed for kunderne, som derefter kan interagere med hinanden. P2P-produkter kan fx være udbud af onlinepoker, som ofte foregår på få, store netværk, og som spiludbyderen køber sig adgang til, men det kan også være udbud af væddemålsbørser, hvor kunderne selv kan købe og sælge væddemål til hinanden. Spiludbyderen skal være opmærksom på, hvis netværksplatformen giver kunden adgang til at interagere med kunder fra andre jurisdiktioner, som ikke nødvendigvis tilgår platformen igennem spiludbyderens danske licens. Den globale netværksplatform er forbundet med en række andre risici, som spiludbyderen også skal forholde sig til, da det kan muliggøre overførsler til kunder i udlandet, som fx har hjemsted i højrisikojurisdiktioner, eller som er underlagt finansielle sanktioner.

Det faktum, at en kunde har mulighed for at tabe indskud til en anden kunde ved at spille mod hinanden, betyder, at der kan ske overførsel af midler mellem kunder (ofte betegnet "chip-dumping"). Overførsel af midler til en anden kunde medvirker til at sløre, at kundens midler oprindeligt stammer fra en strafbar lovovertrædelse.

Eksempel

Kunde A spiller onlinepoker med kunde B. Kunde A sidder i Danmark og kunde B sidder i udlandet. Kunde A og kunde B kender hinanden privat og har aftalt at spille onlinepoker via en global netværksplatform. Formålet med spillet er, at kunde A skal have overført et beløb til kunde B. De aftaler derfor, at kunde A skal lade sig tabe i pokerspillet, hvorved kunde B vinder puljen. Pengene fremstår derved som gevinster fra spil. På denne måde sker der således overførsel af penge fra kunde A i Danmark til kunde B i udlandet.

Da P2P-produkter muliggør overførsler imellem kunder, skal spiludbyderen også forholde sig til, hvilken risiko chip-dumping udgør i relation til terrorfinansiering.

3.7.1.9 Betalingsløsninger, der kan finansieres med kontanter
Når spiludbyderen skal identificere og vurdere risikoen forbundet med sine valgte betalingsløsninger, skal spiludbyderen afklare, om betalingsløsningen giver mulighed for, at kundens midler oprindeligt kan være finansieret med kontanter.

Selvom spiludbyderen efter spillelovgivningen ikke må modtage kontante indbetalinger på spilkontoen, kan visse tilladte betalingsløsninger fungere som et surrogat for kontante indbetalinger. Det er fx tilfældet ved forudbetalte kort, e-wallets og cash vouchers (værdibeviser), hvis værdi oprindeligt kan være finansieret med kontanter.

Kontanter udgør isoleret set en betydelig risiko, idet de ikke efterlader nogle digitale spor. Brugen af kontanter giver således kunden mulighed for at foretage anonyme betalinger. Det forhold, at kontanter er en anonym betalingsløsning, øger risikoen for, at midlerne stammer fra kriminelle forhold. Det kan fx være tilfældet ved aflønning af sort arbejde i kontanter eller salgsprovenu fra narkotika i kontanter.

3.7.1.10 Spiludbyderens væddemål misbruges til hvidvask forbundet til matchfixing
Hvidvasksekretariatet har i sin seneste risikovurdering af hvidvask fra 2022 angivet, at hvidvask gennem spil også kan være forbundet til matchfixing. Ved matchfixing øges chancerne for en sikker gevinst, idet sportsbegivenhedens resultat er aftalt forud for begivenheden med en eller flere af sportsbegivenhedens deltagere.

3.7.2 Landbaseret kasino

3.7.2.1 Identifikation af risikofaktorer
Nedenfor er uddybet nogle af de risikofaktorer, der kan være til stede ved udbud af landbaseret kasino.

Virksomhedens kundetyper

- Kunder, som forventes at have en varig tilknytning til kasinoet (forretningsforbindelser).
- Lejlighedsvise kunder (enkeltstående transaktioner).
- Politisk eksponerede personer (PEP), nærtstående til PEP eller nære samarbejdspartnere til PEP, både indenlandske og udenlandske.
- Kunder fra lande på EU-Kommissionens liste over højrisikotredjelande.
- Kunder fra lande på FATF's sorte og grå lister.
- Kunder, som er underlagt finansielle sanktioner.

Kundeadfærd

- Kunden er tilbageholdende med oplysninger.
- Kunden anmoder om udstedelse af gevinstkvittering.
- Kunden bruger falske dokumenter i forbindelse med kasinoets gennemførelse af kundekendskabs-procedurer.
- Kunden videregiver kontanter efter indløsning af spillemærker eller TITO til tredjemand.

Spilprodukter

- Spiludbyderens produktportefølje, fx roulette, poker og gevinstgivende spilleautomater.
- Spilproduktet udbydes med brug af kasinoets personale.
- Spilproduktets afviklingshastighed.
- Spilproduktets tilbagebetalingsprocent.
- Spilproduktets indskudsgrænse.
- Spilproduktet giver mulighed for, at kunder kan spille imod andre kunder, fx ved poker.

Leveringskanaler

- Kunden anvender kasinoets produkter ved fysiske fremmøde.
- Størrelsen på kasinoets lokaler.

Transaktioner

- Køb og indløsning af spillemærker og TITO for store beløb.
- Køb og indløsning af spillemærker og TITO uden eller lidt spilaktivitet.
- Ændring i kundens sædvanlige forbrugsmønster.
- Flere køb og/eller indløsning af spillemærker eller TITO for mindre beløb, som til sammen udgør store beløb (også kaldet structuring).

Betalingsmidler

- Spiludbyderens forskellige betalingsløsninger, fx kontanter, betalingskort og bankoverførsler.
- Betalingsløsninger, som i mindre grad er sporbare.
- Betalingsløsninger, som er egnet til at sløre, hvor midlerne stammer fra.
- Betalingsløsninger, som kan misbruges.
- Brug af flere forskellige betalingskort til køb af spillemærker eller TITO.

Geografiske risici

- Kasinoets beliggenhed.
- Registrering af kunder, som har hjemsted i udlandet.

Andre relevante risikofaktorer

- Kasinoets ansatte medvirker til eller faciliterer hvidvask på kasinoet.
- Kasinoets ansatte følger bevidst ikke kasinoets forretningsgange.
- Kasinoets ansatte er ikke i tilstrækkelig grad uddannet i hvidvasklovens krav.
- Hyppig udskiftning af kasinoets ansatte.
- Opbevaring af store beløb i kasinoets deponeringsbokse.
- Udstedelse af gevinstkvitteringer.
- Manuel overvågning af kundens transaktioner ved brug af kasinoets personale.
- Type og effektivitet af de eksisterende overvågningsmekanismer.

Nedenfor er en uddybning af nogle af ovenstående risikofaktorer.

Bemærk, at nogle af de oplistede risikofaktorer er behandlet samlet.

3.7.2.2 Lejlighedsvise kunder
Lejlighedsvise kunder, også kaldet enkeltstående transaktioner, er karakteriseret ved, at kunden ikke har en fast og varig tilknytning til kasinoet, idet kunden alene besøger kasinoet ved lejlighed. Det kan fx være tilfældet for turister eller andre kunder, som alene besøger kasinoet få gange, og som ikke er en jævnlig tilbagevendende kunde på kasinoet. Læs mere om enkeltstående transaktioner under afsnit 6.2.

Det forhold, at der er tale om lejlighedsvise kunder, betyder, at kasinoet ikke har et indgående kendskab til kunden. Den lejlighedsvise kunde har sandsynligvis aldrig besøgt kasinoet før, som betyder, at kasinoet fx ikke har kendskab til kundens sædvanlige forbrugsmønster og derfor ikke kan vurdere, om kundens adfærd afviger fra normalen. Hvis en lejlighedsvis kunde fx køber spillemærker for 20.000 kr., kan det være udfordrende for kasinoet at vurdere, om transaktionens størrelse giver anledning til mistanke om hvidvask, idet kasinoet ikke har kendskab til kundens økonomi.

3.7.2.3 Politisk eksponerede personer, nærtstående og nære samarbejdspartnere
Politisk eksponerede personer (PEP'er) er personer, som bestrider et særligt offentligt tillidshverv. På grund af PEP'ens særlige position og indflydelse i samfundet er der en risiko for, at persongruppens embede kan misbruges til hvidvask af kriminelt udbytte. Der er derudover en øget risiko for, at PEP'ens midler stammer fra enten korruption eller bestikkelse, og som gennem spil kan komme til at fremstå som legale spilgevinster.

Kategorien PEP'er omfatter flere forskellige kundetyper, som hver især kan udgøre en særskilt iboende risiko for hvidvask og terrorfinansiering. Udenlandske PEP'er fra lande, som fx har et højt korruptionsniveau, eller som har strategiske mangler i forhold til forebyggelse af hvidvask og terrorfinansiering, vil ofte udgøre en højere iboende risiko sammenlignet med en indenlandsk PEP, hvor virksomhedens forretningsmodel i mindre grad vil være eksponeret for hvidvask og terrorfinansiering.

For nærmere information og definition af PEP, nærtstående og nære samarbejdspartnere henvises til afsnit 6.5.3.

3.7.2.4 Kunden er tilbageholdende med oplysninger
Det er et grundlæggende krav i hvidvaskloven, at kasinoet skal have kendskab til sine kunder. Spiludbyderen vil oftest være forpligtet til blandt andet at indhente relevante oplysninger fra kunden selv. Det kan fx ske, hvis kasinoet anmoder kunden om dokumentation for, hvordan kunden finansierer sit spilforbrug, eller hvis kasinoet skal have verificeret identitetsoplysninger på en kunde. Hvis kasinoet konstaterer, at kunden i de nævnte eksempler er tilbageholdende med at afgive de anmodede oplysninger, eller hvis kunden helt ignorerer anmodningen, er der en risiko for, at kundens intention er at misbruge spiludbyderens virksomhed til

hvidvask. Kundens afvisende eller tilbageholdende adfærd i forbindelse med kasinoets kundekendskabsprocedurer eller undersøgelser kan indikere, at kunden prøver at skjule sin sande identitet, og at kundens midler eksempelvis er kriminelt udbytte.

3.7.2.5 Spilproduktet giver mulighed for, at kunder kan spille mod hinanden
Hvis kunder spiller mod hinanden i fx poker i stedet for mod kasinoet, kan de på forhånd have aftalt, at en kunde bevidst skal tabe til en anden kunde for herved at få kriminelt udbytte til at fremstå som en legal gevinst fra spil.

Det faktum, at en kunde ved spil mod en anden kunde har mulighed for at tabe sit indskud til denne, betyder, at der kan ske overførsel af midler mellem kunder (chip-dumping). Overførsel af midler til en anden kunde medvirker til at sløre, at kundens midler oprindeligt stammer fra en strafbar lovovertrædelse.

3.7.2.6 Køb og indløsning af spillemærker og TITO for store beløb
Der er en risiko for, at kunder, som køber og indløser spillemærker og TITO for betydelige beløb, ikke kan godtgøre over for kasinoet, hvor kunden har sine midler fra.

Hvis kunden ikke kan dokumentere, at midlerne stammer fra legale økonomiske aktiviteter, er der en risiko for, at kundens midler i stedet stammer fra en strafbar lovovertrædelse, og at kunden derfor forsøger at misbruge kasinoet til hvidvask. Det er op til kasinoet selv at vurdere, hvornår kundens køb og indløsning af spillemærker eller TITO har et så betydeligt omfang, at der er en risiko for, at kunden ikke kan dokumentere midlernes oprindelse.

Det afgørende er, at kasinoet er opmærksom på, at køb og indløsning af spillemærker og TITO for store beløb kan have indflydelse på kasinoets iboende risiko for at blive misbrugt til hvidvask.

> Ticket-in, ticket-out (TITO) er et voucher-baseret system, som kunden skal anvende til brug for spil på nogle af kasinoets produkter. Det kan fx være gevinstgivende spilleautomater. TITO-voucheren købes enten i TITO-automaten eller ved kasinoets kasse. Når kunden derefter fx ønsker at spille på kasinoets gevinstgivende spilleautomater, skal kunden indsætte voucheren i spilleautomaten, hvorefter voucherens værdi overføres til maskinen som kredit. Når kunden er færdig med at spille, bliver det resterende beløb på spilleautomatens kredit overført til en ny voucher, som efterfølgende kan blive udbetalt.

3.7.2.7 Køb og indløsning uden væsentlig spilaktivitet
Hvis en kunde ankommer til kasinoet med kontanter, som kunden får vekslet til spillemærker for dernæst at forlade kasinoet igen uden reelt at have spillet særlig meget, kan det medføre, at en indløsning af disse spillemærker til kontanter vil få kontanterne til at fremstå som gevinster fra spil på trods af, at der kan være tale om ulovlige midler.

Det samme gør sig gældende i den situation, hvor købet af enten spillemærker eller TITO sker ved brug af et betalingskort, og hvor der ikke bliver udstedt en gevinstkvittering, når spillemærkerne eller TITO-voucheren efterfølgende bliver indløst til kontanter. Den kriminelle aktør kan fx misbruge et stjålet betalingskort til køb af spillemærker for derefter at konvertere spillemærkerne til kontanter med henblik på at skjule eller tilsløre pengenes ulovlige oprindelse.

3.7.2.8 Ændring i kundens sædvanlige forbrugsmønster
Hvis kundeforholdet mellem kasinoet og kasinoets kunder kan forventes at have en vis varighed, bliver kasinoets kunder karakteriseret som forretningsforbindelser. Det kan fx være tilfældet, hvis kunden har købt et årskort hos kasinoet, eller hvis kunden med jævne mellemrum besøger kasinoet. Læs mere om forretningsforbindelser på landbaserede kasinoer under afsnit 6.4.1.3.

Når en kunde over en længere periode har haft en varig og tæt tilknytning til kasinoet, har kasinoet haft mulighed for at få et godt kendskab til kundens sædvanlige forbrugsmønster. Hvis

kasinoet på et tidspunkt kan konstatere, at der sker ændringer i kundens sædvanlige forbrugsmønster, er der en risiko for, at kunden misbruger kasinoet til hvidvask.

Ændringer i kundens sædvanlige forbrugsmønster kan fx være, at kunden som noget nyt begynder at købe spillemærker ved brug af en betalingsløsning, som kunden hidtil ikke har anvendt. Ændringerne kan også ske i form af, at kunden begynder at gøre brug af nye spilprodukter, eller hvis kunden begynder at købe spillemærker eller TITO for betydelige større beløb, end kunden plejer.

Eksempler

Kunde A har altid købt spillemærker ved brug af sit betalingskort udstedt af Bank Y. Kasinoet kan dog nu konstatere, at kunde A er begyndt at anvende kontanter til at finansiere spillemærkerne.

Kunde A kommer jævnligt på kasinoet og har hidtil altid kun benyttet spilleautomaterne. I løbet af den seneste måned har kasinoet dog konstateret, at kunde A nu er begyndt at spille med i ugentlige pokerturneringer på kasinoet.

Kunde A kommer jævnligt på kasinoet og bruger normalvis omkring 1.000 kr. på en aften. Igennem de seneste to måneder kan kasinoet dog konstatere, at kunde A er begyndt at veksle 10.000 kr. til spillemærker på en enkelt aften et par gange om måneden.

3.7.2.9 Flere køb og/eller indløsning af spillemærker eller TITO for mindre beløb
Risikofaktoren omfatter den situation, hvor en kunde foretager en række køb og/eller indløsning af spillemærker og/eller TITO for mindre beløb, som til sammen udgør store beløb (structuring). Det forhold, at en kunde fx deler et stort kontantbeløb op ved at foretage en række køb af spillemærker for mindre beløb, medvirker til, at de enkelte transaktioner kan forekomme mindre mistænkelige. Ved at dele et stort beløb op i en række mindre transaktioner er der en risiko for, at den kriminelle aktør formår at omgå kasinoets fastsatte tærskelværdier for, hvornår kasinoet foretager en undersøgelse.

3.7.2.10 Manuel transaktionsovervågning
Kasinoet er forpligtet til at monitorere og registrere samtlige transaktioner, som en forretningsforbindelse foretager på kasinoet. Læs mere om overvågningsforpligtelsen under afsnit 6.3.4

Hvis kasinoet har valgt, at det er kasinoets eget personale, som manuelt skal foretage overvågningen af kundernes transaktioner og aktiviteter, kan det indebære en række risici, som kasinoet skal identificere og vurdere. Den manuelle transaktionsovervågning kan blandt andet betyde, at der er en risiko for, at det ikke er alle transaktioner, som bliver registreret, da kasinoet ofte har mange kunder på samme tid, som foretager mange hurtige transaktioner. Risikoen for, at den manuelle transaktionsovervågning ikke er effektiv nok, øges, hvis personalet samtidig også har andre arbejdsopgaver. Det kan fx være tilfældet, hvis den samme medarbejder både er ansvarlig for transaktionsovervågningen og afviklingen af kasinoets spilprodukter på samme tid.

3.7.3 Landbaseret væddemål

3.7.3.1 Identifikation af risikofaktorer
Nedenfor er oplistet nogle af de risikofaktorer, der kan være til stede ved udbud af landbaseret væddemål.

Virksomhedens kundetyper

- Politisk eksponerede personer (PEP'er), nærtstående til PEP eller nære samarbejdspartnere til PEP, både indenlandske og udenlandske.
- Kunder fra lande på EU-Kommissionens liste over højrisikotredjelande.

- Kunder fra lande på FATF's sorte og grå lister.

Kundeadfærd

- Kunden er tilbageholdende med oplysninger.
- Kunden spiller på væddemål til lave odds.
- Kunden spiller på alle udfald af en begivenhed (hedging).
- Kunden benytter sig ofte af Cash-Out.
- Kunden virker ikke til at have et stort kendskab til spillets karakter og indhold.
- Kunden bliver eskorteret af en tredjemand.

Spilprodukter

- Spiludbyderens produktportefølje, fx fastoddsvæddemål og væddemål på elektronisk simulerede sportsbegivenheder.
- Spilproduktets afviklingshastighed.
- Spilproduktets tilbagebetalingsprocent.
- Spilproduktets indskudsgrænse.
- Spilproduktet giver mulighed for Cash-Out.

Leveringskanaler

- Brug af eksterne forhandlere til udbud af væddemål.
- Brug af identifikationsmiddel (spilkort) ved indgåelse af væddemål, præmiesøgning og udbetaling
- Udbud af væddemål via selvbetjeningsterminaler.

Transaktioner

- Indskud af store beløb på væddemål.
- Udbetaling af store beløb fra kundens spilkonto.
- Ændring i kundens sædvanlige forbrugsmønster.
- Indskud på væddemål af en række sammenhængende småbeløb, som til sammen udgør store transaktioner (structuring).
- Udbetaling af en række sammenhængende småbeløb fra kundens spilkonto, som til sammen udgør store transaktioner (structuring).

Betalingsløsninger

- Spiludbyderens anvendte betalingsløsninger, fx kontanter og betalingskort.
- Betalingsløsninger, som i mindre grad er sporbare.
- Betalingsløsninger, som kan misbruges.
- Betalingsløsninger, som giver mulighed for at gennemføre hurtige og store udbetalinger fra spilkontoen.
- Brug af flere forskellige betalingskort til indskud på væddemål og til udbetalinger af midler fra spilkontoen.

- Hyppige skift i brugen af betalingsløsninger.

Geografiske risici

- Forhandlerens geografiske placering.

Andre relevante risikofaktorer

- Spiludbyderens egne ansatte medvirker til hvidvask.
- Spiludbyderens egne ansatte følger bevidst ikke spiludbyderens forretningsgange.
- Spiludbyderens egne ansatte er ikke i tilstrækkelig grad uddannet i hvidvasklovens krav.
- Spiludbyderens væddemål misbruges til hvidvask forbundet til matchfixing

Nedenfor er en uddybning af nogle af ovenstående risikofaktorer.

Bemærk, at nogle af de oplistede risikofaktorer er behandlet samlet.

