Behandling av personopplysninger ved etterlevelsen av hvitvaskingsloven

I hvilken utstrekning gir GDPR-regelverket rapporteringspliktige et handlingsrom til å behandle personopplysninger ved bekjempelsen av hvitvasking?

Kandidatnummer: 002

Antall ord: 14 997

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

10. desember 2024

Innholdsfortegnelse

Innholdsfortegnelse **2**

1. Innledning **4**

1.1 Aktualitet, tema og problemstilling *4*

1.2 Avgrensninger og presiseringer av tema *6*

1.3 Metodiske grep og den videre fremstillingen *6*

2. Kontekst og bakgrunn **8**

2.1 Personopplysningsloven og GDPR *8*

2.1.1 Innledende om GDPR-regelverket 8

2.1.2 Formål og hensyn bak personopplysningsregelverket 9

2.1.3 Personvernprinsippene som regelverkets hovedforpliktelser 11

2.1.4 Personopplysningssikkerhet og personvernkonsekvensvurdering 14

2.2 Hvitvaskingsloven og EU´s fjerde hvitvaskingsdirektiv *14*

2.2.1 Utviklingen av AML-regelverket 14

2.2.2 Formål og hensyn bak hvitvaskingsregelverket 15

2.2.3 Hvitvaskingslovens hovedforpliktelser 16

2.2.4 Hvitvaskingslovens risikoprinsipp 18

3. Forholdet mellom regelverkene **19**

3.1 Aktualitet *19*

3.2 Rettskildene om forholdet *19*

3.3 Regelverkenes kryssende hensyn *23*

4. Et spenningsforhold mellom regelverkene? **23**

4.1 Forholdsmessighetsvurderingen *23*

4.2 Hvitvaskingsloven § 17 om forsterkede kundetiltak *24*

4.2.1 Høyrisikokunder 24

4.2.2 Politisk eksponerte personer og deres nære familiemedlemmer og kjente medarbeidere 25

4.2.3 Grunnkravene i hvitvaskingsloven §§ 12 til 15 29

4.3 Hvitvaskingsloven § 25 om undersøkelsesplikten *31*

4.4 Hvitvaskingsloven § 26 om rapporteringsplikten *35*

4.5 Hvitvaskingsloven § 31 (3) om utveksling av opplysninger *36*

4.6 Begrensninger i innsynsretten *40*

5. Tiltak for harmonisering av dagens regelverk **42**

5.1 Innledende *42*

5.2 Kunnskap og ressursbruk *42*

5.3 Interne retningslinjer og rutiner *42*

5.4 Garantier for informasjonssikkerhet og forbrukerperspektivet *44*

5.5 Lovbestemt plikt til rutiner for antihvitvask og personvernbeskyttelse *45*

5.6 Begrensning av skjønnsvurderinger *46*

5.7 Tilsyn og veiledning for antihvitvask og personvern 47

6. Avsluttende betraktninger 48

Referanseliste 51

Lover og forskrifter 51

Internasjonale konvensjoner, traktater og direktiver 52

Forarbeider, offentlige dokumenter, rundskriv, retningslinjer, mv. 54

Internasjonale veiledninger, rapporter, arbeidsdokumenter mv. 56

Rettspraksis 57

Litteratur (alfabetisk) 59

Avisartikler, innlegg, statistikk, rapporter, mv. (etter publiseringsdato) 61

1. Innledning

1.1 Aktualitet, tema og problemstilling

Hvitvasking og terrorfinansiering har fått et stadig større fokus, både nasjonalt og internasjonalt. FN anslår at hvitvasking på årlig basis utgjør mellom 2-5% av verdens samlede bruttonasjonalprodukt, tilsvarende et sted mellom 800 milliarder og 2 billiarder dollar.[1] Som del av en effektiv bekjempelse av hvitvasking og terrorfinansiering stiller hvitvaskingsloven krav til at enkelte yrkesgrupper skal «kjenne sine kunder» og rapportere mistenkelige forhold til Økokrim. Rapportene skal sendes til Økokrim sin enhet for finansiell etterretning (EFE) og går under betegnelsen «MT-rapporter». Økokrims årsrapport for 2023 viser at mer en 73.600 unike privatpersoner og organisasjoner ble omtalt i totalt 23.703 innsendte MT-rapporter.[2] I mai 2024 vedtok Europaparlamentet og Det europeiske råd den nye, ambisiøse «AML-pakken», som blant annet tilrettelegger for et kommende europeisk antihvitvaskingstilsyn («AMLA»), et sjette hvitvaskingsdirektiv og en hvitvaskingsforordning.[3]

I 2023 utgjorde vinningslovbrudd nærmest 45% av alle anmeldte lovbrudd.[4] En stor andel av begåtte forbrytelser motiveres dermed ofte av ønsket om økonomisk gevinst. Forbrytelser med større utbytte, slik man gjerne ser i internasjonal eller organisert kriminalitet, byr som regel på utfordringer knyttet til håndteringen av midlene. Oppbevaring i kontantformat er problematisk av flere grunner, blant annet grunnet plassmangel, risiko for ødelagte sedler eller for at myndighetene har identifisert sedlenes serienummer og varsles når sedlene benyttes i den legale økonomien. For å kunne nyte godt av illegale midler, må ulovlige penger «vaskes hvite»; derav begrepet «hvitvasking». Som et resultat av kriminelles hvitvaskingsbehov misbrukes ofte legitime næringsvirksomheter. Bankvesenet og andre rapporteringspliktige blir dermed uvitende medhjelpere i hvitvaskingsprosessen.[5]

Som del i arbeidet med å forebygge og avdekke hvitvasking og terrorfinansiering, har lovgiver gjennom hvitvaskingsloven og hvitvaskingsforskriften gitt rapporteringspliktige adgang og plikt til å iverksette tiltak for å bidra til en effektiv bekjempelse av hvitvasking og terrorfinansiering.[6] En stor del av disse tiltakene innebærer innsamling, lagring og deling av

[1] UNODC, (u.d.).
[2] Økokrim (2023), side 31.
[3] European Council (2024); Direktiv 2024/1640; Forordning 2024/1624.
[4] SSB (2024).
[5] Økokrim (2021).
[6] Hvitvaskingsloven § 4.

personopplysninger. Følgelig griper mye av antihvitvaskingsarbeidet inn i personopplysningsvernet til enkeltmennesket.