3.7.3.2 Politisk eksponerede personer, nærtstående og nære samarbejdspartnere
Politisk eksponerede personer (PEP'er) er personer, som bestrider et særligt offentligt tillidshverv. På grund af PEP'ens særlige position og indflydelse i samfundet er der en risiko for, at persongruppens embede kan misbruges til hvidvask af kriminelt udbytte. Der er derudover en øget risiko for, at PEP'ens midler stammer fra enten korruption eller bestikkelse, og som gennem spil kan komme til at fremstå som legale spilgevinster.

Kategorien PEP'er omfatter flere forskellige kundetyper, som hver især kan udgøre en særskilt iboende risiko for hvidvask og terrorfinansiering. Udenlandske PEP'er fra lande, som fx har et højt korruptionsniveau, eller som har strategiske mangler i forhold til forebyggelse af hvidvask og terrorfinansiering, vil ofte udgøre en højere iboende risiko sammenlignet med en indenlandsk PEP, hvor virksomhedens forretningsmodel i mindre grad vil være eksponeret for hvidvask og terrorfinansiering.

For nærmere information og definition af PEP, nærtstående og nære samarbejdspartnere henvises til afsnit 6.5.3.

3.7.3.3 Kunden er tilbageholdende med oplysninger
Det er et grundlæggende krav i hvidvaskloven, at spiludbyderen skal have kendskab til sine kunder. Spiludbyderen vil oftest være forpligtet til blandt andet at indhente relevante oplysninger fra kunden selv. Det kan fx ske, hvis spiludbyderen anmoder kunden om at indsende dokumentation for, hvordan kunden finansierer sit spilforbrug, eller hvis spiludbyderen skal have verificeret identitetsoplysninger på en kunde, som udgør en øget risiko.

Hvis spiludbyderen konstaterer, at kunden i de nævnte eksempler er tilbageholdende med at afgive de anmodede oplysninger, eller hvis kunden helt ignorerer anmodningen, er der en risiko for, at kundens intention er at misbruge spiludbyderens virksomhed til hvidvask. Kundens afvisende eller tilbageholdende adfærd i forbindelse med spiludbyderens kundekendskabsprocedurer eller undersøgelser kan indikere, at kunden prøver at skjule sin sande identitet, og at kundens midler eksempelvis er kriminelt udbytte.

Hvis kunden først efter et stykke tid fremsender de anmodede oplysninger eller dokumentation, kan det ligeledes indikere at kunden bruger anmodningsfristen til at skaffe eller fabrikere de påkrævede oplysninger.

3.7.3.4 Risikofaktorer forbundet med kundens spiladfærd

Hvis spiludbyderen fx udbyder fastoddsvæddemål, har kunden ofte mulighed for at gøre indskud på væddemål til lave odds. Ved spil på lave odds er der en relativ stor sandsynlighed for, at kunden modtager en gevinst for sit indskud, som efterfølgende bliver krediteret spilkontoen. Kunden har derefter mulighed for at få udbetalt sine indestående midler på spilkontoen til sin bankkonto, som derefter vil fremstå som legale spilgevinster.

Det samme gør sig gældende, hvis kunden fx ofte benytter sig af Cash-Out, eller hvis kunden placerer indskud på alle udfald af en begivenhed. På tilsvarende måde udgør den konkrete spiladfærd en risiko for, at kunden misbruger spiludbyderens spilprodukter med høj tilbagebetalingsprocent til at få krediteret kriminelt udbytte til sin spilkonto uden at risikere for store tab, som efterfølgende kan overføres til kundens pengeinstitut.

3.7.3.5 Brug af forhandlere til udbud af landbaserede væddemål

Udbydere af landbaserede væddemål kan sælge deres produkter hos egne forhandlere og/eller eksterne forhandlere. En spiludbyders egne forhandlere er spiludbyderens egne spillebutikker, hvorimod en ekstern forhandler fx kan være en tankstation eller en dagligvarebutik.

Hvis spiludbyderen sælger produkter via egne forhandlere, er der ikke tale om outsourcing, da det er en del af spiludbyderens egen virksomhed

Hvis spiludbydere sælger deres produkter hos eksterne forhandlere, skal spiludbyderen være opmærksom på, i hvilket omfang de outsourcer forpligtelser i hvidvaskloven. Det kan fx være i hvilket omfang, de outsourcer forpligtelsen til at gennemføre kundekendskabsprocedurer.

En ekstern forhandler er ikke omfattet af hvidvaskloven, og en ekstern forhandler vil således ikke være ansvarssubjekt ved en overtrædelse af hvidvasklovgivningen. Det er spiludbyderen, der er omfattet af hvidvasklovens § 1, stk. 1, nr. 19, og det er derfor spiludbyderen, der er ansvarssubjekt, selvom der er sket outsourcing af en forpligtelse til en ekstern forhandler. I de tilfælde, hvor spiludbyderen benytter outsourcing, skal spiludbyderen være opmærksom på, om outsourcing har betydning for spiludbyderens risici.

Udbydere af landbaserede væddemål skal være opmærksomme på, at tilstedeværelsen og vurderingen af de nedenstående risici kan afhænge af spiludbyderens forretningsmodel, herunder, fx hvor og hvordan produkterne sælges.

Forhandlerleddet udgør en række selvstændige risici. Risiciene kan vurderes forskelligt alt afhængig af, om der er tale om egne forhandlere eller eksterne forhandlere.

De ansatte ved forhandlerne kan have en række andre arbejdsopgaver og ansvarsområder, der ikke relaterer sig til salg af spil og gennemførelse af kundekendskabsprocedurer. Den omstændighed, at de ansatte har andre arbejdsopgaver og ansvarsområder, kan bevirke, at de har mindre opmærksomhed på at forebygge og bekæmpe hvidvask. Det kan betyde, at de fx ikke er opmærksomme på kundernes mistænkelige adfærd, at de ikke gennemfører kundekendskabsprocedurer i henhold til hvidvaskloven, eller at de ikke videreformidler relevante informationer til spiludbyderen.

Forhandlerens ansatte er i nogle tilfælde ansat i kortere perioder, hvorfor der er risiko for, at den manglende kontinuitet kan medføre, at de ansatte ikke oparbejder tilstrækkelig viden om og erfaring med at forebygge og bekæmpe hvidvask.

Der er risiko for, at de ansatte ved forhandlerne ikke er undervist tilstrækkeligt i hvidvasklovens krav, eller at forhandlerleddet ikke får implementeret de nyeste ændringer i forretningsgangene. Forhandlerleddet kan derfor ubevidst være med til at facilitere hvidvask gennem spil.

Da forhandleren får provenu ved salg af spiludbyderens landbaserede væddemål, har forhandlerleddet en økonomisk interesse i at sælge spiludbyderens produkter. Forhandlerens egen økonomiske interesse kan medføre, at forhandleren slækker på fx gennemførelse af kundekendskabsprocedurerne. Den risiko kan være forøget, hvis forhandleren er geografisk placeret tæt på andre konkurrenter, der også sælger landbaserede væddemål. Forhandleren kan derfor have en interesse i at give sine kunder en nem, hurtig og smidig forbrugeroplevelse.

Derudover er der en risiko for, at forhandlerleddet bevidst benytter forretningen til hvidvask. Det kan fx ske ved, at forhandleren eller forhandlerens ansatte selv hvidvasker gennem spil, og at de bevidst ikke gennemfører kundekendskabsprocedurer.

Med indførelsen af spilkortet har spiludbyderen nu i højere grad mulighed for selv at udføre kundeoprettelser og gennemføre kundekendskabsprocedurer, fordi kunderne skal oprettes med en spilkonto hos spiludbyderen. Det kan spiludbyderen fx gøre via spiludbyderens app eller hjemmeside. Spiludbyderen kan fortsat vælge at outsource nogle opgaver til en forhandler.

Se afsnit 5.2.1 om undervisning af forhandlerne og afsnit 7.3.6 om outsourcing til eksterne forhandlere.

3.7.3.6 Brug af identifikationsmiddel (spilkort)
Det er obligatorisk for alle kunder at identificere sig med et identifikationsmiddel, når de blandt andet indgår væddemål ved en fysisk forhandler. Identifikationsmidlet kan være et fysisk kort, som bliver udstedt af spiludbyderen, og det også kan være et virtuelt kort, som eksempelvis fremgår af en app.

Selvom indgåelse af et væddemål knyttes op til en bestemt identificeret kunde, er der stadig en række risici forbundet med, at kunden skal anvende et fysisk eller virtuelt identifikationsmiddel. Spiludbyderen skal fx forholde sig til, i hvilket omfang der kan ske misbrug af identifikationsmidlet og derefter vurdere, hvilken indflydelse det har på spiludbyderens iboende risiko for at blive misbrugt til hvidvask og terrorfinansiering. Misbruget kan ske ved, at spilkortet med den tilknyttede spilkonto stilles til rådighed for kriminelle aktører enten under tvang, mod vederlag eller frivilligt. Spiludbyderen kan derfor ikke med garanti gå ud fra, at det er den registrerede kunde, som reelt køber et væddemål ved den fysiske forhandler, eller som anmoder om udbetaling af midlerne fra spilkontoen.

3.7.3.7 Selvbetjeningsterminaler
Spiludbydere, der udbyder væddemål via selvbetjeningsterminaler, skal foretage en grundig risikovurdering af, hvordan udbud af væddemål via selvbetjeningsterminaler påvirker spiludbyderens iboende risiko for at blive misbrugt til hvidvask og terrorfinansiering. Det faktum, at forhandleren ikke har nogen direkte kontakt med en kunde i forbindelse med indgåelsen af et væddemål, øger den risiko, der er til stede for, at der bliver forsøgt på hvidvask af penge. Brugen af selvbetjeningsterminaler kan medvirke til, at forhandleren har udfordringer med at konstatere mistænkelig kundeadfærd i forbindelse med indgåelse af væddemålet. Mistænkelig kundeadfærd kan fx være, at kunden bliver eskorteret og instrueret af en tredjemand, eller at kunden ikke har den store kendskab til spilproduktets karakter og indhold.

Risikoen, som er forbundet med selvbetjeningsterminaler, skal ses i sammenhæng med, at forhandleren kan have en række andre arbejdsopgaver og ansvarsområder, der ikke relaterer sig til salg af spil og gennemførelse af kundekendskabsprocedurer. Det forhold, at forhandleren også kan have andre arbejdsopgaver, kan medføre, at forhandleren i praksis kan have

udfordringer med at opdage mistænkelig adfærd ved selvbetjeningsterminalen. Det gør sig især gældende, hvis forhandleren skal ekspedere en kunde ved kassen samtidig med, at en anden kunde placerer et væddemål på selvbetjeningsterminalen.

Væddemålsterminaler

Spillemyndigheden karakteriserer enhver væddemålsterminal som selvbetjent, hvis man kan endeligt indgå væddemål uden at være i kontakt med butikkens personale.

3.7.3.8 Kontante køb af landbaserede væddemål

Spiludbyderen skal identificere og vurdere risikoen ved, at kunderne kan anvende kontanter til køb af væddemål ved den fysiske forhandler. Kontanter udgør isoleret set en betydelig risiko, idet de ikke efterlader nogle digitale spor. Brugen af kontanter giver således kunden mulighed for at foretage anonyme betalinger. Det forhold, at kontanter er en anonym betalingsløsning, øger risikoen for, at midlerne stammer fra kriminelle forhold. Det kan fx være tilfældet ved aflønning af sort arbejde i kontanter eller salgsprovenu fra narkotika i kontanter.

Kontante køb af væddemål krediteres kundens spilkonto, hvis væddemålet går hjem. Gevinsten kan efterfølgende blive udbetalt til kundens bankkonto, hvilket udgør en øget risiko, da kriminelt udbytte på den måde kan anbringes i det finansielle system. Udbetalingen fra spiludbyderen til kundens bankkonto vil samtidig medvirke til, at det kriminelle udbytte sløres, idet overførslen umiddelbart vil fremstå som spilgevinster i stedet. Det er ikke muligt at indsætte kontanter på sin spilkonto hos en fysisk forhandler. Kontanter kan bruges til køb af væddemål, hvorefter en eventuel gevinst krediteres kundens spilkonto.

3.7.3.9 Indskud af store beløb på væddemål og store udbetalinger fra kundens spilkonto

Der er en risiko for, at kunder, som foretager store indskud på væddemål, og som udbetaler betydelige beløb fra deres spilkonto, ikke kan godtgøre over for spiludbyderen, hvor kunden har sine midler fra.

Hvis kunden ikke kan dokumentere, at midlerne stammer fra legale økonomiske aktiviteter, er der en risiko for, at kundens midler i stedet stammer fra en strafbar lovovertrædelse, og at kunden derfor forsøger at misbruge spiludbyderens virksomhed til hvidvask. Det er op til spiludbyderen selv at vurdere, hvornår størrelsen af kundens transaktioner har et så betydeligt omfang, at der er en risiko for, at kunden ikke kan dokumentere midlernes oprindelse.

Det afgørende er, at spiludbyderen er opmærksom på, at indskud og udbetalinger af store beløb kan have indflydelse på spiludbyderens iboende risiko for at blive misbrugt til hvidvask.

3.7.3.10 Ændring i kundens forbrugsmønster

Når spiludbyderens kunde har været kunde hos spiludbyderen over en længere periode, har spiludbyderen haft mulighed for at få et godt kendskab til kundens sædvanlige forbrugsmønster. Hvis spiludbyderen på et tidspunkt kan konstatere, at der sker ændringer i kundens sædvanlige forbrugsmønster, er der en risiko for, at det er en anden end den identificerede kunde, som fx er begyndt at foretage indskud på væddemål, eller som anmoder spiludbyderen om at udbetale midler fra spilkontoen.

Ændringer i kundens sædvanlige forbrugsmønster kan være, at kunden som noget nyt begynder at foretage indskud på væddemål ved brug af en betalingsløsning, som kunden hidtil ikke har anvendt. Det kan fx være tilfældet, hvis en kunde, som altid har købt væddemål ved brug af betalingskort, begynder at finansiere sine væddemål med kontanter.

Eksempel

Kunde A køber jævnligt væddemål og betaler altid for væddemålet med sit betalingskort. Den seneste måned har spiludbyder X imidlertid kunnet konstatere, at kunde A's indbetalinger i stedet er foregået med kontanter, og at indskuddet desuden har været højere end normalt.

Ændringerne kan også ske i form af, at kunden begynder at gøre brug af nye spilprodukter, eller hvis kunden begynder at foretage betydelig større indskud på spiludbyderens væddemålsprodukter.

3.7.3.11 Spiludbyderens væddemål misbruges til hvidvask forbundet til matchfixing

Hvidvasksekretariatet har i sin seneste risikovurdering af hvidvask fra 2022 angivet, at hvidvask gennem spil også kan være forbundet til matchfixing. Ved matchfixing øges chancerne for en sikker gevinst, idet sportsbegivenhedens resultat er aftalt forud for begivenheden med en eller flere af sportsbegivenhedens deltagere.

Politikker, forretnings-gange og kontroller

4

4.1 Introduktion

Hvidvasklovens § 8, stk. 1

Spiludbydere skal udarbejde skriftlige politikker, forretningsgange og kontroller. Det fremgår af hvidvasklovens § 8, stk. 1.

Spiludbyderens politikker, forretningsgange og kontroller skal udarbejdes på baggrund af den risikovurdering, som spiludbyderen har udarbejdet. Det vil sige, at spiludbyderen først kan tage stilling til indholdet af politikker, forretningsgange og kontroller, når virksomheden har udarbejdet sin risikovurdering.

Når spiludbyderen har udarbejdet spiludbyderens risikovurdering, skal spiludbyderen tage stilling til de risici, der er i spiludbyderens virksomhed og tage stilling til, hvordan dens risici kan nedbringes, og hvordan det sikres, at de forebyggende foranstaltninger står mål med de risici, som virksomheden er udsat for.

Spiludbyderens politikker, forretningsgange og kontroller er spiludbyderens mitigerende foranstaltninger eller risikobegrænsende tiltag – altså det, som spiludbyderen gør for at nedbringe sin iboende risiko. Den risiko, der kan være tilbage efter de mitigerende tiltag, betegnes som 'den residuale risiko'. Det vil sige den risiko, som spiludbyderen i sidste ende løber for at blive misbrugt til hvidvask og terrorfinansiering.

Se model i afsnit 3.1, der illustrerer processen fra konstateringen af den iboende risiko til konstateringen af den risiko, der er tilbage, når spiludbyderen har udarbejdet politikker, forretningsgange mv.

Der er ingen formkrav udover skriftlighed. Skriftlighedskravet betyder, at politikker, forretningsgange og kontroller skal være dokumenterede, hvilket både kan ske skriftligt og fx i form af videoer. De skal derudover være tilgængelige og effektive for spiludbyderen og udbyderens ansatte.

Politikkerne, forretningsgangene og kontrollerne skal som minimum omfatte:

- risikostyring
- kundekendskabsprocedurer
- undersøgelses-, noterings-, og underretningspligt
- opbevaringspligt
- screening af medarbejdere og
- intern kontrol.

Spiludbyderen skal i forbindelse med udarbejdelse af politikker og forretningsgange tage højde for, at virksomhedens egen forretningsmodel kan betyde, at der også er andre emner, der skal indeholdes i politikkerne og forretningsgangene.

4.2 Opdatering

Spiludbyderens politikker, forretningsgange og kontroller skal holdes opdaterede. Der skal som minimum ske opdatering, hvis der sker ændringer i risikovurderingen, som har betydning for spiludbyderens politikker og forretningsgange, herunder hvis der sker ændringer i forretningsmodellen. Det kan fx være, hvis spiludbyderen begynder at tilbyde et nyt produkt, eller hvis risikobilledet i samfundet ændrer sig. Der skal desuden ske opdatering, hvis der sker ændringer i, hvordan arbejdsopgaverne skal løses. Det kan fx være, hvis spiludbyderens fremgangsmåde for intern behandling af sager, hvor der skal ske underretning, ændres.

4.3 Politikker

En politik skal indeholde identifikation, vurdering og afgrænsning af spiludbyderens risikofaktorer samt de overordnede strategiske mål til forebyggelse af hvidvask og terrorfinansiering med udgangspunkt i spiludbyderens risikovurdering.

I politikkerne skal spiludbyderen således tage stilling til, hvilke risici spiludbyderen vil påtage sig, hvordan disse skal håndteres, hvordan det sikres, at nye risici opdages og håndteres, og hvordan de strategiske mål opnås.

I politikkerne skal det derfor beskrives, om der er risici, som man ikke ønsker at påtage sig. Det kan fx være risici forbundet med en bestemt kundetype, et geografisk område eller et produkt.

En politik for risikostyring udgør det overordnede grundlag for strategisk og operationel risikostyring, og fastsætter blandt andet formål, risikoområder, ansvarsfordeling, risikovillighed samt den organisatoriske forankring af risikoledelse- og styring.

Eksempel

I politikken kan det fx fremgå, hvordan spiludbyderen overordnet håndterer de risici, der er forbundet med brugen af selvbetjeningsterminaler eller chip-dumping.

4.4 Forretningsgange

En spiludbyder skal have forretningsgange, der beskriver de aktiviteter, som spiludbyderen skal udføre med henblik på at sikre, at lovgivningen og anden regulering bliver overholdt, samt at spiludbyderens politikker og retningslinjer efterleves. Forretningsgangene er spiludbyderens konkrete og operationelle udmøntning af politikkerne. De skal derfor beskrive de konkrete handlinger, der skal forebygge, at spiludbyderen bliver misbrugt til hvidvask og terrorfinansiering.

Forretningsgangene skal tage udgangspunkt i spiludbyderens forretningsmodel og på en klar og tydelig måde beskrive, hvordan spiludbyderen skal overholde reglerne. Forretningsgangene skal beskrive de enkelte aktiviteter i opgaveudførelsen af hvert område. Det er et krav, at forretningsgangene er lettilgængelige og overskuelige for medarbejderne. I forretningsgangene skal være angivet, hvem der er ansvarlig for de enkelte opgaver, samt hvordan opgaverne skal udføres

Forretningsgangene skal være operationelt anvendelige, og de ansatte skal derfor efter at have læst disse vide, hvordan de skal udføre den konkrete opgave.

4.4.1 Risikostyring

Spiludbyderen skal beskrive sin risikostyring i en forretningsgang. Det vil sige, hvordan risikostyringen skal udføres i praksis, herunder hvem der er ansvarlig for området, hvordan spiludbyderen følger og opdager ændringer i risikobilledet, hvordan der skal reageres på nye risici for, at spiludbyderen kan blive misbrugt til hvidvask eller terrorfinansiering, og hvordan nye risici indarbejdes. Forretningsgangen skal desuden beskrive, hvordan der reageres på overtrædelser af spiludbyderens politikker og forretningsgange.

Risikostyringen skal tage udgangspunkt i spiludbyderens forretningsmodel og de risici, som spiludbyderen har identificeret i risikovurderingen.

Eksempel

Det kan fx være angivet i forretningsgangen, at det er virksomhedens hvidvaskansvarlige, der er ansvarlig for, at nye konstaterede risici bliver indarbejdet i spiludbyderens risikovurdering.

4.4.2 Kundekendskabsprocedurer

Spiludbyderen skal i spiludbyderens forretningsgange beskrive deres kundekendskabsprocedurer, herunder, hvornår der skal gennemføres kundekendskabsprocedurer, hvad kundekendskabsproceduren omfatter, og hvordan de enkelte aktiviteter, der skal udføres, håndteres i praksis.

Det kan fx være en nærmere beskrivelse af, hvilke identitetsoplysninger, der skal indhentes, og hvordan de skal indhentes og efterfølgende kontrolleres. Det kan også være en nærmere beskrivelse af, hvordan spiludbyderen ajourfører sine oplysninger om sine kunder, hvordan spiludbyderen overvåger sine kunder, og hvordan spiludbyderen vurderer risikoen ved sine enkelte kunder. Det kan også være en nærmere beskrivelse af, hvordan spiludbyderen fastlægger, om en kunde udgør en øget risiko.

Se nærmere om kundekendskabsprocedurer i afsnit 6.

4.4.3 Undersøgelses- og noteringspligt

Spiludbyderen skal foretage undersøgelse af visse transaktioner og aktiviteter. Spiludbyderen skal derfor have forretningsgange, der nærmere beskriver, hvornår der er pligt til at iværksætte en undersøgelse, hvordan spiludbyderen bliver opmærksom på de transaktioner og aktiviteter, der er pligt til at undersøge, og hvordan undersøgelsen nærmere skal foregå.

Der er pligt til at notere resultatet af de undersøgelser, som iværksættes. Spiludbyderens forretningsgange skal derfor også beskrive, hvornår der skal noteres, hvad der skal noteres, og hvordan og hvor der skal noteres.

Det kunne fx være beskrevet, at ansatte skal notere observationer og informationer på kundens kundeprofil, og med hvilket interval dette bør ske, eventuelt på baggrund af kundens spilaktivitet.

Se nærmere om undersøgelses- og noteringspligten i afsnit 8.

4.4.4 Underretningspligt

Spiludbyderen skal udarbejde forretningsgange, der nærmere beskriver underretningspligten. Det vil sige, at forretningsgangen nærmere skal beskrive, i hvilke situationer der skal underrettes, hvad der skal underrettes om, hvordan der skal ske underretning, og hvem der skal foretage underretningen.

Det er vigtigt, at medarbejderne efter at have læst forretningsgangen ikke er i tvivl om, hvad en underretning er, og hvilke trin der skal iværksættes.

Se nærmere om underretningspligten i afsnit 9.

4.4.5 Opbevaringspligt

Spiludbyderen skal opbevare visse oplysninger om sine kunder. Forretningsgange for opbevaringspligten skal således indeholde en beskrivelse af opbevaringspligten, herunder hvilke oplysninger der skal gemmes, hvor de skal gemmes, hvor længe de skal gemmes, og hvordan de skal slettes igen.

Se nærmere om opbevaringspligten i afsnit 10.

4.4.6 Screening af medarbejdere

Spiludbyderen skal forebygge, at spiludbyderens medarbejdere kan misbruge deres stilling til hvidvask eller terrorfinansiering. Spiludbyderen skal derfor have forretningsgange, der nærmere beskriver, hvordan spiludbyderen screener sine medarbejdere.

Kravet om screening indeholder to elementer:
1. Spiludbyderen skal sikre, at medarbejderen ikke er dømt for et strafbart forhold, der øger risikoen for, at medarbejderen kan misbruge sin stilling ved spiludbyderen.
2. Spiludbyderen skal sikre, at medarbejderen har tilstrækkelige kvalifikationer til at varetage stillingen. Det betyder, at medarbejderen skal have den nødvendige viden på hvidvaskområdet til at kunne løfte sine arbejdsopgaver på betryggende vis.

Ad 1)
Spiludbyderen skal sikre, at medarbejderen ikke er dømt for et strafbart forhold, der øger risikoen for, at medarbejderen vil misbruge sin stilling til hvidvask. Det kan fx sikres ved, at der forud for ansættelse indhentes og sker kontrol af den pågældende medarbejders straffeattest. Det er vigtigt, at screeningen sker inden ansættelse af den pågældende medarbejder.

I kravet om screening ligger også, at spiludbyderen skal sikre, at spiludbyderen bliver bekendt med, hvis en medarbejder i løbet af ansættelsen bliver dømt for et strafbart forhold, der øger risikoen for misbrug. Dette kan fx sikres ved, at spiludbyderen indsætter et krav om, at medarbejderen skal oplyse, hvis pågældende bliver dømt for et strafbart forhold under ansættelsen, eller ved med et fast interval at indhente alle eller udvalgte medarbejderes straffeattest.

Det er op til spiludbyderen at vurdere, hvilken procedure der passer bedst til spiludbyderen. Den procedure, der vælges, skal fremgå af forretningsgangene.

Det bemærkes, at screeningen skal foretages på baggrund af en risikobaseret tilgang og være proportionel. Det er ikke et krav, at alle medarbejdere screenes. Det afhænger af, hvilken funktion medarbejderen skal varetage. Spiludbyderen skal derfor forholde sig til, hvilke funktioner og arbejdsområder der kræver screening.

Det vil fx ikke være relevant at screene medarbejdere, der ikke skal varetage funktioner, der skal sikre opfyldelse af hvidvaskloven. Det er derimod relevant altid at screene medarbejdere, hvis medarbejderen i kraft af sin funktion, direkte eller indirekte kan misbruge sin stilling til at medvirke til hvidvask eller terrorfinansiering.

Ad 2)
Spiludbyderen skal sikre, at medarbejderen har den nødvendige viden og kvalifikationer til at kunne varetage sin stilling. Dette kan være opfyldt ved ansættelsen, men kan også opfyldes ved, at medarbejderen uddannes efter ansættelse.

Spiludbyderens forretningsgange for screening af medarbejdere skal nærmere beskrive, hvordan spiludbyderen vil sikre, at ovenstående overholdes.

For personer, som ansættes i en stilling, hvor personen direkte eller indirekte kan misbruge stillingen til hvidvask eller finansiering af terrorisme, vil det altid være relevant med en nærmere undersøgelse af personen inden ansættelsen. Medarbejdere i ledende og/eller betroede stillinger vil desuden være særligt relevante at screene.

Screening af medarbejdere kan derudover eksempelvis være relevant, hvis medarbejderen:

- udfører kundekendskabsprocedurer
- har adgang til at foretage transaktioner
- har fået uddelegeret opgaver fra den hvidvaskansvarlige
- arbejder i virksomhedens compliancefunktion og ansatte, der arbejder i virksomhedens interne revision eller interne auditfunktion.

4.5 Kontroller

Spiludbyderen skal etablere en intern kontrol, hvor det skal kontrolleres, at spiludbyderen overholder hvidvasklovens krav og følger spiludbyderens politikker og forretningsgange. Den interne kontrol skal beskrives i spiludbyderens forretningsgange, herunder hvad der skal kontrolleres, hvordan og hvornår det skal udføres og af hvem.

Spiludbyderen skal indrette den interne kontrol efter spiludbyderens størrelse og de risici, der er forbundet med spiludbyderens forretningsmodel.

Kontrollerne skal foretages med passende tidsintervaller på følgende områder:
- Risikostyring
- Kundekendskabsprocedurer
- Undersøgelses-, noterings-, og underretningspligt
- Opbevaringspligt og
- Screening af medarbejdere.

Det er op til spiludbyderen at tage stilling til, hvordan kontrollerne skal gennemføres. Det kan fx ske ved at udtage stikprøver, hvor det kontrolleres, om der er gennemført tilstrækkelige kundekendskabsprocedurer i henhold til forretningsgangene, eller om der er foretaget korrekt notering i forbindelse med en undersøgelse af en kunde.

Eksempel

Spiludbyder X's forretningsgang for interne kontroller fastlægger, at lederen af complianceteamet skal foretage en intern kontrol én gang om måneden af, om kundeserviceteamet har fulgt forretningsgange for gennemførelse af kundekendskabsprocedurer.

Det er vigtigt, at der er tilstrækkelig uafhængighed mellem den, der foretager kontrollen, og den, der kontrolleres.

4.5.1 Kontrol med kontrollerne

I kravet om, at der skal gennemføres kontroller, ligger også et krav om, at der skal føres kontrol med, at der bliver ført kontrol på de pågældende områder, og at kontrollerne er egnede. Dette betyder, at spiludbyderen skal følge op på, om der bliver gennemført kontrol som planlagt, og at kontrollerne omfatter alle de ovenfor oplistede områder. Dette skal også beskrives i spiludbyderens forretningsgange for intern kontrol.

Eksempel

Spiludbyder X har en forretningsgang, der fastlægger, at der skal føres kontrol med, at de interne kontroller er gennemført og egnede én gang hvert halve år. Det er spiludbyderens hvidvaskansvarlige, der står for denne kontrol af kontrollerne.

4.5.2 Dokumentation

Spiludbyderen skal kunne dokumentere de kontroller, der er blevet gennemført. Det vil sige, at spiludbyderen både skal kunne dokumentere, at der er gennemført intern kontrol, men også at der er fulgt op på, at kontrollerne er blevet gennemført.

Ansvar, undervisning og koncerner

5

5.1 Ansvar for overholdelse af reglerne

Det overordnede ansvar for, at spiludbyderen overholder hvidvaskområdet, påhviler spiludbyderens øverste ledelse. Ledelsen bør sikre, at dennes involvering i emner om hvidvask af penge og finansiering af terrorisme er synlig for bestyrelsen og for alle medarbejdere og forretningspartnere. Ledelsen har et personligt ansvar for at sikre, at der er tilstrækkelige kontrolforanstaltninger og procedurer på plads i virksomheden.

Det er ikke et krav for spiludbydere, at de udpeger en ansat, der har fuldmagt til at træffe beslutninger på vegne af virksomheden, jf. hvidvasklovens § 7, stk. 2, modsætningsvis.

5.1.1 Ansvarligt direktionsmedlem

Hvis det vurderes relevant, skal spiludbyderen udpege et medlem af direktionen, der er ansvarlig for virksomhedens gennemførelse af kravene i hvidvaskloven.

Der er ikke et krav om, at spiludbydere uden en direktion er forpligtet til at udpege en person med denne funktion.

Det ansvarlige direktionsmedlems forpligtelse er især at sikre, at spiludbyderen lever op til reglerne i hvidvaskloven. Der kan fx holdes møder med de medarbejdere, der er ansat til at overvåge kundernes spilaktivitet og lignende med henblik på at få en status om overholdelse af reglerne.

5.2 Undervisning

Hvidvasklovens § 8, stk. 6

Spiludbydere skal sikre sig, at deres ansatte samt ledelsen modtager tilstrækkelig undervisning i kravene i hvidvaskloven, regler udstedt i medfør af hvidvaskloven og relevante bestemmelser om databeskyttelse. Det fremgår af hvidvasklovens § 8, stk. 6.

Det er ikke tilstrækkeligt, at spiludbyderens skriftlige politikker og forretningsgange blot bliver udleveret til de ansatte med henblik på, at de selv gennemgår kravene. Det er heller ikke tilstrækkeligt, at undervisningen kun tager udgangspunkt i lovgivningens krav. Undervisningen skal også berøre spiludbyderens virksomhed og de konkrete forhold, der knytter sig hertil i relation til bekæmpelse af hvidvask og terrorfinansiering.

Der er alene krav om, at der skal ske undervisning inden for de arbejdsområder, der er relevante for de enkelte ansatte. Det betyder, at spiludbyderen skal tage stilling til, hvilke ansatte der skal undervises i hvidvasklovens krav. Der er ikke krav om undervisning af ansatte, der ikke varetager funktioner, der relaterer sig til hvidvask eller terrorfinansiering.

Undervisningen skal sikre, at de relevante ansatte har kendskab til de regler og pligter, der gælder på hvidvaskområdet, så de kan varetage deres arbejde på betryggende vis og i overensstemmelse med lovgivningens krav.

Kravet om tilstrækkelig undervisning betyder derudover, at der skal ske efteruddannelse af de ansatte og ledelsen med passende mellemrum, herunder eksempelvis ved opdatering af spiludbyderens risikovurdering og forretningsgange, når det har betydning for den ansattes arbejdsfunktion.

Det er vigtigt, at spiludbyderen sikrer, at de ansatte faktisk deltager i undervisningen.

5.2.1 Særligt om forhandlere af landbaserede væddemål

5.2.1.1 Egne forhandlere
Spiludbyderen er som anført ovenfor forpligtet til efter hvidvasklovens § 8, stk. 6, at undervise egne ansatte.

En spiludbyders egne ansatte omfatter også udbyderens egne forhandlere af landbaserede væddemål - det vil sige, forhandlere og ansatte i spiludbyderens egne butikker.

5.2.1.2 Eksterne forhandlere
En ekstern forhandler og forhandlerens ansatte kan, modsat ansatte i spiludbyderens egne butikker, ikke betragtes som ansatte ved spiludbyderen. Dette betyder, at undervisningsforpligtelsen i § 8, stk. 6, ikke kan udstrækkes til de eksterne forhandlere.

Hvis en spiludbyder sælger sine produkter ved en ekstern forhandler og dermed fx outsourcer gennemførelsen af kundekendskabsprocedurer til den eksterne forhandler, skal spiludbyderen sikre sig, at forhandleren har den fornødne evne til at varetage opgaven på en tilfredsstillende måde. Dette kan fx ske ved, at spiludbyderen underviser den eksterne forhandler.

Se afsnit 7.3.6 om spiludbydernes mulighed for at undervise eksterne forhandlere og forhandlerens ansatte, når der er sket outsourcing af en forpligtelse efter hvidvaskloven.

5.3 Koncernforbundne virksomheder

Hvidvasklovens § 9

Det er et krav, at koncernforbundne virksomheder udover kravene i hvidvasklovens § 8 tillige har skriftlige politikker og forretningsgange for databeskyttelse og udveksling af oplysninger, der udveksles med det formål at bekæmpe hvidvask og terrorfinansiering, inden for koncernen. Det fremgår af hvidvasklovens § 9.

Det er vigtigt at understrege, at kravene kun gælder de virksomheder inden for koncernen, som er omfattet af hvidvaskloven. Som eksempel kan nævnes, at et datterselskab, der ikke er omfattet af hvidvaskloven, således heller ikke er underlagt disse krav.

Procedurerne omkring udveksling af oplysninger i koncernen skal overholde databeskyttelseslovgivningens regler herom.

Der er ligeledes krav om, at risikovurdering, politikker og forretningsgange i et moderselskab dækker hele koncernen, vel at mærke de dele, der er omfattet af hvidvaskloven. I praksis betyder dette, at procedurerne kan udarbejdes fra centralt hold i eksempelvis moderselskabet, men det kræves dog, at de enkelte procedurer er tilpasset den konkrete juridiske enheds forhold.

Kundekendskabsproce-durer

6

6.1 Formålet med kundekendskabsprocedurer

Hvidvasklovens §§ 10-18

Det er et grundlæggende krav i hvidvaskloven, at spiludbydere skal kende deres kunder. Det gælder uanset, om man udbyder spil online eller landbaseret. Formålet med kundekendskabsprocedurer er, at spiludbyderen ved, hvem virksomhedens kunder er, og hvad der er kundens formål med kundeforholdet. For en spiludbyder er det således vigtigt at sikre sig, at kundens formål med at spille ikke er at forsøge at hvidvaske penge eller finansiere terrorisme.

Spiludbyderen skal forholde sig til ændringer i kundeforholdet i et omfang, der bør påkalde sig opmærksomhed, fx hvis en kunde, der normalt kun spiller væddemål, lige pludselig kun spiller på gevinstgivende spilleautomater. For at kunne sikre dette, kræver det, at spiludbyderen kender sine kunder., og at de har forretningsgange for, hvad der skal iagttages og iværksættes, hvis der er tegn på forsøg på hvidvask eller terrorfinansiering.

Reglerne for kundekendskabsprocedurer fremgår af hvidvasklovens kapitel 3, §§ 10-21.

Det bemærkes, at der findes en række bekendtgørelser[5], som regulerer de konkrete udbud af spil, og at disse ligeledes indeholder en række regler om kundekendskab. Spiludbydere skal derfor være opmærksom på dette og sørge for at overholde alle regelsæt.

Spiludbydere skal fx være opmærksomme på, at selvom der er en række sammenfald mellem de identitetsoplysninger, som skal indhentes om kunden, vil en opfyldelse af kravene efter spillelovgivningen ikke nødvendigvis være det samme som, at udbyderen opfylder kravene efter hvidvaskloven. Fx er kravet til kvaliteten af dokumentationskilder større efter hvidvaskloven, end den er i forhold til spillelovgivningen.

6.2 Hvornår skal der gennemføres kundekendskabsprocedurer?

Hvidvasklovens § 10

En spiludbyder skal gennemføre kundekendskabsprocedurer i følgende situationer:

1. Når der etableres en forretningsforbindelse
2. Når en kundes relevante omstændigheder ændrer sig
3. På passende tidspunkter
4. Ved udbud af spil, hvor indsats eller udbetaling af gevinster (eller begge dele) er på mindst 2.000 euro
5. Ved mistanke om hvidvask eller finansiering af terrorisme
6. Ved tvivl om tidligere indhentede oplysninger om kunden

Nedenfor følger en nærmere gennemgang af ovenstående situationer.

6.2.1 Når der etableres en forretningsforbindelse

Spiludbyderen skal gennemføre kundekendskabsprocedurer, når der etableres en forretningsforbindelse. En forretningsforbindelse defineres som et kundeforhold, der på etableringstidspunktet forventes at blive af en vis varighed. Det fremgår af hvidvasklovens § 2, stk. 1, nr. 3.

[5] Bekendtgørelse om online kasino, bekendtgørelse om online væddemål, bekendtgørelse om landbaserede væddemål og bekendtgørelse om landbaserede kasinoer

Der vil være tale om etablering af en forretningsforbindelse, hvis virksomheden vurderer, at kunden vil benytte sig af virksomhedens ydelser gentagne gange og dermed vil være en jævnlig tilbagevendende kunde. Der er altid tale om etablering af en forretningsforbindelse, hvis en kunde får oprettet en konto, herunder en spilkonto eller lignende hos virksomheden.

Modsat er der ved enkeltstående transaktioner eller aktiviteter for kunder som omhandlet i hvidvasklovens § 10, nr. 3, ikke en forventning om, at kundeforholdet vil blive af en vis varighed. Når et kundeforhold ikke kategoriseres som en forretningsforbindelse, karakteriseres kundeforholdet som en enkeltstående transaktion.

6.2.1.1 Online spil
For at blive registreret som kunde hos en online spiludbyder er det et krav, at kunden registrerer sig, og at der oprettes en spilkonto. En spiludbyder etablerer derfor en forretningsforbindelse med en kunde i det øjeblik, hvor der oprettes en spilkonto til kunden.