Økt digitalisering og fokus på menneskerettigheter, herunder rett til privatliv, resulterte i vedtakelsen av EUs generelle personopplysningsforordning (GDPR) i 2016.[7] To år senere oppdaterte lovgiver personopplysningsloven i tråd med EU-forordningen.[8] I etterkant av implementeringen har GDPR-skandaler og millionbøter til private og offentlige institusjoner bidratt til ytterligere bevissthet rundt personopplysningsvern.[9] I arbeidet med antihvitvasking har personopplysningsvernet blitt særlig aktuelt etter EU-domstolens avgjørelse om at offentlig tilgang til registre over reelle rettighetshavere strider med GDPR.[10]

De to regelverkene bygger på svært ulike hensyn som må veies opp mot hverandre. Ved anvendelsen av regelverkene vil hensynet til effektiv bekjempelse av hvitvasking og terrorfinansiering måtte avveies mot hensynet til vern av personopplysninger og privatliv. Utfordringen knyttet til avveiningen oppstår idet hvitvaskingsloven går langt i å pålegge plikt til å behandle personopplysninger for rapporteringspliktige. Eksempelvis fastslår hvitvaskingsloven § 26 en lav terskel for å rapportere til Økokrim, hvor rapporteringsplikten forutsetter omfattende behandling av informasjon, herunder personopplysninger, for at MT-rapporten anses tilstrekkelig dokumentert. Det strenge forbudet mot å informere kunden om delingen av personopplysningene etter hvitvaskingsloven § 28, medfører at borgerne i praksis nærmest aldri får vite at vedkommendes personopplysninger er delt. Avhandlingen problematiserer regelverkenes spenningsforhold og avveiningen av hensynene i *kapittel 3* og *4*.

Ettersom de to risikobaserte regelverkene både er kompliserte og omfangsrike i sitt innhold, er det avgjørende at de som anvender regelverkene har en god forståelse for innholdet i og formålet bak både hvitvaskings- og GDPR-reglene. God forståelse for regelverkenes sammenhenger gir rettsanvenderen mulighet til å implementere tiltak som er tilpasset risikoen, samtidig som kravene til nasjonale og internasjonale standarder blir ivaretatt.

Avhandlingen tar sikte på å avklare forholdet mellom hvitvaskingsloven og GDPR. Avklaringen innebærer en vurdering av i hvilken grad og på hvilken måte det foreligger et spenningsforhold mellom hvitvaskingslovens bestemmelser og GDPR ved behandling av personopplysninger

[7] Forordning 2016/679.
[8] Personopplysningsloven § 1.
[9] NRK (2018).
[10] *Luxembourg Business Registers* [GC] C-37/20 og C-601/20, avsnitt 83.

som ledd i bekjempelse av hvitvasking. Forutsatt et spenningsforhold vil jeg drøfte i hvilken utstrekning GDPR-regelverket gir rapporteringspliktige et handlingsrom til å behandle personopplysninger ved etterlevelsen av hvitvaskingsloven samt hvilke tiltak som kan iverksettes for best mulig harmonisering av lovverkene.

1.2 Avgrensninger og presiseringer av tema

Hvitvaskingsloven regulerer det som etter straffeloven klassifiseres som hvitvasking og terrorfinansiering.[11] Avhandlingens tema, spenningsforholdet mellom hvitvaskingsloven og personopplysningsloven, medfører ikke et behov for å skille mellom begrepene hvitvasking og terrorfinansiering. For alle praktiske formål vil det som skrives om hvitvasking også gjelde for terrorfinansiering.

Selv om problemstillingen om et spenningsforhold mellom hvitvaskingsloven og GDPR oppstår gjennomgående ved anvendelse av hvitvaskingsloven, vil jeg foreta en analyse av utvalgte rettsregler. Avhandlingen avgrenses til hvitvaskingslovens bestemmelser om forsterkede kundetiltak etter § 17, gjennomføring av undersøkelser etter § 25, rapporteringsplikt etter § 26, rapporteringspliktiges adgang til å utveksle opplysninger etter § 31 (3) og innsynsrett i rapporteringspliktiges behandling av personopplysninger. Bakgrunnen for utvalget skyldes at bestemmelsene inneholder regler hvor det særlig kan oppstå spenningsforhold mellom hvitvaskingsloven og personopplysningsregelverket. Avgrensningen er hensiktsmessig, ettersom bestemmelsene regulerer hvilke tiltak rapporteringspliktige kan og skal iverksette. Øvrige lovbestemmelser i hvitvaskingsloven vil behandles der dette er hensiktsmessig i relasjon til de overnevnte bestemmelsene.

I tillegg vil avhandlingen fokusere på bankers behandling av personopplysninger ved etterlevelsen av hvitvaskingsloven. Avhandlingen avgrenses dermed mot de øvrige institusjonene som angitt i hvitvaskingsloven § 4 (1) bokstav b til o. Avgrensingen skyldes at banker utgjør den største MT-rapporteringsgruppen, med hele 75% av det totale antallet MT-rapporter som ble sendt til EFE i 2023.[12]

1.3 Metodiske grep og den videre fremstillingen

Det foreligger ikke avklarende norsk rettspraksis eller tilsynspraksis om temaet. For å få en grundigere forståelse av problemstillingens praktiske sider, har jeg foretatt konfidensielle

[11] Hvitvaskingsloven § 2 (1) bokstav a og b, smh. straffeloven §§ 332 og 337.
[12] Økokrim (2023), side 4.

samtaler med Datatilsynet samt banker av varierende størrelse. Samtalepartnerne har gitt meg innspill til problemstillinger og informasjon på utvalgte områder om hvordan rettsreglene anvendes i praksis. Sistnevnte informasjon var av uforpliktende art og følger ikke av empiriske undersøkelser.