6.2.1.2 Landbaseret væddemål
For at kunne indgå et væddemål hos en udbyder af landbaserede væddemål er det en betingelse, at kunden registreres hos spiludbyderen. Kunden får i den forbindelse udstedt et identifikationsmiddel (spilkort), hvortil der er tilknyttet en spilkonto. Der etableres således en forretningsforbindelse med kunden ved oprettelse af et spilkort med dertilhørende spilkonto.

6.2.1.3 Landbaseret kasino
På et landbaseret kasino bliver alle kunder registreret ved ankomsten. Det er dog forskelligt, om kunden i hvidvasklovens forstand vil anses for at være en forretningsforbindelse, eller om der udføres en enkeltstående transaktion for kunden.

For at en kunde skal betragtes som en forretningsforbindelse kræver det som anført under afsnit 6.2.1, at det må forventes, at relationen mellem spiludbyderen og kunden får en vis varighed. Hvad der nærmere ligger i "en vis varighed" er op til spiludbyderen at definere. Det må dog forventes, at relationen er af en vis varighed, og dermed omfattet af definitionen af en forretningsforbindelse, hvis den samme kunde vender tilbage med jævne mellemrum til det samme kasino.

Hvis kunden har et uge-, måneds-, eller årskort betragtes kunden som en forretningsforbindelse.

Modsat vil kunder, der ikke har et uge- måneds- eller årskort og hvor de ikke må forventes, at relationen med kunden får en vis varighed, skulle betragtes som enkeltstående transaktioner. Dette kan fx omfatte lejlighedskunder som turister mv.

Det bemærkes, at et kasino i henhold til bekendtgørelsen om landbaserede kasinoer er forpligtet til at registrere og kontrollerer navn, adresse, cpr-nummer og ankomsttidspunkt for alle kunder, uanset om der er tale om en forretningsforbindelse eller en enkeltstående transaktion.

6.2.2 Når en kundes relevante omstændigheder ændrer sig

Spiludbyderen skal gennemføre kundekendskabsprocedurer på ny, hvis en forretningsforbindelses relevante omstændigheder ændrer sig. Det kan fx være, hvis en kunde får status som politisk eksponeret person (PEP) eller hvis kundens adfærd/spilmønster ændrer sig væsentligt, fx ved at kunden begynder at spille på en anden måde og for højere beløb end tidligere. Spiludbyderen skal ud fra en risikovurdering tage stilling til, om der på grund af de ændrede forhold skal indhentes nye oplysninger om kunden, herunder fx identitetsoplysninger eller lignende på ny. Det afhænger af den konkrete situation, hvilke oplysninger, der skal indhentes. Det kan fx være tilstrækkeligt at foretage yderligere foranstaltninger for at kontrollere en kundes identitet, hvis spiludbyderen bliver opmærksom på, at en kunde har skiftet navn eller

cpr-nummer. I andre situationer, fx hvis kundens adfærd ændrer sig, er det ikke sikkert, at det er tilstrækkeligt kun at kontrollere kundens identitetsoplysninger.

Kundekendskabsproceduren skal gennemføres, når spiludbyderen bliver bekendt med de ændrede omstændigheder, hvilket fx være gennem spiludbyderens løbende overvågning af kunden.

6.2.3 På passende tidspunkter

Der påhviler ligeledes spiludbyderen en forpligtelse til at gennemføre kundekendskabsprocedurer på passende tidspunkter, hvilket vil sige med passende faste intervaller i kundeforholdet med forretningsforbindelsen. Dette skal sikre, at de oplysninger, som spiludbyderen har om kunden, er korrekte og tilstrækkelige. Spiludbyderen skal derfor ud over at gennemføre kundekendskabsprocedurer, hvis en kundes relevante omstændigheder ændrer sig, også sikre, at det sker med passende faste intervaller.

Kravet kan ikke fraviges, og spiludbyderen skal fastsætte, hvad passende intervaller er på et risikobaseret grundlag. Det betyder, at intervallet kan fastsættes ud fra en risikovurdering af den enkelte kunde, og kunderne kan med fordel opdeles i grupper (fx begrænset risiko, mellem eller øget risiko) alt afhængig af eksempelvis spilaktivitet, spilforbrug og så videre. Der kan herefter fastsættes intervaller for de pågældende kundegrupper, så der fx fastsættes ét interval for kunder med mellem risiko og et andet interval for kunder med øget risiko. Vurderingen kan ikke føre til, at der ikke skal gennemføres kundekendskabsprocedurer.

Den risikobaserede tilgang betyder, at spiludbydere skal anvende deres ressourcer der, hvor der er øget risiko, hvorfor der for kunder med lavere risiko ikke nødvendigvis er behov for nær så jævnlige gentagne procedurer. Omfanget af kundekendskabsproceduren fastlægges ud fra en risikovurdering af kundeforholdet. Der er ikke krav til, hvordan kundekendskabsproceduren gennemføres, og dette kan derfor både ske ved fx en automatiseret eller manuel proces. Kravene til spiludbyderens processer afhænger af virksomhedens størrelse, og der stilles således større krav til store spiludbyderes processer.

6.2.4 Udbud af spil, hvor indsats eller udbetaling af gevinst (eller begge dele) er på mindst 2.000 euro

Spiludbyderen er forpligtet til at gennemføre kundekendskabsprocedurer, i de tilfælde, hvor kunden lægger en indsats, får udbetalt en gevinst eller begge dele på mindst 2.000 euro, hvad enten transaktionen sker på én gang eller som flere transaktioner, der ser ud til at være indbyrdes forbundet. Dette gælder dog kun i de tilfælde, hvor der ikke er etableret en forretningsforbindelse og der dermed allerede er gennemført kundekendskabsprocedurer.

6.2.5 Mistanke om hvidvask eller terrorfinansiering

Det er et krav, at spiludbyderen foretager kundekendskabsprocedurer i de tilfælde, hvor spiludbyderen har viden eller mistanke om hvidvask eller finansiering af terrorisme. Kravet gælder også selvom en indsats eller udbetaling af en gevinst eller begge dele er under 2000 euro.

Hvis kunden nægter at afgive nødvendige oplysninger for at kunne gennemføre kundekendskabsproceduren, skal spiludbyderen foretage en underretning til Hvidvasksekretariatet med de oplysninger, som spiludbyderen er i besiddelse af.

Se i øvrigt afsnit 6.6 om afvikling af en etableret forretningsforbindelse og utilstrækkelige oplysninger og afsnit 9 om underretningspligten.

6.2.6 Ved tvivl om tidligere indhentede oplysninger om kunden

Hvis spiludbyderen får grund til at så tvivl om, hvorvidt tidligere indhentede oplysninger om kunden er korrekte eller tilstrækkelige, er spiludbyderen forpligtet til at gennemføre kundekendskabsprocedurer på ny.

Der skal foretages en konkret vurdering af, hvilke oplysninger der er nødvendige at indhente. Spiludbyderen skal ud fra en risikovurdering vurdere, om det er hele eller kun dele af kundekendskabsproceduren, der skal gennemføres igen. Dette kan også afhænge af, om der er tale om utilstrækkelige oplysninger eller oplysninger, der ikke er korrekte.

6.3 Hvad består kundekendskabsprocedurer af?

Hvidvasklovens § 11

De almindelige krav til kundekendskabsprocedurer fremgår af hvidvasklovens § 11.

6.3.1 Indhentelse af identitetsoplysninger

Spiludbydere skal indhente en kundes identitetsoplysninger. Dette omfatter kundens navn og cpr-nummer eller lignende. Hvis kunden ikke har et cpr-nummer eller lignende, skal spiludbyderen indhente kundens fødselsdato.

For kunder, der ikke bor i Danmark, kan et alternativ til cpr-nummer fx være et nationalt id-nummer. Anvendes en kundes nationale id-nummer, er det væsentligt, at der er tale om et unikt nummer, og at nummeret er varigt eller i hvert fald kundens aktive nationale nummer. Fødselsdato kan alene anvendes i det relativt sjældne tilfælde, hvor der ikke foreligger et unikt nummer.

6.3.2 Kontrol af identitetsoplysninger

Identitetsoplysningerne indhentet fra kunden skal kontrolleres ved dokumenter, data eller oplysninger, som stammer fra en pålidelig og uafhængig kilde. Herved forstås eksempelvis elektroniske identifikationsmidler, relevante tillidstjenester eller enhver anden sikker form for fjernidentifikationsproces eller elektronisk identifikationsproces, der er reguleret, anerkendt, godkendt eller accepteret af de kompetente nationale myndigheder. Kontrollen af kundens oplysninger skal således ske gennem en anden kilde end kunden.

Spiludbyderen skal sikre sig, at der er tale om en aktuel kilde, hvilket er særlig relevant, når det omhandler id-dokumenter og gyldigheden af disse. Dette kan fx være id-dokumenter såsom pas, kørekort, nationale id-kort og lignende.

Hvis spiludbyderen vurderer, at der er øget risiko ved kunden, skal der foretages yderligere handlinger, uanset om kundens identitetsoplysninger er kontrolleret. Det er i øvrigt en konkret vurdering, hvor meget dokumentation der skal foreligge, for at der kan siges at være tilstrækkelig kontrol af kundens oplysninger. Der må dog i den konkrete situation ikke være anledning til tvivl om, at kunden er den person, som kunden udgiver sig for at være.

Supplerende dokumentation kan være:

- søgning i en database som cpr-registret
- indsendelse af billedlegitimation
- krav om, at første indbetaling sker ved en overførsel fra kundens konto i et pengeinstitut, hvor kunden har identificeret sig
- kunden kontaktes telefonisk, idet telefonnummeret skal være kontrolleret ved pålideligt opslag.

I situationer, hvor kunden er fysisk fremmødt, vil kontrol i form af billedlegitimation give spiludbyderen større sikkerhed for, at kunden er den person, denne udgiver sig for at være.

I situationer, hvor kunden og spiludbyderen ikke mødes fysisk (distanceforhold), er der øget behov for, at spiludbyderen har mitigerende tiltag, som kan sikre, at kunden reelt set er den person, som vedkommende udgiver sig for at være.

Hvad angår MitID og brugen heraf som kontrolkilde, bemærkes det, at MitID kan stå alene som elektronisk kontrolkilde for kunder, der ikke er underlagt skærpede kundekendskabsprocedurer. Det betyder, at spiludbyderen kan indhente identitetsoplysninger og foretage kontrol heraf i forhold til kunder der udgør en begrænset eller mellem risiko, men ikke ved kunder, der udgør en øget risiko. Har spiludbyderen således vurderet, at en kunde udgør en øget risiko, skal spiludbyderen foretage yderligere kontrol af kundens identitetsoplysninger. Den yderligere kontrol kan fx være at spiludbyderen kræver yderligere dokumenter fra kunden, foretager opslag i eksterne kilder eller kræver, at første indbetaling sker som en bankoverførsel. For nærmere oplysninger om MitID som kontrolkilde henvises til Finanstilsynets vejledning om anvendelse af MitID som kontrolkilde i kundekendskabsprocedurer.

6.3.2.1 Særligt for landbaserede kasinoer
Ved registrering ved fysisk fremmøde skal kunden fremvise legitimation, der bekræfter de registrerede oplysninger om kunden. Det kan fx være pas eller kørekort.

Kasinoet skal være overbevist om, at kunden er den, som kunden udgiver sig for at være. Der må derved ikke være omstændigheder, der kan give anledning til tvivl om, at kunden er den, som fremgår af legitimationsdokumenterne.

6.3.2.2 Midlertidige spilkonti
Hvis spiludbyderen ved registreringen af kunden ikke øjeblikkelig kan kontrollere kundens identitetsoplysninger, kan der oprettes en midlertidig spilkonto. Det fremgår af hvidvasklovens § 14, stk. 4. Hvis spiludbyderens kontrol af identitetsoplysningerne sker øjeblikkelig, fx ved brug af MitID, er der ikke tale om en midlertidig spilkonto men en verificeret spilkonto.

Hvis spiludbyderen har oprettet en midlertidig spilkonto til kunden, skal kontrollen af kundens identitetsoplysninger gennemføres hurtigst muligt og senest inden for 30 dage efter registrering af kunden. Kan kontrollen af identitetsoplysningerne ikke gennemføres, skal den midlertidige spilkonto lukkes. Reglerne om midlertidig spilkonto reguleres i spillelovgivningen.

Hvis spiludbyderen ikke kan gennemføre kontrollen af identitetsoplysningerne, fx fordi kunden har afgivet forkerte identitetsoplysninger, kan det i sig selv være mistænkeligt. Det samme kan gøre sig gældende, hvis spiludbyderen af andre årsager ikke kan gennemføre kontrollen af identitetsoplysningerne. Spiludbyderen skal i sådanne tilfælde overveje om der skal foretages en underretning til Hvidvasksekretariatet.

6.3.3 Formål og tilsigtet beskaffenhed

Spiludbydere skal vurdere og hvor det er relevant indhente oplysninger om en forretningsforbindelses formål og tilsigtede beskaffenhed. Det fremgår af hvidvasklovens § 11, stk. 1, nr. 4. Vurderingen skal ske ved etablering af forretningsforbindelsen og løbende gennem kundeforholdet. Det betyder derfor, at spiludbyderen skal foretage vurderingen, når kunden opretter en online spilkonto eller fx et uge- måneds- eller årskort til et landbaseret kasino.

Spiludbydere skal således i alle tilfælde vurdere forretningsforbindelsens formål og tilsigtede beskaffenhed. Kun hvis det er relevant, skal spiludbyderen også indhente oplysninger herom

fra kunden. Hvorvidt det er relevant at indhente oplysninger fra kunden, er en konkret vurdering.

Når spiludbyderen har viden om kundens formål og tilsigtede beskaffenhed, kan spiludbyderen bedre vurdere, om kundens formål med at benytte virksomheden er legitimt og dermed få en bedre indsigt i kundens risikoprofil.

Når en kunde opretter en spilkonto eller besøger et kasino er udgangspunktet at kundens formål er at spille. Dette skyldes, at spiludbydernes forretningsmodel er begrænset til udelukkende at udbyde spilprodukter.

I forbindelse med vurderingen af kundens formål med forretningsforbindelsen kan spiludbyderen inddrage oplysninger om antallet, størrelsen og omfanget af de transaktioner, som kunden forventes at gennemføre. Det vil sige, hvor mange penge kunden har tænkt sig at spille for og hvor ofte kunden vil spille. Spiludbyderen kan foretage vurderingen ud fra de oplysninger, som de allerede har om kunden, det kan fx være oplysninger om indbetalingsgrænse eller ved at bede kunden om oplysningerne.

Spiludbydere skal derudover vurdere forretningsforbindelsens tilsigtede beskaffenhed. Det betyder, at spiludbyderen skal kende de egenskaber og forhold, der tilsammen giver forretningsforbindelsen dens særpræg. Det kan i den forbindelse fx være relevant at forstå kundens indtægts- og formueforhold, altså hvordan kunden vil finansiere sit spil.

Spiludbyderen skal bruge oplysningerne om kundens midler til at vurdere om kundens indtægtsforhold stemmer overens med kundens forventede og løbende forbrug. Hvis spiludbyderen fx har kendskab til at kunden ikke har en indtægt skal disse oplysninger inddrages i spiludbyderens tilrettelæggelse af overvågningen af kunden, så spiludbyderen kan blive opmærksom på, hvis kundens spilforbrug ikke harmonerer med kundens indkomst- og formueforhold.

Det vil oftest være nødvendigt at spiludbyderen indhenter oplysningerne ved kunden, da det ellers kan være vanskeligt at fastlægge kundens formueforhold, fx ved brug af open source-søgninger.

6.3.4 Løbende overvågning

Spiludbydere skal løbende overvåge en etableret forretningsforbindelse. Det fremgår af hvidvasklovens § 11, stk. 1, nr. 5. Kravet gælder både i forhold til transaktioner, som kunden foretager og i forhold til kundens andre aktiviteter, generelt betegnet som kundens adfærd.

Det er op til spiludbyderen hvordan overvågningen skal foretages og dette kan ske både manuelt og systemisk. For en spiludbyder vil overvågningen typisk kræve en effektiv it-løsning grundet omfanget af kunder og kompleksiteten af produkter og transaktioner, men dette er ikke et krav, så længe det sikres, at der foretages den fornødne overvågning.

Formålet med overvågningen er at sikre, at transaktionerne er i overensstemmelse med spiludbyderens viden om kunden og kundens forretnings- og risikoprofil, herunder om nødvendigt midlernes oprindelse. Det betyder, at spiludbyderen løbende skal overvåge, om der forekommer usædvanlige transaktioner eller aktiviteter. Dette kan fx være usædvanlige transaktioner eller aktivitet på kundens spilkonto, set i forhold til den viden, som spiludbyderen har om kunden, og samtidig om kundens transaktioner og aktiviteter er overensstemmende med andre kunder med samme forretnings- og risikoprofil.

Kundens forretningsprofil defineres som oplysninger om formålet med forretningsforbindelsen, omfanget og størrelse af transaktioner, hyppighed og varighed.

Ved kundens risikoprofil forstås, at overvågningen skal ske ud fra den profil af kunden, som spiludbyderen er kommet frem til på baggrund af sin risikovurdering af kunden. En risikovurdering kan aldrig føre til, at en forretningsforbindelse ikke overvåges.

Spiludbyderen skal tilpasse overvågningen til den enkelte kunde. Overvågningen skal løbende justeres på baggrund af spiludbyderens kendskab til kunden, herunder hvis kundens risikoprofil ændres. Hvis en kundes forretnings- og risikoprofil ændrer sig, skal spiludbyderen justere overvågningen af kunden. Hvis der er tale om, at virksomheden har foretaget en undersøgelse af kunden på baggrund af mistænkelige forhold, kan det være relevant at udvide overvågningen. Se afsnit 8.1.2. For at kunne indrette og gennemføre tilstrækkelig overvågning af den enkelte kunde, er det væsentligt, at de oplysninger, som spiludbyderen har om kunden er opdaterede og korrekte.

Hvis en transaktion er usædvanlig ud fra spiludbyderens viden om kundens formueforhold, skal spiludbyderen ud fra en risikovurdering indhente oplysninger om oprindelsen af kundens midler. Spiludbyderen skal i det tilfælde kende oprindelsen af midlerne. Det vil typisk ikke være tilstrækkeligt blot at indhente yderligere oplysninger fra kunden om midlernes oprindelse. Spiludbyderen skal indhente dokumentation fx. i form af lønsedler, årsopgørelser, boopgørelse eller lignende.

Midlernes oprindelse dækker over oplysninger om,
- hvorfra kundens formue oprinder,
- hvorfra de midler, der indgår i transaktionen, oprinder, eller
- hvor midlerne, der er en del af forretningsforbindelsen, kommer fra.

Det er således relevant at undersøge, hvilke værdier eller hvilken formue kunden har, samt hvordan kunden tjener sine penge. I forbindelse med en transaktion kan det dermed være nødvendigt at foretage en undersøgelse af alle tre forhold for at undersøge, om en transaktion er sædvanlig eller usædvanlig for den pågældende kunde. Dermed har spiludbyderen mulighed for at kunne be- eller afkræfte en mistanke om hvidvask. Det kan fx være hvis en kunde har indsat et stort beløb, som spiludbyderen vurderer, er usædvanligt for kunden, hvorefter spiludbyderen fx indhenter oplysninger og dokumentation for oprindelsen af de midler, som kunden har indsat. I forhold til de skærpede kundekendskabskrav kan det være nødvendigt i relation til kunder, der vurderes som øget risiko at kende midlers oprindelse, inden der foretages transaktioner for kunden.

6.3.4.1 Særligt for landbaserede kasinoer

Nogle kunder på et landbaseret kasino vil skulle betragtes som enkeltstående transaktioner. Nogle kunder, kan dog være forretningsforbindelser, som kasinoet er forpligtet til løbende at overvåge. Det er som anført ovenfor op til kasinoet, hvordan kasinoet vil indrette overvågningen, herunder om dette skal ske manuelt, systemisk eller ved en kombination af disse. Det væsentlige er, at den overvågning, der iværksættes, er tilstrækkelig til at overvåge kundens transaktioner og adfærd, som anført ovenfor.