I den videre fremstillingen skal jeg først ta for meg konteksten og bakgrunnen for de gjeldende regelverkene for antihvitvaskingsarbeidet og personopplysningsvernet (*kapittel 2*). Kapittelet vil ta for seg lovreguleringenes historiske bakteppe, sette avhandlingens problemstilling i kontekst samt gjengi regelverkenes overordnede hovedtrekk. I *kapittel 3* presenteres forholdet mellom hvitvaskingsloven og personopplysningsloven. Kapittelet tar sikte på å undersøke sammenhengen mellom regelverkene, sett i lys av at lovene skal ivaretar ulike formål; effektiv bekjempelse av hvitvasking og terrorfinansiering, og å ivareta personopplysningsvernet og retten til privatliv.

Som følge av at lovene bygger på ulike formål og hensyn vil avhandlingens *kapittel 4* omfatte en analyse av spenningsforholdet som oppstår mellom de to regelverkene. Selv om problemstillingen oppstår gjennomgående ved anvendelse av hvitvaskingsloven, vil avhandlingen gjøre en nærmere vurdering av utvalgte rettsregler, der problemstillingen gjør seg særlig aktuell. Kapittelet vil ta for seg bestemmelsene i hvitvaskingsloven §§ 17, 25, 26 og 31 (3) og begrensninger i innsynsretten, samt en vurdering av grensen for rapporteringspliktiges adgang til å behandle personopplysninger i samsvar med GDPR for disse bestemmelsene. Analysen vil kartlegge hvilke tilfeller som klart er i strid med GDPR-regelverket, hvilke tilfeller som faller innenfor regelverket og en vurdering av om det er mulig å fastslå en konkret grense for gråsone-tilfellene.

Kapittel 5 i avhandlingen vil omfatte vurderinger av hvilke tiltak som kan bidra til en mer harmonisert etterlevelse av regelverkene når rapporteringspliktige behandler personopplysninger. Det vil også gjøres bemerkninger knyttet til hvilke tiltak Finanstilsynet, Datatilsynet og lovgiver kan iverksette som løsning på dagens utfordringer. De avsluttende betraktningene i *kapittel 6* består av en konsekvensvurdering av dagens regelverk og et kritisk blikk på lovverket. Det vil også knyttes bemerkninger til EUs nye «AML-pakke» som gjenstand for veien videre.

2. Kontekst og bakgrunn

2.1 Personopplysningsloven og GDPR

2.1.1 Innledende om GDPR-regelverket

Som følge av økende digitalisering trådte personregisterloven i kraft 1. januar 1980. Personregisterloven var den første generelle norske loven om behandling av personopplysninger.[13] Etter at personverndirektivet ble inntatt i EØS-avtalen,[14] erstattet personopplysningsloven (2000) den tidligere personregisterloven. Den oppdaterte 2000-loven baserte seg på EU-direktivet og resulterte i en bredere norsk lov enn tidligere, ettersom loven med tilhørende forskrifter ga detaljerte regler om hvordan personopplysninger generelt skulle behandles.[15]

I 2012 vedtok EU en kraftig reform av reglene om personopplysningsvern, og i 2016 kom personvernforordningen.[16] Overgangen fra direktiv til forordning fikk følger for alle EU- og EØS-medlemmene, og resulterte i et svært generelt regelverk.[17] At regelverket er generelt illustreres blant annet gjennom forordningens brede virkeområdet for privat og offentlig sektor, regelverkets kompleksitet samt at regelverket bygger på lovbestemte prinsipper. Endringen fra direktiv til forordning ble begrunnet i et ønske om å styrke enkeltpersoners personopplysningsvern, åpne for fri utveksling av personopplysninger innad i EU og EØS samt å sikre et samkjørt og harmonisert personopplysningsregelverk i unionen.[18] Ifølge EØS-avtalen artikkel 7 bokstav a er «en rettsakt som tilsvarer en EØF-forordning» bindende for Norge, og skal gjennomføres uten inkorporerte endringer. Innlemmelsen av GDPR i EØS-avtalen, resulterte dermed i at forordningen skulle gjelde som norsk lov. Dagens personopplysningslov består dermed av både GDPR og nasjonale lovbestemmelser som supplerer reglene i forordningen.

[13] Wessel-Aas og Ødegaard (2018), side 87.
[14] Direktiv 95/46/EF.
[15] Wessel-Aas og Ødegaard (2018), side 92.
[16] Official Journal of the European Union, 2012/C 192/05.
[17] Schartum (2020), side 29.
[18] Justis- og beredskapsdepartementet (2018).

2.1.2 Formål og hensyn bak personopplysningsregelverket

Personopplysningsregelverket bygger grunnleggende sett på retten til privatliv og retten til personopplysningsvern. GDPRs formål er å sikre enkeltindividers grunnleggende rettigheter og friheter og samtidig tilrettelegge for fri utveksling av personopplysninger.[19] Den europeiske menneskerettighetsdomstolen har ved flere anledninger konstatert at behandling av personopplysninger anses som inngrep i Den europeiske menneskerettighetskonvensjonen (EMK) artikkel 8 om retten til privatliv.[20] EU-domstolen har konstatert tilsvarende.[21]

Retten til privatliv er nedfelt i Grunnloven § 102, EMK artikkel 8 og EU-Charteret artikkel 7. Den grunnleggende menneskerettigheten favner vidt,[22] der personopplysningsvernet kun utgjør en del av privatlivrettigheten. At retten til privatliv har grunnlovsrang, medfører at bestemmelsen også får betydelig gjennomslagskraft ved utformingen og fortolkningen av lavere rangs lovgivning. Høyesterettspraksis har i flere tilfeller illustrert hvordan grunnlovsbestemmelser kan får avgjørende betydning for tolkningen av annen nasjonal lovgivning.[23] Personopplysningsvernet utgjør en del av privatlivrettigheten og er gitt vern i Charteret artikkel 8. Ettersom Charteret ikke er en del av EØS-avtalen,[24] er ikke rettskilden bindende for Norge. Charteret gir imidlertid uttrykk for EU´s grunnleggende rettigheter. Der Charteret samsvarer med bestemmelser i EMK, fremstår det kunstig å ikke anse Charteret som en relevant rettskilde for tolkningen av EØS-retten.[25] Det europeiske personvernrådet (EDPB), som gir veiledning om tolkningen av GDPR, har uttalt at rådets veiledninger baseres på Charteret og de EMK-bestemmelsene som samsvarer med Charteret.[26] Personopplysningsvernet konstateres også i TFEU artikkel 16.[27]

Øvrig folkerett understreker ytterligere den brede oppfatningen av personopplysningsvernets viktighet.[28] Tilsvarende illustrerer det ulovfestede personvernet rettighetens dype forankring. Høyesterett har ved flere anledninger nektet bevisføring i straffesaker, med grunnlag i det

[19] GDPR artikkel 1.
[20] *S. og Marper mot UK* (2008), avsnitt 67; *Mockutė mot Litauen* (2018), avsnitt 99.
[21] *Luxembourg Business Registers* [GC] C-37/20 og C-601/20.
[22] Rt-2012-2039, avsnitt 70; *Üner mot Nederland* (1999).
[23] Rt-2015-833, avsnitt 14; Rt-2014-976, avsnitt 37; HR-2016-831-U.
[24] Stortinget (2020).
[25] Fredriksen (2013).
[26] EDPB Recommendations 02/2020, punkt 2.
[27] Traktaten om den europeiske unions virkemåte (TFEU).
[28] FN-konvensjonen om sivile og politiske rettigheter artikkel 17; OECD Guidelines (1980).

alminnelige personvernhensynet.[29] Følgelig vil retten til privatliv og personopplysningsvernet, utgjøre en tungtveiende faktor i interesseavveininger ved anvendelsen av GDPR-regelverket.

Retten til privatliv er likevel ikke absolutt, og det kan unntaksvis gjøres inngrep. Ifølge EMK artikkel 8 (2) kan inngrep legitimeres, dersom inngrepet er «i samsvar med lov» og er «nødvendig i et demokratisk samfunn» av hensyn til et nærmere angitt formål. Adgangen til inngrep beror dermed på hvorvidt inngrepet er forankret i lov, forfølger et legitimt formål og er forholdsmessig. Ifølge Høyesterettspraksis skal Grunnloven § 102 tolkes likt.[30] Tilsvarende vilkår følger av EU-Charteret artikkel 52 (1). Forholdsmessighetsvurderingen innebærer et spørsmål om inngrepet er proporsjonalt sett opp mot formålet som begrunner inngrepet.[31] I hvilken grad inngrep i privatlivet kan aksepteres er dermed avhengig av formålet med behandlingen av personopplysningene.

Inngrep i privatlivet som følge av behandling av personopplysninger ved etterlevelsen av hvitvaskingsregelverket er begrunnet i allmenne hensyn. Etter EMK artikkel 8 (2) kan hensynet til kriminalitetsforebygging og landets økonomiske sikkerhet rettferdiggjøre inngrep. Behandlingen av personopplysninger i antihvitvaskingsarbeidet kan begrunnes i begge formål.[32] Hvorvidt rapporteringspliktige kan behandle personopplysninger ved etterlevelsen av hvitvaskingsloven beror på en avveining mellom retten til privatliv og hensynet til kriminalitetsbekjempelse.

Beskyttelsen av retten til personopplysningsvern og privatliv har godt fotfeste i både nasjonale og internasjonale forpliktelser. Viktigheten av vernet om rettighetene bygger på at enkeltpersoner skal kunne ha kontroll over informasjon om seg selv og at informasjonen behandles på en forsvarlig og rettferdig måte. Lovregulering bidrar til å forebygge misbruk av personopplysninger, for eksempel i forbindelse med økonomisk kriminalitet eller som gjenstand for medisinsk feilbehandling. I tillegg sikrer regulering opprettholdelse av tillit til private og offentlige institusjoner som behandler opplysningene, samt demokratisk stabilitet slik at individer kan uttrykke seg fritt uten frykt for overvåkning eller represalier. Beskyttelse av personopplysningsvernet bidrar også til at retten til å ikke bli diskriminert på bakgrunn av for eksempel etnisitet, kjønn eller helsestatus blir overholdt.

[29] Rt-1991-616, side 623; Rt-1996-1114, side 1119.
[30] Rt-2015-93, avsnitt 60.
[31] *Olsson mot Sverige* (1988), avsnitt 67.
[32] Se kapittel 2.2.2.

Gjennomgangen ovenfor illustrerer hvordan retten til privatliv, samt person- og personopplysningsvernet har et godt fotfeste i både nasjonale og internasjonale forpliktelser. De grunnleggende rettighetene må følgelig få betydning ved rettsanvendelsen av øvrig nasjonal lovgivning, deriblant hvitvaskingsloven.