6.4 Risikovurdering af kunden

Spiludbyderen skal gennemføre alle kundekendskabskrav efter hvidvasklovens § 11, stk. 1 og 2. Omfanget af kundekendskabsprocedurerne afhænger af en risikovurdering. Det fremgår af hvidvasklovens § 11, stk. 3.

Spiludbyderen skal være opmærksom på, at en risikovurdering af kunden aldrig kan føre til, at der ikke gennemføres kundekendskabsprocedurer. Det betyder, at selv i tilfælde, hvor spiludbyderen har vurderet, at en kunde udgør en begrænset risiko, kan spiludbyderen ikke undlade at kontrollere kundens identitetsoplysninger.

Spiludbyderen skal som minimum inddrage følgende i risikovurderingen af kunden:
- Formål

- Omfang
- Regelmæssighed
- varighed

Spiludbyderen skal foretage en vurdering af risikoen ved den enkelte kunde, når spiludbyderen etablerer en forretningsforbindelse. Det vil sige, når en kunde opretter en spilkonto eller fx et uge-måneds- eller årskort til et landbaseret kasino. Spiludbyderen skal derudover afdække relevante risikofaktorer ved kunden for at vurdere omfanget af de kundekendskabsproceduer, der skal gennemføres. Den overordnede risikovurdering efter hvidvasklovens § 7, stk. 1, skal spiludbyderen anvende til at vurdere niveauet for kundekendskabsproceduren i det enkelte kundeforhold.

Formålet med risikovurderingen af kunden er, at spiludbyderen skal forstå, hvor og i hvilket omfang den enkelte kunde kan misbruge spiludbyderen til hvidvask og terrorfinansiering. Risikovurderingen af kunden skal bruges til at kunne fastlægge omfanget af kundekendskabsproceduren. For kunder, som udgør en øget risiko betyder det, at der skal iværksættes yderligere foranstaltninger.

Risikovurderingen af kunden indebærer, at spiludbyderen skal identificere og vurdere risikofaktorer, som kan have betydning for kundens risiko. Hvidvasklovens bilag 2 og 3 oplister en række risikofaktorer, der kan medføre henholdsvis begrænset og øget risiko. Spiludbyderen skal tage udgangspunkt i de risikofaktorer, der er oplistet i bilagene. Det betyder, at spiludbyderens risikovurdering af kunden skal omfatte oplysninger om, hvorvidt kunden er bosiddende i lande, som er opført på FATF's grå og sorte liste, og som dermed medvirker til, at kundens risiko øges. Det er dog vigtigt at fremhæve, at der ikke er tale om udtømmende lister, hvorfor spiludbyderen om nødvendigt skal inddrage og indsamle andre relevante oplysninger om kunden, så spiludbyderen sikrer, at alle relevante risikofaktorer er afdækket. Spiludbyderen kan fx inddrage de produkter og betalingsløsninger, som kunden anvender.

Ved vurdering af risikofaktorer forstås, at spiludbyderen ud fra en holistisk betragtning skal vurdere, i hvilket omfang de identificerede risikofaktorer udsætter virksomheden for at blive misbrugt til hvidvask eller terrorfinansiering. En måde at vurdere risici kan være at vægte de enkelte risikofaktorer, der medfører den samlede risikovurdering af kunden. Resultatet af vurderingen af de relevante risikofaktorer er derefter udtryk for risikovurderingen af kunden. I praksis kan spiludbyderen vælge at inddele kunderne i forskellige niveauer eller risikoprofiler fx begrænset risiko, mellem risiko og øget risiko.

Eksempel

En kunde opretter en spilkonto hos en spiludbyder, der udbyder onlinekasino og væddemål. Kunden spiller udelukkende spil mod andre kunder og finansierer sit spil med flere forskellige betalingsløsninger, herunder betalingskort og e-wallet. Kunden er bosiddende i Danmark og har tilkendegivet, at vedkommende forventer at spille for 15.000 kr. om måneden. Spiludbyderen vurderer på baggrund af de konkrete oplysninger om kunden og spiludbyderens forretningsmodel i øvrigt, at kunden udgør en øget risiko.

Det fremgår af hvidvasklovens § 11, stk. 4, at spiludbyderen skal kunne godtgøre, at risikovurderingen af den enkelte kunde er tilstrækkelig i forhold til risikoen for hvidvask og terrorfinansiering Det betyder, at spiludbyderen skal sikre sig, at spiludbyderen anvender tilstrækkelige oplysninger til at kunne foretage en saglig risikovurdering af kunden, hvor alle relevante risikofaktorer er taget i betragtning.

Spiludbyderen skal være opmærksom på, at kundens risikoprofil kan ændres under kundeforholdet. Det kan fx være, at spiludbyderen finder ud af, at kunden er blevet en politisk eksponeret person, eller at kunden som noget nyt begynder at anvende spiludbyderens produkter og betalingsløsninger, som er forbundet med en øget risiko. Det kan også være, at kunden gentagne gange placerer væddemål på begivenheder, som er observeret i enten egne

eller eksterne alarmsystemer, som en mulig manipuleret begivenhed (matchfixing). De nye oplysninger om kunden kan resultere i, at kundens risikoprofil ændrer sig fra begrænset risiko til øget risiko eller omvendt.

Spiludbyderens forpligtelse til at gennemføre kundekendskabsprocedurer skal opfyldes gennem hele kundeforholdet. Spiludbyderen er derfor forpligtet til løbende at opdatere kundens risikoprofil.

6.5 Skærpede kundekendskabsprocedurer

Der gælder et krav om skærpede kundekendskabsprocedurer i en række tilfælde, hvor der vurderes at være en øget risiko for hvidvask eller terrorfinansiering.

Hvad de skærpede kundekendskabsprocedurer konkret skal bestå i, vil være op til spiludbyderen at definere ud fra den risikovurdering, der i øvrigt er foretaget af spiludbyderen med henblik på de situationer, hvor der er skærpede krav.

Der er desuden krav om skærpede kundekendskabsprocedurer, hvis kunden har hjemsted i et land, der er opført på Europa-Kommissionens liste over højrisikotredjelande, eller hvis kunden er en politisk eksponeret person. Begge omstændigheder gennemgås nedenfor under afsnit 6.5.2 og 6.5.3.

6.5.1 Kunder, der udgør en øget risiko for hvidvask

Hvidvasklovens § 17, stk. 1

Der skal iværksættes skærpede kundekendskabsprocedurer, hvis en spiludbyder vurderer, at en kunde udgør en øget risiko for hvidvask eller terrorfinansiering. Det fremgår af hvidvasklovens § 17, stk. 1.

Skærpede kundekendskabsprocedurer anvendes ud over de almindelige kundekendskabsprocedurer, der følger af hvidvasklovens § 11. Det betyder, at de skærpede kundekendskabsprocedurer supplerer de almindelige procedurer i de situationer, hvor der er øget risiko for hvidvask og terrorfinansiering. Spiludbyderen skal på baggrund af en risikovurdering af kunden således tage stilling til, hvilke yderligere foranstaltninger der er påkrævet for at håndtere den øgede risiko kunden udgør.

Skærpede kundekendskabsprocedurer betyder således, at spiludbyderen skal iværksætte yderligere foranstaltninger for at håndtere de øgede risici, som den konkrete kunde medfører.

Det er op til spiludbyderen at vurdere, hvorvidt der foreligger en øget risiko, men spiludbyderen skal i vurderingen tage de højrisikofaktorer i betragtning som fremgår af bilag 3 til hvidvaskloven, samt andre højrisikofaktorer, som vurderes at være relevante.

Der kan derfor ikke gives en udtømmende liste over, hvilke situationer der medfører skærpede kundekendskabsprocedurer, og hvad disse ultimativt skal omfatte, da det er spiludbyderen, der på baggrund af sin risikovurdering skal vurdere, hvad der kan begrænse den øgede risiko for hvidvask og/eller terrorfinansiering. Det er den samlede vurdering af alle risikofaktorer, der fastlægger risikoen ved den enkelte kunde. Bilag 3 er en ikke udtømmende liste og spiludbyderen skal inddrage andre risikofaktorer alt efter spiludbyderens produkter, kundetyper mv., jf. hvidvasklovens § 7. Som udgangspunkt skal der dog altid iværksættes øget overvågning af en kunde der udgør en øget risiko med henblik på at afgøre om transaktioner eller aktiviteter er mistænkelige.

Spiludbyderen skal kunne godtgøre, at de iværksatte foranstaltninger i forhold til kundekendskab, er tilstrækkelige i forhold til risikoen for hvidvask og terrorfinansiering.

6.5.1.1 Hvornår skal vurderingen foretages?
Spiludbyderen skal i forbindelse med etableringen af forretningsforbindelsen vurdere, om kunden udgør en øget risiko.

Skærpede kundekendskabsprocedurer skal gennemføres i hele kundeforholdet. Risikovurderingen af den enkelte kunde kan ændre sig i løbet af kundeforholdet, fx hvis kunden ikke længere benytter et produkt, der har medført, at kunden er vurderet til at udgøre en øget risiko eller hvis kundens transaktionsmønster ændrer sig.

Modsat kan en kunde, der ikke tidligere har udgjort en øget risiko fx ændre transaktionsmønster eller få et usædvanligt spilmønster i forhold til tidligere, og hvor spiludbyderen derfor vurderer, at kunden nu udgør en øget risiko. I sådanne tilfælde skal spiludbyderen iværksætte skærpede kundekendskabsprocedurer, selvom kunden ikke tidligere har udgjort en øget risiko. Det forhold at spiludbyderen adskillige gange har underrettet Hvidvasksekretariatet om kunden kan også indgå i vurderingen af, om kunden udgør en øget risiko.

Spiludbyderen kan som følge af den løbende overvågning af kunden fx blive opmærksom på, at kunden ændrer transaktionsmønster. Dette vil udgøre en risiko, som kan føre til, at spiludbyderen foretager skærpede kundekendskabsprocedurer over for den pågældende kunde. Spiludbyderen kan i den forbindelse fx indhente oplysninger om midlernes oprindelse, altså hvordan kunden finansierer sit spil.

6.5.1.2 Hvad består skærpede kundekendskabsprocedurer af?
Der kan som anført ikke gives en udtømmende liste for hvad skærpede kundekendskabsprocedurer består af.

Spiludbyderen skal på baggrund af vurderingen af kunden tage stilling til, hvilke foranstaltninger der skal gennemføres.

Skærpede kundekendskabsprocedurer kan fx være:

- Indhentelse af oplysninger om adresse eller fødested (adresseoplysninger kan også være nødvendige for at afdække risikofaktorerne i kundeforholdet).
- Indhentelse af yderligere information om kunden (formål og tilsigtet beskaffenhed).
- Kontrol af kundens identitetsoplysninger ved flere uafhængige og pålidelige kilder.
- Indhentelse af oplysninger om kundens formue og midlers oprindelse.
- Gennemførelse af kundekendskabsprocedurer med et kortere interval.
- Løbende undersøgelse af kundens transaktioner.

6.5.2 Kunder fra højrisikotredjelande

Hvidvasklovens § 17, stk. 2

En spiludbyder skal gennemføre skærpede kundekendskabsprocedurer, hvis kunden har hjemsted i et land, der er opført på Europa-Kommissionens liste over højrisikotredjelande. Dette gælder uanset spiludbyderens risikovurdering af kunden. Det fremgår af hvidvasklovens § 17, stk. 2.

Det betyder, at en spiludbyder skal være opmærksom på Europa-Kommissions liste og om nye eller eksisterende kunder har eller har fået hjemsted i et af de oplistede lande.

6.5.2.1 Hvad omfatter de skærpede kundekendskabsprocedurer?
Hvis kunden har hjemsted i et højrisikotredjeland, omfatter de skærpede kundekendskabsprocedurer følgende:

1. Indhentelse af yderligere oplysninger om kunden

- Det kan fx være oplysning om kundens adresse eller fødested.

2. Indhentelse af yderligere oplysninger om forretningsforbindelsens tilsigtede karakter.
3. Indhentelse af oplysninger om midlernes oprindelse og kilden til kundens formue
   - Det vil sige oplysninger om, hvorfra kundens formue, de midler, der indgår i transaktionen eller forretningsforbindelsen stammer fra.
4. Indhentelse af oplysninger om årsagerne til de ønskede transaktioner.
5. Skærpet overvågning af forretningsforbindelsen ved at øge antallet af kontroller og ved at udvælge transaktionsmønstre, der kræver nøjere undersøgelse.

   Dette betyder, at spiludbyderen skal foretage en indgående overvågning af kunden og transaktionerne for at fastslå om kundens tilsigtede beskaffenhed med forretningsforbindelsen stemmer overens med det kendskab, som spiludbyderen har til kunden.

6.5.3 Politisk eksponerede personer

Hvidvasklovens § 18

Spiludbydere skal have forretningsgange til at afgøre, om en kunde er politisk eksponeret person (PEP), nærtstående eller nær samarbejdspartner til en politisk eksponeret person. Det fremgår af hvidvasklovens § 18, stk. 1.

6.5.3.1 Hvad forstås ved en politisk eksponeret person?
Politisk eksponerede personer er personer, der bestrider et særligt offentligt tillidshverv, og som følge heraf kan være modtagelige for bestikkelse og anden korruption.

Det bemærkes, at det forhold, at en person er en PEP, ikke betyder, at personen automatisk bliver betragtet som værende en person, der er modtagelig for korruption og bestikkelse. Reglerne er således forebyggende og skal også ses i lyset af, at bestikkelse og korruption på globalt plan er et stort problem.

Nedenfor angives hvidvasklovens definition af en PEP:

- Statschef, regeringschef, minister og viceminister eller assisterende minister. Dette omfatter alle ministre samt departementschefer.
- Parlamentsmedlem eller medlem af et tilsvarende lovgivende organ. Dette omfatter både medlemmer af Folketinget og medlemmer af Europa-Parlamentet.
- Medlem af et politisk partis styrelsesorgan. Dette omfatter personer i hovedbestyrelser eller tilsvarende styrende organ i Folketingets partier, hvis organets rolle er defineret i partiers vedtægter.
- Højesteretsdommer, medlem af forfatningsdomstolen og af anden højtstående retsinstans, hvis afgørelser kun er genstand for yderligere prøvelse under ekstraordinære omstændigheder. Udover danske Højesteretsdommere omfatter dette også danske dommere ved internationale domstole.
- Medlem af revisionsret og øverste ledelsesorgan for en centralbank. Dette omfatter direktionen for Danmarks Nationalbank, danske statsrevisorer og det danske medlem af Den Europæiske Revisionsret.
- Ambassadør, chargé d'affaires og højtstående officer i de væbnede styrker. Dette omfatter de øverste chefer i de væbnede styrker, nærmere defineret som forsvarschef, viceforsvarschef, værnschefer og ambassadører for danske ambassader.
- Medlem af statsejet virksomheds administrative, ledende eller kontrollerende organ.
- Direktør, vicedirektør og medlem af bestyrelsen eller person med tilsvarende hverv i en international organisation. Definitionen omfatter også direktøren i styrelser og medlemmer af bestyrelsen i styrelser, hvor denne personkreds har en egentlig beslutningskompetence.
- Direktører, vicedirektører, bestyrelsesmedlemmer og personer med tilsvarende hverv i internationale organisationer. Dette omfatter personer, der er indstillet, udpeget eller ansat af regeringen, et ministerium eller en minister i en international organisation, som er etableret ved indgåelse af en formel international politisk aftale.

Både indenlandske og udenlandske PEP'er, nærtstående og nære samarbejdspartnere til PEP er omfattet af hvidvaskloven.

6.5.3.2 Nærtstående til en politisk eksponeret person
En nærtstående til en politisk eksponeret person defineres som værende:
- ægtefælle, registrerede partner eller samlever,
- forældre og
- børn og disses ægtefæller, registrerede partnere eller samlevere.

Begrebet omfatter dermed ikke søskende eller stedbørn og stedforældre.
Nærtstående skal identificeres, da de kan drage nytte af deres nære forbindelse til den politisk eksponerede person eller misbruges som konsekvens heraf.

Spiludbydere skal behandle nærtstående efter samme regler som PEP'er. Den konkrete risikovurdering af en PEP er derfor afgørende for, hvordan kundekendskabsprocedureren tilrettelægges for PEP¨ens nærtstående. Er PEP'en blevet vurderet til at udgøre en høj risiko, skal PEP'ens nærtstående betragtes på samme måde, medmindre den individuelle risikovurdering af den pågældende nærtstående taler herimod.

6.5.3.3 Nær samarbejdspartner til en politisk eksponeret person
En nær samarbejdspartner til en politisk eksponeret person defineres som værende en fysisk person, som:
- er reel ejer af en virksomhed eller en anden form for juridisk person i fællesskab med en eller flere PEP'er,
- på anden måde har en nær forretningsforbindelse med en eller flere PEP'er, fx som samhandelspartner over en længere periode,
- er den eneste reelle ejer af en virksomhed eller en anden form for juridisk person, der udelukkende er oprettet til fordel for en PEP.

Spiludbydere skal behandle nære samarbejdspartnere efter samme regler som PEP'er. Den konkrete risikovurdering af en PEP er derfor afgørende for, hvordan kundekendskabsprocedureren tilrettelægges for PEP'ens nære samarbejdspartner. Er PEP'en blevet vurderet til at udgøre en høj risiko, skal PEP'ens nære samarbejdspartnere betragtes på samme måde, medmindre den individuelle risikovurdering af den pågældende nære samarbejdspartner taler herimod.

6.5.3.4 Fastlæggelse af PEP-status
Spiludbydere skal have forretningsgange til at afgøre, om en kunde er en PEP. Dette gælder ved etableringen af en forretningsforbindelse, eller hvis forretningsforbindelsen ændrer omfang., men også ved udførelsen af en enkeltstående transaktion.

Der skal som anført under afsnit 6.2.1, gennemføres kundekendskabsprocedurer, når der etableres en forretningsforbindelse. Spiludbyderen skal i den forbindelse samtidig fastlægge om kunden er PEP.

Landbaserede kasinoer skal, uanset om der er tale om en forretningsforbindelse eller en enkeltstående transaktion, altid screene for PEP-status, når kunden registreres ved ankomst.

Det er op til spiludbyderen at fastlægge de nærmere rammer for, hvordan spiludbyderen identificere at en kunde er PEP.

Når en kunde identificeres som en PEP, skal spiludbydere på basis af en risikovurdering indhente oplysninger om kunden. Selvom niveauet for kundekendskab skal anses for at være en skærpende omstændighed set i forhold til "almindelige" kunder, tillades der spiludbyderen en vis fleksibilitet.

PEP'en selv vil som regel være den primære kilde til oplysningerne, men det er muligt og somme tider nødvendigt at indhente oplysninger fra andre kilder.

Spiludbyderen skal have forretningsgange, der sikrer, at identificeringen af, om en kunde er en PEP, sker, når kundeforholdet etableres eller udvides. Her skal spiludbyderen blandt andet iagttage følgende:

1. Søge afklaret, hvorvidt en kunde er en PEP, fx ved at konsultere Finanstilsynets liste over indenlandske PEP'er. For så vidt angår udenlandske PEP'er kan dette ske ved at søge på internettet eller abonnere på tjenesteudbydere, der tilbyder denne service.
2. Spiludbyderen skal træffe rimelige foranstaltninger til at identificere de kunder, der måtte være nærtstående eller nære samarbejdspartnere til en PEP, fx ved at konsultere PEP'en.
3. Spiludbyderen skal træffe rimelige foranstaltninger for at identificere, om en kunde er en udenlandsk PEP.

6.5.3.5 Rimelige foranstaltninger
Ved "rimelige foranstaltninger" forstås eksempelvis nedenstående tiltag. Det er op til spiludbyderen i det konkrete tilfælde at vurdere, hvad der er tilstrækkeligt til at opfylde kravene i hvidvaskloven.