2.1.3 Personvernprinsippene som regelverkets hovedforpliktelser

I forlengelsen av de formål og hensyn som personopplysningsregelverket bygger på, danner personvernprinsippene grunnlaget for GDPR-bestemmelsene som utgjør faktiske rettigheter i egentlig forstand. Prinsippene operer som overordnede normer,[33] som samtidig fungerer som «retningslinjer for datatilsynsmyndigheter, domstoler og andre klageorganer» ved etterlevelsen av lovverket.[34] I tillegg utgjør prinsippene grunnleggende krav til behandling av personopplysninger, som til enhver tid må hensyntas ved tolkningen av forordningens øvrige bestemmelser.[35]

«Lovlighet, rettferdighet og åpenhet»

Det følger av GDPR artikkel 5 (1) bokstav a at behandlingen av personopplysninger må være «lovlig, rettferdig og åpen» for den registrerte. At behandlingen av personopplysninger skal være lovlig innebærer at den må ha hjemmel. Hva som utgjør rettslig grunnlag følger av GDPR artikkel 6, 9 og 10 samt annen spesiallovgivning. Eksempelvis stilles det krav til at behandlingen av personopplysninger ved antihvitvaskingsarbeidet skal følge av norsk lov, noe som følger av hvitvaskingsloven og hvitvaskingsforskriften. Lovligheten må dessuten tilfredsstille de krav som følger av EU-retten, menneskerettigheter og nasjonale konstitusjoner.[36] Mens lovlighet knytter seg til fastsatte rettsregler, knytter «rettferdighet» seg til de innholdsmessige interesseavveiningene som personvernspørsmål aktualiserer.[37] Rettferdighetsprinsippet innebærer at sammenhengen mellom behandlingen og formålet med behandlingen, må fremstå som rimelig for den registrerte. For antihvitvaskingsarbeidet vil rettferdighetsprinsippet innebære en vurdering av om personopplysningsbehandlingen er rettferdig sett i forhold til formålet om å bekjempe hvitvasking. At behandlingen skal være «åpen» gir uttrykk for at den skal være transparent. Ifølge GDPR fortalepunkt 39 krever prinsippet at informasjonen og kommunikasjonen rundt behandlingen av opplysningene skal være enkelt tilgjengelig og lett å forstå for den registrerte. Artikkel 29-gruppen, et uavhengig

[33] HR-2021-966-A, avsnitt 37.
[34] Schartum og Bygrave (2016), side 114-115.
[35] Prop.56 LS (2017), side 257; Skullerud mfl. (2018), side 74-75.
[36] Skullerud mfl. (2018), side 75.
[37] Schartum (2020), side 89.

rådgivende EU-organ for databeskyttelse og personopplysningsvern, har uttalt at åpenhet i GDPR dekker tre området: (i) informasjon til den registrerte om rettferdig behandling av data, (ii) den behandlingsansvarliges kommunikasjon med registrerte angående vedkommendes rettigheter etter GDPR, og (iii) den behandlingsansvarliges tilretteleggelse for at de registrerte kan utøve sine rettigheter.[38]

«Formålsbegrensning»

I bestemmelsens bokstav b lovfestes prinsippet om formålsbegrensning, et prinsipp som innebærer at personopplysninger bare må innhentes for «spesifikke, uttrykkelig angitte og berettigede formål». I Rt-2013-143 avsnitt 47 uttalte Høyesterett at prinsippet innebærer at «innsamling av opplysninger skal skje til uttrykkelig angitte formål, og at senere behandling ikke må være uforenelig med disse formål». At formålet må være spesifikt og uttrykkelig angitt, innebærer at bakgrunnen for behandlingen ikke kan være uklart for den registrerte.[39] Kravet om berettiget formål innebærer at behandlingen må være i samsvar med annet regelverk og andre samfunnskrav.[40] Formålsbegrensningsprinsippet består dermed av to deler: det skal være klart for den registrerte hvorfor personopplysningene behandles, og opplysningene skal ikke brukes til noe annet enn det forutbestemte og konstaterte formålet. Ved etterlevelse av hvitvaskingsloven kan personopplysninger dermed ikke benyttes til andre formål enn bekjempelse av hvitvasking.[41]

«Dataminimering»

Prinsippet om dataminimering innebærer at personopplysninger bare kan behandles, dersom de er «adekvate, relevante og begrenset til det som er nødvendig for å nå formålene de behandles for», jf. artikkel 5 (1) bokstav c. Det må følgelig være en nær og naturlig sammenheng mellom behandlingsformålet og de opplysningene som behandles, samtidig som opplysningene må være egnet til å oppnå formålet med behandlingen.[42] Personopplysninger kan bare behandles dersom formålet med behandlingen ikke med rimelighet kan oppnås på andre måter.[43] Prinsippet forutsetter dermed et krav om nødvendighet, herunder hvorvidt andre opplysninger av mindre inngripende art kan gjøre samme nytte.

«Riktighet»

[38] Artikkel 29-gruppen (2017/2018), side 4.
[39] Skullerud mfl. (2018), side 76.
[40] Skullerud mfl. (2018), side 76.
[41] Se kapittel 2.2.2.
[42] Skullerud mfl. (2018), side 77.
[43] GDPR fortalepunkt 39.

GDPR artikkel 5 (1) bokstav d gir uttrykk for prinsippet om personopplysningenes riktighet, ved at opplysningene må være «korrekte og om nødvendig oppdaterte». At opplysningene er korrekte er av stor betydning for den registrerte, men viktigheten av korrekte opplysninger vil likevel være avhengig av hva personopplysningene skal brukes til. Det vil åpenbart være av større betydning for den registrerte, dersom bostedsadressen er ukorrekt ved inkassokrav sammenlignet med utsendelse av reklamebrosjyrer.