- Spiludbyderen indhenter oplysninger hos den pågældende PEP.
- Spiludbyderen bruger den information om kunden, der allerede er tilgængelig i udbyderens systemer.
- Spiludbyderen bruger de eksterne kilder, som virksomheden har adgang til, fx internet og nyhedsmedier.
- Spiludbyderen abonnerer hos en eller flere af de tjenesteudbydere, der tilbyder information om, hvem der er PEP, nærtstående til en PEP eller nær samarbejdspartner med en PEP.
- Spiludbyderen verificerer aktivt oplysninger, som virksomheden er usikker på, fx ved at spørge de relevante kunder.

6.5.3.6 Finanstilsynets lister over politisk eksponerede personer
Finanstilsynet fører, opdaterer og offentliggør lister over aktuelle politisk eksponerede personer i Danmark, Grønland og på Færøerne. Der er et link til listerne på Spillemyndighedens hjemmeside under afsnittet om "Bekæmpelse af hvidvask".

Listerne indeholder oplysninger om navn, fødselsdato og stillingsbetegnelse. Listerne indeholder ikke oplysninger om nærtstående eller nære samarbejdspartnere til PEP'er, som derfor må identificeres på anden måde.

Listerne bygger på oplysninger, der bliver indberettet til Finanstilsynet. Reguleringen pålægger de virksomheder, styrelser og organisationer, der står i et arbejdsgiverlignende forhold til en PEP, at indberette navneoplysninger og at indberette, når der sker ændringer.

Bemærk, at listerne er et værktøj til at foretage en søgning med henblik på at identificere om en kunde er PEP, men at spiludbyderen kan være nødsaget til at indsamle oplysninger andetsteds, fx ved indenlandske PEP'er og nærtstående og nære samarbejdspartnere i øvrigt for at fastslå, at der er identitetssammenfald og ikke blot navnesammenfald.

6.5.3.7 Kommercielle udbydere af PEP-lister
Spiludbydere kan som en del af sine forretningsgange abonnere på private kommercielle udbydere af løsninger til PEP-lister og fastlæggelse af nærtstående og nære samarbejdspartnere til PEP'er.

Sådanne systemer kan hjælpe spiludbydere til at skaffe oplysningerne om PEP-status, herunder status på PEP og på en nærtstående eller nær samarbejdspartner til en PEP.

Spiludbydere skal dog samtidig vurdere om der er behov for eventuelt også at benytte andre kilder til at opnå informationen.

Der er ikke krav om anvendelse af sådanne systemer, og det er således op til spiludbyderne selv at vurdere, om det er et værktøj, som de vil købe adgang til.

Kravene til spiludbyderens processer afhænger af virksomhedens størrelse, og der stilles således større krav til store spiludbyderes processer.

6.5.3.8 Fastlæggelse af oprindelsen af PEP 'ens midler og formue
Spiludbyderen skal for PEP'ens vedkommende også træffe passende foranstaltninger til at fastslå oprindelsen af PEP 'ens midler og formue, der er omfattet af forretningsforbindelsen eller transaktionen. Det fremgår af hvidvasklovens § 18, stk. 2. Indhentelse af oplysninger for at fastslå midlernes oprindelse skal ske ud fra en risikovurdering af det kundeforhold, der er søgt etableret fra PEP'ens side.

I risikovurderingen kan fx. indgå elementer såsom, i hvilket land kunden har bopæl, kundens stilling, kundens renommé m.v. Passende foranstaltninger kan også være, at der indlægges en risikovurdering i forhold til det produkt, en kunde har valgt. Ved produkter med høj risiko og store transaktioner, må der foretages mere tilbundsgående undersøgelser end ved produkter med en begrænset risiko.

Spiludbyderen kan på baggrund af risikovurderingen fx anmode PEP'en om at indlevere de fornødne oplysninger. Det kan fx være bankudskrifter, lønsedler eller lignende. Det kan være nødvendigt at indhente oplysningerne ved kunden, hvis spiludbyderen ikke i forvejen har oplysningerne eller hvis de oplysninger, som spiludbyderen har ikke længere er aktuelle.

I de tilfælde, hvor spiludbyderen har et indgående indblik i PEP'ens økonomiske forhold, fx som følge af et flerårigt kundeforhold, vil spiludbyderen på baggrund af en risikovurdering kunne beslutte, at den viden, som spiludbyderen ligger inde med, er tilstrækkelig til at fastslå oprindelsen af midlerne og formuen, der er omfattet af forretningsforbindelsen. Spiludbyderen kan også indhente oplysninger fra eksterne kilder eller lignende fx ved søgning på internettet.

6.5.3.9 Skærpet overvågning
Der er krav om skærpet overvågning af en forretningsforbindelse med en PEP, dennes nærtstående samt nære samarbejdspartnere. Dette fremgår af hvidvasklovens § 18, stk. 4.

Omfanget af den skærpede overvågning kan baseres på en risikovurdering af PEP'en. Personer fra lande, hvor der foreligger et højt korruptionsniveau, vil potentielt kunne siges at udgøre en højere risiko for hvidvask eller terrorfinansiering, og det vil derfor være nødvendigt at have ekstra opmærksomhed på sådanne personer. Der er således mulighed for at differentiere mellem politisk eksponerede personer med bopæl i Danmark og politisk eksponerede personer med bopæl i et land med et øget korruptionsniveau. Den foretagne risikovurdering kan ikke føre til, at der ikke foretages skærpet overvågning.

Et eksempel på overtrædelse af bestemmelsen er en virksomhed, hvor en politisk eksponeret person overvåges på samme måde som resten af kundeporteføljen, som ikke i øvrigt er underlagt skærpet overvågning.

Eksempel

Skærpet overvågning af en PEP kan fx være, at tærskelværdierne for, hvornår der udløses en alarm sættes lavere eller hyppigere for den pågældende PEP eller at der foretages hyppigere opdatering af kundekendskabet.

6.5.3.10 Løbende vurdering af PEP-status

Selvom en kunde ikke er blevet identificeret som PEP ved etablering af forretningsforbindelsen, kan kundens status ændre sig i løbet af kundeforholdet. En kunde, der ikke tidligere har været PEP, kan således blive PEP.

På samme måde kan PEP'ens status ændre sig i løbet af kundeforholdet. En PEP kan under kundeforholdet således ophøre med at være PEP.
Spiludbydere skal derfor løbende sikre, om eksisterende kunder enten er blevet PEP eller er ophørt med at være PEP, nærtstående eller nære samarbejdspartnere til en PEP. Det kan fx ske ved:

- Tilstrækkeligt hyppigt at screene alle eksisterende kunder mod Finanstilsynets liste over PEP'er.
- Tilstrækkeligt hyppigt at screene eksisterende kunder mod PEP-lister udbudt af en kommerciel udbyder af PEP-lister.
- Manuelt PEP-tjek, når et kundeforhold i øvrigt gennemgås, fx hvis en kundes transaktioner giver anledning til nærmere undersøgelse.
- Søgning i eksterne kilder, fx internet og nyhedsmedier.

6.5.3.11 Ophør af PEP-status

Når en person ikke længere bestrider det hverv, der gjorde, at personen var en PEP, skal spiludbyderen i minimum 12 måneder efter ophøret af personens PEP-status vurdere, om personen udgør en øget risiko for hvidvask og terrorfinansiering. Der skal anvendes skærpede kundekendskabsprocedurer efter hvidvasklovens § 17, stk. 1, indtil personen ikke vurderes at udgøre en øget risiko.

I vurderingen skal fx indgå forhold såsom personens fortsatte relation til sit tidligere hverv, herunder relation til tidligere samarbejdspartnere og kolleger.

Hvis personen ved ophør af hvervet vurderes ikke at udgøre en øget risiko for hvidvask eller terrorfinansiering, skal spiludbyderen gennemføre kundekendskabsprocedurer i henhold til hvidvasklovens § 10, og kunden vil på ny skulle risikovurderes i henhold til hvidvasklovens § 11.

Dette gælder ikke for nærtstående eller nære samarbejdspartnere til en PEP, der som udgangspunkt skal behandles som andre kunder fra det øjeblik, hvor PEP'en ophører med at være PEP. Nærtstående og nære samarbejdspartnere skal således kun undergives skærpede kundekendskabsprocedurer efter hvidvasklovens § 17, hvis kunden, der tidligere var PEP, vurderes at udgøre en øget risiko for hvidvask eller terrorfinansiering.

6.6 Afvikling af en etableret forretningsforbindelse og utilstrækkelige oplysninger

Hvidvasklovens §14, stk. 5 og § 15

6.6.1 Pligt til at afvikle en kunde

En spiludbyder er i visse tilfælde forpligtet til at afbryde eller afvikle en etableret forretningsforbindelse. Dette er tilfældet, hvis kravene i hvidvasklovens § 11, stk. 1, nr. 1-4, og stk. 2 og 3 (kundekendskabsprocedurer), ikke kan opfyldes. Det fremgår af hvidvasklovens § 14, stk. 5.

Bestemmelsen eller loven regulerer ikke i øvrigt spiludbyderes mulighed for at afslå en kunde eller afbryde eller afvikle en etableret forretningsforbindelse. Hvorvidt der i øvrigt er mulighed for at afbryde eller afvikle en kunde, kan dog være reguleret i anden lovgivning eller i kontrakten med kunden.

Før en spiludbyder har pligt til at afbryde eller afvikle en etableret forretningsforbindelse, skal spiludbyderen undersøge, om kundekendskabsprocedurerne kan gennemføres på en anden måde i forhold til den konkrete kunde end efter den fremgangsmåde og procedure, som spiludbyderen normalt følger.

Det vil fx ikke være tilstrækkeligt til at afbryde forretningsforbindelsen, hvis kunden ikke vil udlevere en kopi af sit pas. Spiludbyderen skal i sådanne situationer vurdere, om årsagen til, at kunden nægter at udlevere oplysningerne, kan medføre en mistanke om hvidvask eller terrorfinansiering. Hvis årsagen ikke medfører en mistanke, fx fordi kunden blot ikke ønsker, at spiludbyderen skal opbevare en kopi af passet, skal spiludbyderen forsøge at indhente de ønskede oplysninger på anden måde.

Der er således kun pligt til efter hvidvaskloven at afbryde eller afvikle en forretningsforbindelse, hvis det ikke er muligt for spiludbyderen at gennemføre kundekendskabsprocedurerne, og der er mistanke om hvidvask eller terrorfinansiering.

Beslutter en spiludbyder, at en forretningsforbindelse skal afbrydes eller afvikles, må der ikke udføres yderligere transaktioner eller aktiviteter for kunden. Spiludbyderen skal samtidig undersøge, om der skal foretages en underretning til Hvidvasksekretariatet. Da der som udgangspunkt kun er pligt til at afbryde eller afvikle en forretningsforbindelse, hvis der er mistanke om hvidvask eller terrorfinansiering, vil spiludbyderen i langt de fleste tilfælde skulle foretage en underretning, hvis de afbryder eller afvikler en kunde.

6.6.2 Utilstrækkelige oplysninger

Hvis en spiludbyder bliver bekendt med, at de oplysninger, der er indhentet i forbindelse med kundekendskabsprocedurerne, er utilstrækkelige og ikke kan ajourføres, skal spiludbyderen træffe passende foranstaltninger for at imødegå risikoen for hvidvask og terrorfinansiering, herunder overveje om forretningsforbindelsen skal afvikles efter hvidvasklovens § 14, stk. 5, som anført ovenfor.

Det kan fx være tilfældet, hvor spiludbyderen i forbindelse med de løbende kundekendskabsprocedurer bliver opmærksom på, at de oplysninger, der er indhentet, er utilstrækkelige, eller hvis spiludbyderen ikke kan ajourføre oplysningerne, fx fordi kunden ikke ønsker at udlevere oplysningerne, eller det ikke er muligt at komme i kontakt med kunden.

Spiludbyderen skal i de tilfælde konkret vurdere, hvilke tiltag der skal iværksættes så risikoen for hvidvask og terrorfinansiering på anden måde kan imødegås.

'Passende foranstaltningerne' kan fx være, at kunden ikke tilbydes nye produkter, at overvågningen af kunden intensiveres, eller at der sættes beløbsgrænser på kundens transaktioner. De foranstaltninger, som spiludbyderen iværksætter, skal altid være passende i forhold til den konkrete risiko for hvidvask og terrorfinansiering i forhold til kunden. I vurderingen af, hvilke tiltag der skal iværksættes, kan spiludbyderen inddrage de oplysninger, som spiludbyderen allerede har indhentet om kunden i forbindelse med kundekendskabsprocedureren.

Bestemmelsen er relevant i de tilfælde, hvor der ikke er hjemmel til at afbryde eller afvikle en forretningsforbindelse efter § 14, stk. 5, da der således kan være behov for at imødegå risikoen for hvidvask og terrorfinansiering på anden måde.

Bistand fra tredjemand, koncerner og outsourcing

7

7.1 Bistand fra tredjemand

Hvidvasklovens § 22

En spiludbyder kan vælge at overlade det til en tredjemand at indhente og kontrollere identitetsoplysninger på kunder efter hvidvasklovens § 11, stk. 1, nr. 1-4. Det fremgår af hvidvasklovens § 22.

Det er den, der etablerer kundeforholdet – altså spiludbyderen – der er ansvarlig for, at reglerne og forpligtelserne i hvidvaskloven overholdes. De oplysninger, det kan overlades tredjemand at indhente, er begrænset til oplysninger efter hvidvasklovens § 11, stk. 1, nr. 1-4. Spiludbyderen skal derfor selv indhente oplysninger, der supplerer dem, som tredjemanden har tilvejebragt og i tillæg hertil selv gennemføre øvrige relevante skærpede foranstaltninger. En tredjemand kan dog godt bistå med oplysning om, at en kunde er en politisk eksponeret person.

7.1.1 Betingelserne for brug af bistand fra tredjemand

En spiludbyder kan gøre brug af bistand fra en tredjemand til indhentning og kontrol af identitetsoplysninger, hvis oplysningerne stilles til rådighed af én af de nedenstående:

- En virksomhed eller person, der er omfattet af hvidvasklovens § 1, stk. 1.
  Det betyder, at en spiludbyder kan vælge at indhente oplysninger om kunden hos en anden virksomhed eller person omfattet af loven, hvis tredjemanden allerede har foretaget kundekendskabsprocedurer på kunden. Det er ikke en betingelse, at der er tale om samme type virksomhed. Det vil sige, at en spiludbyder godt kan lægge oplysninger om en kundes identitet til grund, som er indhentet fra eksempelvis et pengeinstitut.

- En tredjemand, der er etableret i et EU/EØS-land eller et øvrigt land, der er underlagt krav om bekæmpelse af hvidvask og terrorfinansiering, der svarer til de krav, der følger af 4. hvidvaskdirektiv. Det er en betingelse, at den tredjemand, der afgiver oplysningerne, er underlagt krav om kundekendskab og opbevaring af oplysninger, der svarer til kravene i 4. hvidvaskdirektiv og er underlagt et tilsyn med overholdelsen af reglerne.

  En spiludbyder kan ikke benytte bistand fra en tredjemand, der er etableret i lande, som er opført på Europa-kommissionens liste over lande, hvor der vurderes at være en høj risiko for hvidvask. Hvis en spiludbyder vælger at benytte sig af oplysninger indhentet af tredjemand etableret i et land uden for EU, er det spiludbyderens ansvar at vurdere, om tredjemanden er underlagt krav om kundekendskab mv., der svarer til kravene i hvidvaskloven.

- En medlemsorganisation eller sammenslutning af virksomheder eller personer som nævnt under pkt. 1 og 2, der er underlagt krav om bekæmpelse af hvidvask og terrorfinansiering, der svarer til de krav, der følger af 4. hvidvaskdirektiv, og er underlagt tilsyn af en myndighed.

Hvis en spiludbyder benytter bistand fra en tredjemand, skal spiludbyderen indhente tilstrækkelige oplysninger om tredjemanden til at kunne lægge til grund, at tredjemanden opfylder kravene til kundekendskabsprocedurer og opbevaring af oplysninger. Det fremgår af hvidvasklovens § 22, stk. 2. Spiludbyderen kan opfylde dette krav ved at bede tredjemanden om at redegøre for, hvilke forretningsgange tredjemanden har indført og følger for at opfylde hvidvasklovens krav.

Gør en spiludbyder brug af en tredjemand til indhentning af oplysninger, skal spiludbyderen sikre sig, at tredjemand forpligter sig til efter anmodning straks at fremsende kopi af identitets- og kontroloplysninger om kunden samt anden relevant dokumentation til spiludbyderen Dette fremgår af § 22, stk. 3. Det kan være nødvendigt, at øvrige oplysninger, herunder

oplysninger om spilomfang og angivne spiltyper, pr. automatik tilgår spiludbyderen, så oplysningerne kan indgå i spiludbyderens risikovurdering eller overvågning af kunden.

Det vil også være relevant at indhente oplysninger om, hvorvidt tredjemand har modtaget påbud fra tilsynsmyndigheder i relation til legitimation og identifikation af kunder, og om disse i givet fald er opfyldt.

7.2 Koncerner

Hvidvasklovens § 23

Spiludbydere, der er en del af en koncern, kan overlade det til en anden enhed af koncernen at opfylde kravene om kundekendskabsprocedurer i hvidvasklovens § 11, stk. 1, nr. 1-4. Det fremgår af hvidvasklovens § 23.

Koncernforbundne spilvirksomheder har dermed mulighed for at få bistand fra hinanden i relation til indhentelse af identitetsoplysninger og kontrollen heraf, og en virksomhed kan således lægge oplysninger om kundens identitet mv. til grund, når de er indhentet af en koncernforbunden virksomhed. Det er dog et krav for at kunne benytte denne mulighed, at koncernen anvender kundekendskabsprocedurer, regler om opbevaring af oplysninger og programmer til bekæmpelse af hvidvask og terrorfinansiering i overensstemmelse med de krav, der følger af 4. hvidvaskdirektiv. I tillæg hertil er det et krav, at der på koncernniveau føres tilsyn af en myndighed med overholdelse af kravene.

Med programmer til bekæmpelse af hvidvask og terrorfinansiering menes koncernens politikker og forretningsgange på hvidvaskområdet.

Behandling af personoplysninger i forbindelse med anvendelse af tredjemænd skal ske i overensstemmelse med reglerne i databeskyttelseslovgivningen.

7.3 Outsourcing

Hvidvasklovens § 24

7.3.1 Hvilke opgaver kan outsources?

En spiludbyder kan efter hvidvasklovens § 24 vælge at outsource opgaver til en anden virksomhed (i det følgende kaldet leverandøren) med henblik på at overholde kravene i hvidvaskloven. Som udgangspunkt kan alle forpligtelser, der følger af hvidvaskloven, outsources til en leverandør. Det kan fx være opgaver som:

- Indhentelse af identitets- og kontroloplysninger til brug for spiludbyderens kundekendskabsprocedurer
- Opbevaring af oplysninger
- Underretninger.

I forhold til de databeskyttelsesretlige krav bemærkes det, at der skal indgås en databehandleraftale mellem spiludbyderen og leverandøren. Der henvises i den anledning til Datatilsynets vejledninger, som er tilgængelige på www.datatilsynet.dk.

7.3.2 Betingelser for outsourcing

Der er visse krav, som skal være opfyldt, før en spiludbyder kan indgå en kontrakt om outsourcing. Det følger af hvidvasklovens § 24, stk. 1.

Før der kan ske outsourcing af en opgave, skal spiludbyderen sikre, at leverandøren har:

- den fornødne evne og kapacitet til at håndtere opgaven på tilfredsstillende måde, og
- den eller de nødvendige tilladelser.

7.3.2.1 Den fornødne evne og kapacitet
At leverandøren skal have den fornødne evne, betyder, at leverandøren skal have et relevant og fagligt kendskab til hvidvaskloven og de opgaver, som leverandøren skal udføre for spiludbyderen i henhold til hvidvaskloven.