«Lagringsbegrensning»

Prinsippet om lagringsbegrensning følger av bokstav e, og innebærer at opplysningene ikke må lagres lenger enn det som er nødvendig, og forutsetter dermed at personopplysninger på et tidspunkt må slettes. Lagring må være nødvendig for å oppnå formålet med behandlingen, og skal etter prinsippet slettes eller anonymiseres når formålet er oppnådd. Unntaksvis kan opplysningene lagres lenger, dersom lagringen er i samsvar med de formål som følger av GDPR artikkel 89.

«Integritet og konfidensialitet»

Prinsippet om sikring av «integritet og konfidensialitet følger av bokstav f, og innebærer at den behandlingsansvarlige sørge for en forsvarlig og tilstrekkelig sikring av personopplysningene. Prinsippet anses å ha fått gjennomslag grunnet den teknologiske utviklingen, som har medført vesentlig forhøyet risiko for innsyn i, uautorisert behandling, tap, endring og ødeleggelse av opplysningene.[44]

«Ansvarlighet»

Ansvarlighetsprinsippet er utskilt i artikkel 5 (2), og innebærer at den behandlingsansvarlige er ansvarlig for etterlevelsen av de øvrige prinsippene i artikkel 5 (1) bokstav a til f. Ansvarlighetsprinsippet krever også at den behandlingsansvarlige skal kunne påvise etterlevelsen.[45] Sett i sammenheng med de øvrige prinsippene, kan ansvarlighetsprinsippet sies å innebære at den behandlingsansvarene må opptre på en ansvarsfull måte under alle ledd i behandlingsprosessen.

[44] Skullerud mfl. (2018), side. 78.
[45] Skullerud mfl. (2018), side 79.

2.1.4 Personopplysningssikkerhet og personvernkonsekvensvurdering

GDPR er et risikobasert regelverk, som innebærer at adgangen til å behandle personopplysninger må baseres på en konkret risikovurdering. Etter GDPR artikkel 32 skal det alltid foretas en risikovurdering av personopplysningssikkerheten. Vurderingen skal identifisere områder som kan resultere i uautorisert eller utilsiktet behandling av personopplysningene som skal behandles.[46] Hensikten er å avdekke kunnskap om risikoene som eksiterer, slik at man kan iverksette adekvate tiltak for å senke risikoen for ulovlig behandling. I tillegg krever GDPR artikkel 35 at databehandleren foretar en risikovurdering av personvernkonsekvensene ved behandlingen (DPIA). Risikovurderingen innebærer en kartlegging av risikoen for at behandlingen av personopplysninger krenker den registrertes personopplysningsvern.[47]

2.2 Hvitvaskingsloven og EU´s fjerde hvitvaskingsdirektiv

2.2.1 Utviklingen av AML-regelverket

I løpet av 1980- og 1990-tallet bidro utviklingen i de globale finansmarkedene til at det ble enklere å skjule bidrag av midler til terrorfinansiering og å skjule opprinnelsen til økonomisk utbytte av kriminell virksomhet i finanssystemene.[48] Resultatet ble begynnelsen på en omfattende regulering internasjonalt og nasjonalt samt opprettelsen av det mellomstatlige organet FATF.[49] Behovet for etterlevelse av internasjonale forpliktelser og en effektiv sikring av den kriminaliserende straffebestemmelsen om hvitvasking, førte følgelig til vedtakelsen av Norges første hvitvaskingslov i 2003.[50] Etter EUs vedtakelse av tredje hvitvaskingsdirektiv, ble hvitvaskingsloven (2003) erstattet av hvitvaskingsloven (2009).[51] Denne loven ble igjen erstattet av dagens hvitvaskingslov i 2018, som implementerer EUs fjerde hvitvaskingsdirektiv.[52]

Et særlig viktig tilskudd i dagens hvitvaskingslov er bestemmelsen om Finanstilsynets adgang til å ilegge overtredelsesgebyr.[53] Under henvisning til finansieringsvirksomhetsloven (1988) § 5-1 medførte brudd på de tidligere hvitvaskingslovene at bare påtalemyndigheten kunne ilegge sanksjoner, i form av straff. Bakgrunnen for endringen var en økende tendens der

[46] GDPR artikkel 32 (1)
[47] Skullerud mfl. (2018), side 220.
[48] Ot.prp.nr.72 (2002-2003), side 14.
[49] Ot.prp.nr.72 (2002-2003), side 9-10.
[50] Høgberg (2008), side 27.
[51] Direktiv 2005/60/EF.
[52] Direktiv 2015/849.
[53] Hvitvaskingsloven § 49.

kriminalitetsbekjempelsen ikke oppnådde den forventede effektiviteten. Påtalemyndigheten som eneste sanksjonsmyndighet resulterte i et politi som manglet kompetanse og ressurser til å prioritere offerløs kriminalitet. Ved å gi Finanstilsynet sanksjoneringsadgang, kunne hvitvaskingsloven håndheves i større og mer effektiv grad enn tidligere.

Kombinasjonen av økt internasjonalt fokus, EUs stadig nye hvitvaskingsdirektiver, avdekking av store bankskandaler i Norden [54] og den teknologiske utviklingen har resultert i at utviklingen av hvitvaskingsregelverket har måttet skje raskt. Det kan se ut til at den raske produksjonen av lovgivning blant annet har resultert i et uforutsett spenningsforhold mellom hvitvaskingsloven og GDPR.[55]

2.2.2 Formål og hensyn bak hvitvaskingsregelverket

Etter hvitvaskingsloven § 1 er lovens formål «å forebygge og avdekke hvitvasking og terrorfinansiering». Ordlyden «forebygge og avdekke» tilsier at hvitvaskingsloven skal virke preventivt og effektivt for bekjempelsen av hvitvasking og terrorfinansiering. Formålet bygger dermed delvis på prevensjonsformål og delvis på formålet om å produsere etterretningsinformasjon som myndighetene kan benytte til etterforskning og bevis ved straffeforfølgelse.[56]

Under henvisning til lovutvalgets uttalelse oppsummerer Finansdepartementet at lovens formål er å forebygge at finanssystemet benyttes til hvitvasking og terrorfinansiering samt «beskytte det økonomiske systemet og samfunnet som helhet mot hvitvasking og terrorfinansiering».[57] Forarbeidenes forståelse bygger i all hovedsak på det fjerde hvitvaskingsdirektivet, der det i artikkel 1 (1) heter at direktivets formål er å forebygge bruken av unionens finansielle system for hensikten å hvitvaske. I fortalepunkt 1 begrunnes behovet for direktivet med at hvitvasking kan skade den finansielle sektors integritet, stabilitet og omdømme. I tillegg skal direktivet sikre beskyttelse av det økonomiske systemet og samfunnet i sin helhet.[58] Sistnevnte kommer til uttrykk i hvitvaskingsloven § 1 (2), som fastslår at «[t]iltakene i loven skal beskytte det finansielle og økonomiske systemet samt samfunnet som helhet».

[54] DN (2018); E24 (2019).
[55] Se *kapittel 4*.
[56] Rui mfl. (2024), side 80.
[57] Prop.40 L (2017-2018), side 17-18.
[58] Fjerde hvitvaskingsdirektiv fortalepunkt 1-2.

Formålet om produksjon av etterretningsinformasjon er også understreket av Høyesterett i HR-2024-761-A. Under henvisning til juridisk teori konstaterer domstolen i avsnitt (38) at «hovedformålet med hvitvaskingsloven er at rapporteringspliktige skal fremskaffe mest mulig etterretningsinformasjon med høyest mulig kvalitet». Hvitvaskingsloven skiller seg dermed fra straffeloven, som bygger på hensynet til en repressiv reaksjon; et onde for en handling som allerede er utført.[59]

2.2.3 Hvitvaskingslovens hovedforpliktelser

I HR-2024-761-A avsnitt (37) uttalte Høyesterett at hvitvaskingsloven pålegger rapporteringspliktige fire hovedforpliktelser «for å realisere lovens formål om å «forebygge og avdekke» hvitvasking». Rapporteringspliktige skal gjøre seg kjent med sine kunder, overvåke kundene ved løpende oppfølging, undersøke forhold som kan indikere hvitvasking eller terrorfinansiering og rapportere mistanke til myndighetene.[60]

Kravet om å gjøre seg kjent med sine kunder gjennom kundetiltak innebærer at banken må iverksette tiltak for å ha tilstrekkelig kunnskap om bankens kunder («know your costumer», KYC). Reglene følger av hvitvaskingsloven §§ 9 til 23, og har som formål at den rapporteringspliktige skal skaffe seg kjennskap til sine kunder.[61] Finansdepartementet uttalte i lovforarbeidene at «kjennskap til kundens identitet og formål med kundeforholdet» vil gjøre rapporteringspliktige i stand til å oppdage «om kundeforholdet misbrukes til andre formål enn det kunden oppga i forbindelse med inngåelsen av kundeforholdet».[62] Uten kjennskap til kundene vil rapporteringspliktige ha problemer med å innfri lovens øvrige krav om løpende oppfølging, undersøkelser av avvik fra kundens normale oppførsel, og rapporteringsplikt til myndighetene. KYC-kravet forutsetter omfattende behandling av personopplysninger.[63] Som drøftet i avhandlingens *kapittel 4.2* om forsterkede kundetiltak etter hvitvaskingsloven § 17, forutsetter KYC-kravet omfattende behandling av personopplysninger.

Overvåkningskravet følger av hvitvaskingsloven § 24, og innebærer at rapporteringspliktige skal overvåke kundene sine gjennom løpende oppfølging. Bestemmelsens (1) krever kundeovervåkning for å vurdere om kundens adferd samsvarer med kundens oppgitte opplysninger om kundeforholdet. I tillegg skal bestemmelsen sikre at rapporteringspliktige har

[59] Rui mfl. (2024), side 67.
[60] Hvitvaskingsloven §§ 9-26.
[61] Rui mfl. (2024), side 280.
[62] Prop.40 L (2017-2018), side 48.
[63] Se kapittel 4.2.

oppdatert informasjon om kunden, jf. (2). Etter forarbeidene er formålet med oppfølgingen «særlig å oppdage avvikende atferd fra kunden».[64] Sett i sammenheng med KYC-kravet er det avgjørende at bankene kjenner kundens normale adferd og intensjoner med kundeforholdet.

Rapporteringspliktiges undersøkelsesplikt, som tredje hovedforpliktelse, følger av hvitvaskingsloven § 25. Dersom rapporteringspliktige «avdekker forhold som kan indikere» at midlene er tilknyttet hvitvasking, stiller hvitvaskingsloven § 25 (1) krav om at rapporteringspliktige må «foreta nærmere undersøkelser». Selv om ordlyden «kan indikere» medfører en svært lav terskel for undersøkelsesplikt, kreves objektive holdepunkter for at forholdene kan indikere hvitvaskingsforhold.[65] Hvorvidt forhold «kan indikere» hvitvasking er en skjønnsmessig vurdering, som må vurderes av den rapporteringspliktige. Tilsvarende gjelder for hvilke tiltak som skal iverksettes, da loven kun krever at rapporteringspliktige må «foreta nærmere undersøkelser». Bestemmelsens (2) pålegger rapporteringspliktige til å alltid foreta nærmere undersøkelser av kunden, dersom det avdekkes avvik i kundens normale adferd eller det som er forventet av kunden. Som i bestemmelsens (1) presiserer ikke loven hva som ligger i «nærmere undersøkelser». Den manglende presiseringen medfører at vurderingen av «nærmere undersøkelser» i stor grad er en skjønnsmessig risikovurdering, som lovgiver har valgt å overlate til den rapporteringspliktige. Hvilke «nærmere undersøkelser» som skal foretas er dermed nærmest utelukkende overlatt til bankens skjønn. At hvitvaskingsloven ikke inneholder noen begrensinger vedrørende hvilken informasjon som kan innhentes innebærer at lovteksten åpner for at rapporteringspliktige kan foreta all slags undersøkelser og innhente all slags informasjon, herunder personopplysninger, dersom de anser det nødvendig for å innfri hvitvaskingslovens forpliktelser. Hvilke personopplysninger som bør eller skal innhentes beror dermed i stor grad på en vurdering foretatt av den rapporteringspliktige.