Det betyder fx, at leverandøren skal have viden om, hvordan, hvornår og hvorfor der skal gennemføres kundekendskabsprocedurer, så hvidvasklovens regler overholdes. Spiludbyderen skal således sikre sig, at leverandøren har tilstrækkelig viden om og værktøjer til at kunne gennemføre kundekendskabsprocedurer, før opgaven outsources.

At leverandøren skal have den fornødne kapacitet, betyder, at leverandøren skal have tilstrækkelige ressourcer til at varetage de opgaver, der outsources.

7.3.2.2 De fornødne tilladelser
Det er endvidere en betingelse, at leverandøren lovligt kan opfylde indholdet i den outsourcede forpligtelse. Dette krav indebærer, at leverandøren skal have de fornødne tilladelser på tværs af relevant lovgivning for at kunne opfylde forpligtelsen og dermed påtage sig opgaven. Dette kan fx være en bestyrergodkendelse ved udbud af landbaserede væddemål.

7.3.3 Hvem kan der outsources til?

Der stilles ingen krav i hvidvaskloven til, hvem der kan outsources til, og det er ikke en betingelse, at leverandøren selv er omfattet af hvidvaskloven.

Det er dog vigtigt, at spiludbyderen sikrer sig, at betingelserne for outsourcing er opfyldt, inden spiludbyderen indgår en aftale om outsourcing. Der skal foreligge en kontrakt mellem spiludbyderen og leverandøren om de opgaver samt forpligtelser, som leverandøren påtager sig. I kontrakten skal der være opstillet de krav, som leverandøren skal leve op til.

7.3.4 Kontrol

Spiludbyderen skal løbende føre kontrol med leverandøren for at sikre, at leverandøren lever op til de forpligtelser, der følger af aftalen parterne imellem, og at aftalen om outsourcing fortsat er forsvarlig. Det fremgår af hvidvasklovens § 24, stk. 2.

Bestemmelsen stiller således et krav om, at spiludbyderen løbende kontrollerer, at leverandøren opfylder de forpligtelser, der følger af aftalen, og i forlængelse heraf vurderer, om den indgåede aftale fortsat er forsvarlig – altså om leverandøren har den fornødne evne og kapacitet til at varetage opgaven, og at der foreligger de påkrævede tilladelser.

Forsvarligheden skal vurderes ud fra de krav, som påhviler spiludbyderen i henhold til hvidvaskloven. For at opfylde kravet om kontrol er det væsentligt, at spiludbyderen inden aftaleindgåelsen sikrer sig, at spiludbyderen kan få adgang til at gennemføre den relevante kontrol. Hvor ofte der skal føres kontrol og omfanget af kontrollen, skal vurderes på baggrund af en risikovurdering, outsourcingaftalens kompleksitet samt resultatet af eventuelle tidligere gennemførte kontroller mv. Dette kan fx være, hvis en leverandør tidligere ikke har overholdt krav i outsourcingaftalen.

Spiludbyderen skal dermed stille de samme krav til leverandøren, som hvidvaskloven stiller til spiludbyderen. Det vil sige, at leverandøren skal opfylde reglerne om fx

kundekendskabsprocedurer på samme måde, som hvis det var spiludbyderen selv, der stod for at foretage kundekendskabsprocedurer.

Det er således et krav, at der ved indgåelsen af en outsourcingaftale ikke sker en forringelse af opfyldelsen af lovgivningens krav ved at outsource til en leverandør.

7.3.5 Ansvaret

Som anført kan alle forpligtelser, der følger af hvidvaskloven, outsources – dog ikke ansvaret. Ansvaret påhviler altid spiludbyderen og medfører, at spiludbyderen altid bærer det fulde ansvar for de forpligtelser, som spiludbyderen har i henhold til hvidvaskloven og anden EU-retlig eller databeskyttelsesretlig lovgivning. Det betyder, at ansvaret for, at outsourcede opgaver varetages i overensstemmelse med hvidvaskloven, påhviler spiludbyderen. Spiludbyderen er derfor også ansvarlig for, at leverandøren følger spiludbyderens eventuelle forretningsgange til bekæmpelse af hvidvask og terrorfinansiering, der er relevante for den opgave, der er outsourcet. Det følger af hvidvasklovens § 24, stk. 4.

7.3.6 Særligt om eksterne forhandlere af landbaserede væddemål

Når en spiludbyder udbyder landbaseret væddemål gennem en ekstern forhandler, og i den anledning har outsourcet hvidvaskforpligtelser, fx kundekendskabsprocedurer, vil forhandleren anses som leverandør, og der skal på denne baggrund indgås en kontrakt om outsourcing. Der skal endvidere oprettes en databehandleraftale med den pågældende forhandler. Dette skal gøres for at sikre, at forhandleren kender kravene i hvidvaskloven og databeskyttelseslovgivningen.

Det er forhandleren, der møder kunden på spilstedet, og som derfor kan reagere i de tilfælde, hvor der fx er mistanke om hvidvask på baggrund af kundens aktivitet og adfærd.

For at forhandleren kan udføre kundekendskabsprocedurer i overensstemmelse med lovgivningen, skal spiludbyderen sikre sig, at forhandleren og forhandlerens ansatte har den fornødne evne og kapacitet til at kunne varetage opgaven på tilfredsstillende vis, og dermed ved, hvordan opgaven skal løses.

Spiludbyderen kan løfte sit ansvar via de forretningsgange, som spiludbyderen skal udarbejde til sit forhandlernetværk efter hvidvasklovens § 8, stk. 1. Dette kan eksempelvis være forretningsgange for, hvad der kan være mistænkelig aktivitet eller adfærd. Forretningsgangene skal gøre det muligt for forhandleren at konstatere, hvordan denne skal kontrollere og bedømme, om en kunde udviser mistænkelig adfærd.

Spiludbyderen kan endvidere løfte sit ansvar ved fx at undervise sine forhandlere og forhandlerens ansatte i opgaven og reglerne. Dette kan fx fremgå af outsourcingaftalen.

Spiludbyderen skal løbende føre kontrol med, at forhandleren udfører den outsourcede opgave i overensstemmelse med kravene i loven, og på den baggrund vurdere, om forhandleren fortsat kan løfte spiludbyderens forpligtelser i hvidvaskloven. Hvis spiludbyderen i forbindelse med kontrollen konstaterer, at forhandleren ikke løfter den outsourcede opgave, skal spiludbyderen vurdere, om det fortsat er forsvarligt, at forhandleren skal sælge spiludbyderens produkter.

Kravene til omfanget af kontrollen afhænger også af, hvordan spiludbyderen i sin risikovurdering efter hvidvasklovens § 7, stk. 1, har identificeret og vurderet den iboende risiko, der er forbundet med, at spiludbyderen har valgt at sælge sine produkter via eksterne forhandlere. Som anført under afsnit 7.3.5 er det spiludbyderen, der er ansvarssubjekt og dermed er ansvarlig, hvis forhandleren ikke lever op til lovgivningens krav.

Se også afsnit 3.2.3 om risikofaktorer for landbaserede væddemål og afsnit 5.2.1 om undervisning.

Undersøgelses- og noteringspligt

8

8.1 Undersøgelsespligt

Hvidvasklovens § 25, stk. 1 og 2

Spiludbydere omfattet af hvidvaskloven skal i medfør af hvidvasklovens § 25, stk. 1, undersøge baggrunden for og formålet med alle transaktioner, der

1. er komplekse,
   - involverer transaktionen flere parter eller flere jurisdiktioner eller
   - giver transaktionen kunden mulighed for at modtage betalinger fra en ukendt tredjemand.
2. er usædvanlig store,
   - ud fra kendskabet til den konkrete kunde og den pågældendes transaktionsmønstre og produkt-portefølje.
3. foretages i et usædvanligt mønster eller
   - ud fra kundens eller kundetypens sædvanlige adfærdsmønstre.
4. ikke har et åbenbart økonomisk eller lovligt formål.

Hvis blot én af ovenstående betingelser er opfyldt, skal spiludbyderen iværksætte en undersøgelse af baggrunden for og formålet med transaktionen. Spiludbyderen skal, hvor det er relevant, udvide overvågningen af kunden med det formål at afgøre, om transaktionerne eller aktiviteterne forekommer mistænkelige Dette fremgår af hvidvasklovens § 25, stk. 2. Se nærmere herom i afsnit 8.1.2.

Spiludbyderen skal have forretningsgange, der gør det muligt at identificere de ovenstående transaktioner. I praksis betyder det, at det er spiludbyderen, som skal definere, hvad der forstås ved "komplekse transaktioner", "usædvanligt store transaktioner" samt "usædvanlige transaktionsmønstre" og aktiviteter, der "ikke har et åbenbart økonomisk eller lovligt formål" i deres kontekst. Det er således ikke tilstrækkeligt blot at konstatere, at man undersøger usædvanlige transaktioner. Spiludbyderens viden om en kundes adfærd kan også være med til at styrke en mistanke, hvis der foregår nogle usædvanlige aktiviteter i relation til kundens spilkonto. Det kan fx være, at en kunde går fra kun at spille på spilleautomater til lige pludselig at spille væddemål. Der er her tale om en ændring i kundens adfærd, og det bør undersøges af spiludbyderen, hvad der har fremkaldt denne ændring. En usædvanlig aktivitet kan også forekomme, hvis kunden beder om, at gevinster fremover skal indsættes på en anden bankkonto end hidtil.

Hvis det på baggrund af kundens adfærd står klart, at der er tale om hvidvask eller terrorfinansiering, kan der ske underretning til Hvidvasksekretariatet uden, at spiludbyderen iværksætter en egentlig undersøgelse. Formålet med undersøgelsen er at be- eller afkræfte en formodning eller en mistanke om, at en transaktion eller aktivitet har eller har haft tilknytning til hvidvask eller terrorfinansiering. Undersøgelsen kan derfor kun undlades, hvis det står spiludbyderen klart allerede inden undersøgelsen, at der er tale om hvidvask eller terrorfinansiering.

8.1.1 Hvad består undersøgelsen i?

Udgangspunktet i en undersøgelse af en kunde vil være at sammenholde de oplysninger, spiludbyderen allerede har om kunden, herunder oplysninger om formål og tilsigtet beskaffenhed, med det, der ser mistænkeligt ud. Spiludbyderen skal ikke bevise, at der er foregået hvidvask eller terrorfinansiering, men har alene en pligt til at undersøge et mistænkeligt forhold for dernæst at reagere ved at underrette til Hvidvasksekretariatet, hvis en mistanke ikke kan afkræftes.

Spiludbyderen kan derudover fx foretage opslag i diverse søgemaskiner og opslagsværker for at se, om mistanken kan afkræftes. Det kan fx være på de sociale medier, boligsider, Statstidende, virk.dk og lignende.

Spiludbyderen kan også kontakte kunden for at indhente oplysning om formålet med transaktionen/aktiviteten. Kundens forklaring vil i mange tilfælde ikke være nok til at afkræfte en mistanke. Det kan derfor være relevant at bede kunden om dokumentation for sin forklaring. Dette kan være ved at bede kunden dokumentere oplysningerne herunder midlernes oprindelse, ved fx at fremvise/indsende kopi af lønsedler fra et ansættelsesforhold.

I nogle tilfælde vil spiludbyderen ud fra sit kendskab til kunden selv kunne afkræfte en mistanke. Det kan fx være, hvis den ansatte på et landbaseret kasino konstaterer, at det er en kendt pokerspiller, der foretager en usædvanlig stor transaktion. Kasinoet ved dog, at pokerspilleren lige har vundet en stor pokerturnering, hvorfor den usædvanligt store transaktion kan forklares i kraft af gevinsten fra pokerturneringen.

Hvis mistanken kan afkræftes, er der ikke pligt til at foretage en underretning. Men det er ikke tilstrækkeligt, at mistanken blot er svækket.

Kravene til at afkræfte en mistanke indebærer ikke, at spiludbyderen skal sætte en omfattende undersøgelse i gang eller foretage en efterforskning. Det indebærer heller ikke, at spiludbyderen altid skal indhente dokumentation fra en kunde, når der er opstået en mistanke om hvidvask. Det betyder blot, at spiludbyderen skal underrette Hvidvasksekretariatet, når spiludbyderen ikke mener at kunne komme længere med en undersøgelse inden for rimelige grænser.

Hvis spiludbyderen vurderer, at en forespørgsel til kunden vil give kunden et fingerpeg om, at spiludbyderen har en mistanke og derfor er i gang med at foretage en undersøgelse, eller hvis spiludbyderen finder det uhensigtsmæssigt at kontakte kunden om sagen, skal spiludbyderen foretage en underretning til Hvidvasksekretariatet, hvis mistanken ikke kan afkræftes på anden måde. Se afsnit 13 om spiludbyderes tavshedspligt.

Kan mistanken ikke afkræftes ved undersøgelse, er spiludbyderen forpligtet til omgående at underrette Hvidvasksekretariatet.

Midlernes oprindelse

Midlernes oprindelse dækker over oplysninger om

- hvorfra kundens formue oprinder
- hvorfra de midler, der indgår i transaktionen, oprinder, eller
- hvor midlerne, der er en del af forretningsforbindelsen, kommer fra.

Det er således relevant at undersøge, hvilke værdier eller hvilken formue kunden har, og hvordan kunden tjener sine penge. I forbindelse med en transaktion kan det være nødvendigt at undersøge alle tre forhold for at undersøge, om en transaktion er sædvanlig eller usædvanlig for den pågældende kunde og dermed muligheden for en spiludbyder at kunne be- eller afkræfte en mistanke om hvidvask.

8.1.2 Udvidet overvågning

Spiludbydere skal, hvor det er relevant, udvide overvågningen af kunden med det formål at afgøre, om transaktionerne eller aktiviteterne forekommer mistænkelige, jf. hvidvasklovens § 25, stk. 2.

Der påhviler således spiludbyderen et ansvar at vurdere, om der ud fra en risikovurdering skal iværksættes udvidet overvågning af en kunde, fx hvis der er sket underretning til Hvidvasksekretariatet.

En udvidet overvågning kan blandt andet bestå i, at spiludbyderen fastsætter en lavere tærskelværdi for, hvornår en alarm skal lyde i overvågningen af kunden. Det vil også være relevant at notere på kundens profil, at denne har ændret adfærd, og at dette derfor har udløst en udvidet overvågning, så de ansatte bliver opmærksomme på kunden. Herudover kan spiludbyderen vælge at kontrollere kundens transaktioner oftere for at se, om der sker ændringer i adfærden, transaktionerne eller aktiviteterne.

8.2 Noteringspligt

Hvidvasklovens § 25, stk. 3

Resultaterne af de undersøgelser, en spiludbyder har foretaget efter hvidvasklovens § 25, stk. 1, skal noteres. Dette følger af hvidvasklovens § 25, stk. 3.

Pligten til at notere oplysninger omfatter faktuelle oplysninger om kunden og transaktionen eller aktiviteten samt en konklusion af, hvad undersøgelsen er udmundet i. Notatet skal være tilstrækkeligt til at genopfriske hukommelsen og give andre en forståelse af sagen og dennes omfang. Udgangspunktet vil ofte være kundens egen forklaring om formålet med transaktionen eller aktiviteten, dokumentation af kundens forklaring, eventuelt sammenholdt med forklaringer indhentet fra andre medarbejdere, som har kontakt med eller opgaver i relation til kunden.

Noteringspligten omfatter både:
1. undersøgelser, som fører til, at Hvidvasksekretariatet underrettes
2. undersøgelser, som resulterer i, at mistanken afkræftes, hvorved der ikke sker underretning til Hvidvasksekretariatet.

Noteringspligten omfatter ikke de tilfælde, hvor et maskinelt overvågningssystem genererer såkaldte false positives, det vil sige »hits«, hvor det med rimelighed kan lægges til grund, at disse ikke giver indikationer om konkret mistænkelige enkeltsager.

8.2.1 Begrænsning i retten til indsigt

Den registrerede person har ikke ret til indsigt i personoplysninger, der er eller vil blive behandlet i forbindelse med en undersøgelse ved mistanke om hvidvask og terrorfinansiering. Det betyder, at kunden ikke kan få viden om igangværende eller allerede foretagne undersøgelser. Dette følger af hvidvasklovens § 25, stk. 4.

Underretningspligt

9

9.1 Pligt til at underrette

Hvidvasklovens § 26

En spiludbyder er forpligtet til omgående at underrette Hvidvasksekretariatet, hvis spiludbyderen får viden om, har mistanke om eller en rimelig grund til at formode, at en transaktion, midler eller en aktivitet har eller har haft tilknytning til hvidvask eller terrorfinansiering. Dette fremgår af hvidvasklovens § 26, stk. 1.

Underretningen skal ske omgående. Det betyder, at spiludbyderen skal underrette Hvidvasksekretariatet, så snart de interne processer er afsluttede. Ved interne processer forstås stadiet fra overvågning af kundetransaktioner og konstatering af noget mistænkeligt til undersøgelse og afklaring af, om mistanken kan anses for afkræftet eller ej. Det er en forudsætning, at spiludbyderen prioriterer behandlingen og undersøgelsen af den mistænkelige transaktion eller aktivitet, så undersøgelsen ikke forhales. Da der skal underrettes omgående, er det vigtigt, at spiludbyderen er oprettet i det system (GoAML), hvor underretningerne skal sendes.

Pligten til at underrette gælder også i de tilfælde, hvor en mulig kunde fx bliver afvist ved oprettelse af en spilkonto, fordi der er mistanke om hvidvask eller terrorfinansiering, ligesom et forsøg på en transaktion, som ikke bliver gennemført, også fordrer pligt til at underrette, hvis spiludbyderen vurderer, at det giver anledning til mistanke.

Det bemærkes, at en underretning ikke er det samme som en politianmeldelse.

Spillemyndigheden er som tilsynsmyndighed også forpligtet til at underrette om forhold, der kan have tilknytning til hvidvask eller finansiering af terrorisme. Dette følger af hvidvasklovens § 28.

9.2 Typer af underretninger

Der kan foretages tre typer af underretninger til Hvidvasksekretariatet:

- **STR** (suspicious transaction report): Underretning om mulig hvidvask med transaktioner mellem selskaber eller personer, kontanthævninger eller kontantindsættelse.
- **SAR** (suspicious activity report): Underretning om mistænkelig aktivitet eller adfærd.
- **TFR** (terror financing report): Underretning om mulig terrorfinansiering.

9.3 Hvordan skal underretningen ske?

Der er udstedt en bekendtgørelse om formkrav til indsendelse af underretninger mv. til Hvidvasksekretariatet.

> Bekendtgørelse nr. 657 af 26. maj 2023 om indsendelse af underretninger m.v. til Hvidvasksekretariatet

Det fremgår blandt andet heraf, at underretning skal ske digitalt via www.hvidvask.dk, og at underretningen skal indeholde en række oplysninger.

Spiludbyderen skal kontrollere, om underretningen er accepteret eller afvist inden udløbet af den efterfølgende bankdag.

For nærmere information om underretninger og kravene til indhold henvises til Hvidvasksekretariatets hjemmeside www.hvidvask.dk.

9.4 Begrænsning i retten til indsigt

En registreret person har ikke ret til indsigt i personoplysninger, der vedrører den pågældende selv, og som er eller vil blive behandlet i forbindelse med en underretning. En registreret person har heller ikke ret til indsigt i overvejelserne omkring at foretage en underretning. Dette følger af hvidvasklovens § 26, stk. 7.

9.5 Berostillelse af transaktioner

9.5.1 Mistanke om hvidvask

Ved underretninger om mistanke om hvidvask skal spiludbyderen undlade at gennemføre en transaktion, indtil der er sket underretning til Hvidvasksekretariatet, hvis transaktionen ikke allerede er gennemført. Det fremgår af hvidvasklovens § 26, stk. 3.

Det kan fx være i situationer, hvor kunden anmoder om udbetaling fra en spilkonto, og hvor spiludbyderen har en mistanke om at transaktionen har tilknytning til hvidvask.

I visse situationer kan det dog være nødvendigt at lade en transaktion gennemføre inden underretning til Hvidvasksekretariatet. Det kan fx være, hvis en undladelse af at gennemføre en transaktion vil kunne skade en efterforskning, eller hvis der er risiko for, at en udskydelse eller forsinkelse af en transaktion eller aktivitet vil vække en mistanke hos den, der forsøger at hvidvaske penge. Der skal herefter omgående ske underretning til Hvidvasksekretariatet.

I nogle tilfælde, fx ved 'straksoverførsler', er transaktionen gennemført, inden spiludbyderen bliver vidende om eller får mistanke om, at transaktionen kan have tilknytning til hvidvask. Det kan fx være ved indbetaling til en spilkonto, hvor overførslen sker med det samme. Spiludbyderen skal i det tilfælde udvide overvågningen af kunden, hvis der efterfølgende foretages undersøgelse af en transaktion.

9.5.2 Transaktioner af større eller særlig mistænkelig karakter

Virksomheder og personer skal undlade at gennemføre transaktioner, indtil der er sket underretning efter hvidvasklovens § 26, stk. 1, og de har indhentet godkendelse fra Hvidvasksekretariatet, hvis de har viden om, mistanke om eller rimelig grund til at formode, at transaktionen vedrører hvidvask og er af større eller særlig mistænkelig karakter. Det fremgår af hvidvasklovens § 26, stk. 4. Dette betegnes også som fast track-ordningen.

I bekendtgørelse nr. 431 af 11. april 2023 om transaktioner omfattet af fast track-ordning for hvidvaskunderretninger fremgår det, at der ved transaktioner af større eller særlig mistænkelig karakter skal forstås transaktioner, der vedrører indestående pengebeløb på 1 mio. kr. eller derover.

Det betyder, at der kun skal ske tilbageholdelse af midlerne, og dermed undladelse af at gennemføre transaktionen, hvis der foreligger mistanke om hvidvask **og** hvis transaktionen vedrører et beløb på 1 mio. kr. eller derover.

Hvidvasksekretariatet beslutter hurtigst muligt og senest inden udløbet af den efterfølgende bankdag, om transaktionen kan gennemføres, eller om der skal ske beslaglæggelse.

9.5.3 Mistanke om finansiering af terrorisme

Ved underretninger om mistanke om terrorfinansiering skal spiludbyderen undlade at gennemføre en transaktion, indtil der er sket underretning til Hvidvasksekretariatet, og Hvidvasksekretariatet har godkendt, at transaktionen kan gennemføres. Det fremgår af hvidvasklovens § 26, stk. 6.

Hvidvasksekretariatet beslutter hurtigst muligt og senest inden udløbet af den efterfølgende bankdag, om transaktionen kan gennemføres, eller om der skal ske beslaglæggelse.

Opbevaringspligt

10

10.1 Hvilke oplysninger skal opbevares?

Hvidvasklovens § 30

Spiludbydere skal i medfør af hvidvasklovens § 30, stk. 1, opbevare følgende oplysninger:

- Oplysninger indhentet i forbindelse med opfyldelse af kravene i kapitel 3 om kundekendskabsprocedurer.
- Dokumentation for registreringer af transaktioner, der gennemføres som led i en forretningsforbindelse eller en enkeltstående transaktion.
- Dokumenter og registreringer vedrørende undersøgelser gennemført i henhold til hvidvasklovens § 25, stk. 1 og 3.

10.1.1 Oplysninger indhentet i forbindelse med kundekendskabsprocedurer

Spiludbyderen skal opbevare oplysninger indhentet i forbindelse med kundekendskabsprocedurer.

De identitetsoplysninger, som spiludbyderen indhenter, er eksempelvis navn og cpr-nummer.

Ved kontroloplysninger forstås de oplysninger, som spiludbyderen har indhentet til brug for en kontrol af, om de indhentede identitetsoplysninger er korrekte. Hvis der i den forbindelse har været brugt et elektronisk id fra en dansk national identifikationsordning eller elektroniske databaser, skal spiludbyderen opbevare et revisionsspor, som kan dokumentere, at der er sket den pågældende kontrol.

Det er desuden et krav, at kopi af foreviste legitimationsdokumenter opbevares. Det kan fx være kopi af pas eller kørekort. Det forekommer derudover, at der ved oprettelse af en spilkonto hos en onlineudbyder kræves indsendelse af kopi af kreditkort, og et sådant legitimationsdokument vil også være omfattet af opbevaringspligten.

Oplysninger om spilprofil, gennemsnitsindskud på spilkonti, aktivitetsniveau, midlernes oprindelse, samt oplysninger indhentet med henblik på at kunne risikovurdere kunden, er også oplysninger, som skal opbevares.

10.1.2 Dokumentation for og registreringer af transaktioner

Spiludbyderen skal opbevare dokumentation og registreringer af transaktioner, der gennemføres som led i en forretningsforbindelse eller en enkeltstående transaktion. Det er alene oplysninger, som har relevans for en specifik transaktion, der er pligt til at opbevare. For onlinespil gælder det eksempelvis, at dokumentation for transaktioner foretaget som led i kundens indsats på væddemål skal opbevares.

10.1.3 Dokumenter og registreringer vedrørende undersøgelser i henhold til hvidvasklovens § 25, stk. 1 og 3

Oplysninger, dokumenter og registreringer, som er indhentet som led i opfyldelsen af undersøgelsespligten, skal opbevares. Dette gælder også noteringer, der er foretaget vedrørende resultatet af undersøgelser foretaget efter § 25.

Det kan fx være, at man i forbindelse med en undersøgelse har indhentet informationer og dokumentation for, hvor kundens midler stammer fra, og sådanne informationer skal opbevares.

10.2 Hvor lang tid skal oplysningerne opbevares?

Oplysninger, dokumenter og registreringer skal opbevares i mindst 5 år efter forretningsforbindelsens ophør eller den enkeltstående transaktions gennemførelse.

Hvad angår forretningsforbindelser, bemærkes det, at i det tilfælde, hvor en spilkonto er blevet lukket, men hvor den samme kunde inden for 5 år efter oprettes på ny som kunde, "vågner" det tidligere kundeforhold igen, hvorfor de tidligere indhentede oplysninger ikke skal slettes efter 5 år fra første kundeforholds ophør.

Det bemærkes, at personoplysninger skal slettes 5 år efter forretningsforbindelsens ophør eller den enkelte transaktions gennemførelse, medmindre andet er fastsat i anden lovgivning.

10.3 Videregivelse af oplysninger

Oplysninger, dokumenter og registreringer skal videregives, når Hvidvasksekretariatet eller andre kompetente nationale myndigheder henvender sig til en spiludbyder for at få oplyst, om de har eller i de sidste 5 år forud for forespørgslen har haft forretningsforbindelser med nærmere angivne personer, og hvori disse forbindelser består eller har bestået. Videregivelsen skal ske gennem en sikker kanal, der sikrer fuld fortrolighed om undersøgelserne. Det bemærkes, at reglerne i retsplejeloven finder sideløbende anvendelse.

Whistleblowerordning, ansatte og rapporte-ringspligt

11

11.1 Whistleblowerordning

Hvidvasklovens § 35

Spiludbydere skal etablere en whistleblowerordning, hvor deres ansatte via en særlig, uafhængig og selvstændig kanal kan indberette overtrædelser eller potentielle overtrædelser af hvidvasklovgivningen begået af virksomheden, herunder af ansatte eller medlemmer af bestyrelsen i virksomheden. Alle indberetninger skal kunne foretages anonymt. Det fremgår af hvidvasklovens § 35

Kravet om en whistleblowerordning gælder for alle virksomheder, der beskæftiger flere end fem ansatte. Ordningen skal være etableret senest tre måneder efter, at virksomheden har ansat den sjette medarbejder. Alle ansatte, der har en ansættelseskontrakt med spiludbyderen, skal tælles med i opgørelsen af antal ansatte hos udbyderen.

Hvis spiludbyderen allerede har en whistleblowerordning som følge af anden lovgivning, kan denne ordning også omfatte indberetninger efter hvidvaskloven. Det skal dog være muligt for den ansatte at foretage indberetningen anonymt, uanset om dette kræves af den lovgivning, som den eksisterende ordning er etableret som følge af.

En whistleblowerordning kan også outsources til en ekstern leverandør eller etableres via kollektiv overenskomst, fx ved etablering i et fagforbund, hvortil ansatte hos spiludbyderen kan foretage indberetninger.

Spillemyndigheden har som tilsynsmyndighed ligeledes en whistleblowerordning, hvortil ansatte hos spiludbydere kan foretage indberetninger om overtrædelser eller potentielle overtrædelser af hvidvaskloven. Den er tilgængelig på Spillemyndighedens hjemmeside under fanebladet "Kontakt". Ordningen tilbyder mulighed for tovejskommunikation, ligesom der kan foretages telefonisk henvendelse eller aftales et fysisk møde. Det bemærkes, at Spillemyndighedens whistleblowerordning ikke erstatter spiludbyderens pligt til at etablere en whistleblowerordning. Den fungerer således kun som et supplement. For nærmere information om Spillemyndighedens tavshedspligt i forbindelse med modtagelse af indberetninger, se vejledning om Spillemyndighedens hvidvasktilsyn.

11.1.1 Uafhængig og selvstændig

At ordningen skal være uafhængig og selvstændig, betyder, at den skal være uafhængig af den daglige ledelse, og at indberetningerne skal kunne foretages udenom normale procedurer.

11.1.2 Anonymitet

Det kan være svært for en ansat at beslutte sig for at indberette en overtrædelse til spiludbyderen, hvis dette ikke kan ske anonymt. Det er derfor et krav, at der kan garanteres fuldstændig anonymitet, så det ikke er muligt at spore afsenderen. Indberetningerne bør desuden kun være tilgængelige for den afdeling eller medarbejder, der behandler dem.

Eksempel

Anvendes der it-baserede løsninger, som fx en online kontaktformular skal indberetningen således kunne sendes uden angivelse af kontaktoplysninger og uden mulighed for sporing af computerens IP-adresse eller lignende.

11.1.3 Spiludbydere med færre end fem ansatte

Hvis spiludbyderen har færre end fem ansatte, er der ikke krav om en whistleblowerordning.

For medarbejdere hos spiludbydere med under fem ansatte er det muligt at foretage indberetninger til Spillemyndighedens whistleblowerordning.

Spillemyndigheden kan dispensere fra kravet om oprettelse af en whistleblowerordning, hvis det vurderes, at det vil være formålsløst, at der oprettes en whistleblowerordning. Dette kan fx være tilfældet, hvis virksomheden kun i en begrænset periode beskæftiger flere end fem ansatte, eller hvis virksomheden er under afvikling.

11.1.4 Dokumentation

En spiludbyder skal følge op på indberetninger til ordningen og skriftligt kunne dokumentere, hvordan der bliver fulgt op på indberetninger.

Spillemyndigheden vil som tilsynsmyndighed kunne anmode om at se den skriftlige dokumentation, der er opbevaret. Som minimum skal oplysningerne indeholde, hvad indberetningen går ud på, dokumentation for, hvordan indberetningen er blevet behandlet, og hvilke beslutninger der er blevet truffet som følge af behandlingen af indberetningen.

Spiludbyderen bør desuden opbevare relevant mailkorrespondance, interne undersøgelsesrapporter samt andet relevant materiale, der er med til at dokumentere, at spiludbyderen på betryggende vis har fulgt op på de modtagne indberetninger. Dokumentationen bør som minimum opbevares i 5 år.

11.1.5 Særligt for forhandlere af landbaserede væddemål

En spiludbyder, der udbyder landbaseret væddemål, bør gøre udbyderens whistleblowerordning tilgængelig for forhandlere og deres ansatte, så de kan foretage indberetninger om overtrædelser eller potentielle overtrædelser via den pågældende spiludbyders whistleblowerordning. Det vil ligeledes som et supplement være muligt for forhandlere og deres ansatte at foretage indberetninger til Spillemyndighedens whistleblowerordning.

11.2 Ansatte

Hvidvasklovens § 36

En ansat eller tidligere ansat, der har foretaget en indberetning til spiludbyderens eller Spillemyndighedens whistleblowerordning, må ikke blive udsat for ufordelagtig behandling eller ufordelagtige følger som følge af indberetningen. Det samme er tilfældet, hvis en ansat eller tidligere ansat foretager en intern underretning på baggrund af en mistanke eller en underretning til Hvidvasksekretariatet om mistanke om hvidvask eller finansiering af terrorisme. Det samme gælder ved fastsættelse, tildeling og udbetaling af variabel løn til ansatte eller tidligere ansatte. Det fremgår af hvidvasklovens § 36.

Det bemærkes, at Spillemyndigheden ikke fører tilsyn med spiludbyderes overholdelse af hvidvasklovens § 36.

11.2.1 Godtgørelse

Hvis den ansatte eller tidligere ansatte oplever at blive udsat for ufordelagtig behandling eller ufordelagtige følger efter at have foretaget en indberetning, kan den ansatte eller den tidligere

ansatte gøre krav på en godtgørelse gældende over for spiludbyderen ved de almindelige domstole.

11.3 Rapporteringspligt

Hvidvasklovens § 36 a

Den daglige ledelse hos spiludbyderen skal uden unødigt ophold rapportere til virksomhedens øverste ledelsesorgan om advarsler om hvidvask eller terrorfinansiering modtaget fra ansatte eller andre, fx udenlandske myndigheder eller whistleblowere. Tilsvarende gælder for nøglepersoner, der uden unødigt ophold skal rapportere til den daglige ledelse eller virksomhedens øverste ledelsesorgan. Det fremgår af hvidvasklovens § 36 a.

Ved krav om rapportering forstås, at virksomhedens øverste ledelsesorgan skal gøres bekendt med alle relevante oplysninger om advarslen, herunder indholdet, afsenderen (hvis denne oplysning haves), og under hvilke omstændigheder advarslen er modtaget.

Hvis den modtagne meddelelse er åbenbart grundløs, fx fordi den vedrører forhold, som ikke er tilstrækkeligt konkrete, eller hvis meddelelsen kommer fra en afsender, der ikke formodes at have indsigt i truslen om hvidvask eller terrorfinansiering, vil der ikke skulle ske rapportering til virksomhedens øverste ledelsesorgan, da meddelelsen herved falder uden for advarselsbegrebet. En beslutning om ikke at rapportere skal dokumenteres.

Virksomhedens øverste ledelsesorgan skal forholde sig til rapporteringen om advarslen og på baggrund heraf foranledige nødvendige og passende foranstaltninger. Det kan fx bestå i at standse en mistænkelig transaktion, underrette Hvidvasksekretariatet eller foretage en intern undersøgelse af mistænkelige forhold og som følge heraf ændre virksomhedens forretningsgange.

Finansielle sanktioner

12

12.1 Finansielle sanktioner

Spiludbydere omfattet af hvidvaskloven skal overholde love og forordninger indeholdende regler om finansielle sanktioner mod lande, personer, grupper, juridiske personer eller organer og derved blandt andet sikre imod, at udbuddet muliggør en kundes direkte eller indirekte råden over økonomiske midler, hvis kunden er oplistet i indefrysningsbilagene til den konkrete forordning. Situationen er relevant, hvor der udbydes spil i lande eller til personer omfattet af reguleringen, og hvis fx kunder i Danmark kan interagere med disse personer igennem P2P-platforme, såsom pokerplatforme.

Det betyder, at en spiludbyder skal screene sine kunder mod de til enhver tid gældende og opdaterede lister. Det er op til spiludbyderen at sikre, at der foretages screening. Dette kan fx ske ved brug af udbydere af screeningsværktøjer.

Alle EU-forordninger, der indeholder sanktioner, kan findes på EU's hjemmeside. EU-forordningerne ændres regelmæssigt med nye personer og EU har oprettet et "Sanctions Map", hvor samtlige personer der er direkte underlagt sanktioner kan findes. Personer underlagt krav om indefrysning er markeret med et frost-symbol.

Udover de personer, der er oplistet i EU-forordningerne, er spiludbyderen også forpligtet til at sikre, at virksomhedens kunder ikke er oplistet på FN's konsoliderede indefrysningsliste. Af listen fremgår navnene på de individer, grupper, virksomheder og enheder, som FN enten har tilføjet eller slettet fra en indefrysningsliste. Disse oplysninger er endnu ikke gennemført i EU-lovgivning. Navnene på listen vil blive slettet, når EU har gennemført opdateringerne i EU-forordningerne og offentliggjort den i EU-tidende. Listen findes på Erhvervsstyrelsens hjemmeside.

Indefrysning er et administrativt midlertidigt indgreb. Indefrysning berører ikke ejerskabet af midlerne, der fortsat tilhører ejeren. Når personen ikke længere fremgår af sanktionslisten, skal midlerne derfor tilbage til ejeren. Indefrysning skal ske straks, når en person kommer på en sanktionsliste.

Opdateringer af fx forordninger om indefrysningslister kan forekomme jævnligt, og det er derfor vigtigt, at spiludbyderen sikrer sig, at virksomheden altid anvender de opdaterede lister.

For yderligere information om sanktioner og indefrysning henvises til Erhvervsstyrelsens hjemmeside, hvor der ligeledes findes en vejledning om indefrysning.

Tavshedspligt

13

13.1 Hvilke oplysninger har man pligt til at hemmeligholde?

Hvidvasklovens § 38, stk. 1

Spiludbydere har efter hvidvasklovens § 38, stk. 1, pligt til at hemmeligholde nedenstående oplysninger:

- At der er sket underretning til Hvidvasksekretariatet
- At det overvejes, at der skal ske underretning
- At der er iværksat en undersøgelse
- At der vil blive iværksat en undersøgelse.

Det er alene ovenstående oplysninger, som er omfattet af tavshedspligten. Der kan derfor godt være situationer, hvor der sker videregivelse af oplysninger om en mistanke til andre juridiske enheder i en koncern, som ikke er omfattet af tavshedspligten. Det kan også ske, at der sker videregivelse til andre juridiske enheder, som ikke er i samme koncern, fx hvis en underleverandør konstaterer en mistænkelig adfærd hos en kunde og herefter oplyser spiludbyderen om denne. En spiludbyder må således også godt oplyse en anden spiludbyder om, at førstnævnte har mistanke om, at en ansat hos sidstnævnte har begået en overtrædelse af hvidvaskloven. I alle tilfælde gælder, at der er databeskyttelsesretlige regler, som man skal være opmærksom på og overholde.

Tavshedspligten er tidsubegrænset, hvilket betyder, at spiludbyderen ikke må oplyse en kunde om, at spiludbyderen har foretaget en underretning af kunden tidligere, men at underretningen ikke førte til noget.

Der er tavshedspligt om ovenstående oplysninger, da det vil kunne skade en eventuel efterforskning, hvis oplysningerne ikke hemmeligholdes. I

13.2 Undtagelser til tavshedspligten

Hvidvasklovens §§ 37 og 38, stk. 2

Spillemyndigheden kan anmode spiludbydere om oplysninger til brug for Spillemyndighedens tilsynsvirksomhed. Ved anmodning kan spiludbyderen i medfør af hvidvasklovens § 38, stk. 2, videregive nedenstående oplysninger til Spillemyndigheden:

- At der er sket underretning til Hvidvasksekretariatet
- At det overvejes, at der skal ske underretning
- At der er iværksat en undersøgelse
- At der vil blive iværksat en undersøgelse.

Undtagelserne medfører ikke en generel pligt for spiludbyderen til at informere Spillemyndigheden om underretninger.

Herudover kan der ske videregivelse til retshåndhævelsesformål, som omfatter forebyggelse, efterforskning, opdagelse og retsforfølgning af straffelovsovertrædelser og desuden beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed.

Det anses ligeledes ikke som et brud på tavshedspligten, hvis en spiludbyder i god tro giver underretninger eller oplysninger i medfør af underretningspligten i hvidvasklovens § 26, og det påfører dermed heller ikke spiludbyderen, dens ledelse eller ansatte nogen form for ansvar. Det fremgår af hvidvasklovens § 37.