Det siste hovedkravet som oppstilles for rapporteringspliktige er plikten til å rapportere mistenkelige forhold til myndighetene. Kravet følger av hvitvaskingsloven § 26, og har tett sammenheng med undersøkelsesplikten; dersom nærmere undersøkelser gir grunnlag for mistanke om hvitvasking, skal det rapporteres til Økokrim. Rapporteringsplikten innebærer at banken må oversende «opplysninger» om forholdene til Økokrim, samt «andre nødvendige opplysninger» etter forespørsel fra Økokrim. Bestemmelsen gir dermed uttrykk for at Økokrim både har en passiv og aktiv tilgang til opplysningene som banken har samlet inn. Økokrim kan

[64] NOU 2016:27, side 106.
[65] Rui mfl. (2024), side 459.

få informasjon ved at det er banken selv som sender en MT-rapport (passivt), eller ved at Økokrim selv tar kontakt med banken uten at banken har varslet om mistenkelige forhold (aktivt). Hvilke opplysninger som skal oversendes fremgår ikke eksplisitt av lovbestemmelsen. Spørsmålet om hvilke personopplysninger som kan og må deles oppstår dermed også under etterlevelsen av rapporteringsplikten. I forlengelsen av dette er det også bemerkelsesverdig at terskelen for mistanke er lav, men at «generell risiko, vage holdepunkter eller en «mageføelse [er] tilstrekkelig».[66] At rapporteringsplikten har svært lav terskel medfører at det er lav terskel for når rapporteringspliktige må dele personopplysninger om potensiell kriminalitet. Selv om slike opplysninger ikke er sensitive etter GDPR artikkel 9, kan det likevel oppleves stigmatiserende og sensitivt for kunden som får knyttet sitt eget navn til mistanke om hvitvasking og terrorfinansiering.

2.2.4 Hvitvaskingslovens risikoprinsipp

Ved anvendelsen av hvitvaskingsloven skal rapporteringspliktige «legge til grunn vurderinger av risiko for hvitvasking og terrorfinansiering», jf. hvitvaskingsloven § 6. Bestemmelsen gir uttrykk for risikoprinsippet, som utgjør et av regelverkets grunnprinsipper. Risikoprinsippet krever at anvendelsens av lovens øvrige bestemmelser skjer med grunnlag i en vurdering av risikoen for hvitvasking. Risikovurderingen får betydning for både kundetiltakene etter hvitvaskingsloven §§ 10 til 20 og den løpende oppfølgingen etter § 24. Hvilke tiltak som skal iverksettes vil dermed være avhengig av hvitvaskingsrisikoen. Hensikten med en risikobasert tilnærming til loven er å optimalisere arbeidet med å avdekke og bekjempe hvitvasking.[67] En risikobasert tilnærming tilrettelegger for at rapporteringspliktige kan avdekke og bekjempe hvitvasking på en mest mulig effektiv måte, ved at rapporteringspliktige prioriterer ressursene der hvitvaskingsrisikoen er høyest.

[66] NOU 2016:27, side 114.
[67] Rui mfl. (2021), side 134.

3. Forholdet mellom regelverkene

3.1 Aktualitet

Behandling av personopplysninger utgjør inngrep i retten til privatliv og retten til personopplysningsvern etter EMK artikkel 8, Grunnloven § 102 og EU-Charteret artikkel 7 og 8.[68] Lovlig behandling av personopplysninger krever at behandlingen har hjemmelsgrunnlag, følger et legitimt formål samt at behandlingen er forholdsmessig sett opp mot formålet med behandlingen.[69] Alle vilkår må være innfridd for at behandlingen er lovlig.[70] Hvitvaskingsregelverket synes imidlertid å praktiseres på en slik måte at regelverket nærmest uavkortet går foran GDPR.[71] I denne sammenheng oppstår spørsmålet om hvordan kravene til lovhjemmel, formål og forholdsmessighet ved anvendelsen av GDPR skal forstås når rapporteringspliktige etterlever forpliktelsene i hvitvaskingsregelverket.

3.2 Rettskildene om forholdet

GDPR artikkel 6 (1) oppstiller gyldige hjemmelsgrunnlag for behandling av personopplysninger. Etter bestemmelsens (1) bokstav c kan personopplysninger behandles, dersom behandlingen er «nødvendig» for å oppfylle «en rettslig forpliktelse». GDPR artikkel 6 (3) krever at den rettslige forpliktelsen er fastsatt i unionsrett eller nasjonal rett. Behandlingsadgangen må dermed utledes fra et supplerende rettsgrunnlag samt være «nødvendig». GDPR fortalepunkt 41 krever at det supplerende rettsgrunnlag er tydelig og presist.

Hvitvaskingsloven § 29 regulerer lovens forhold til personopplysningsloven, og fastslår i (1) at rapporteringspliktige «kan behandle personopplysninger for å oppfylle forpliktelser i loven eller forskrifter». Bestemmelsen gir ikke uttrykk for en «rettslig forpliktelse», men åpner for at forpliktelsene i hvitvaskingsloven og hvitvaskingsforskriften er tilstrekkelig presise som supplerende rettsgrunnlag, slik GDPR fortalepunkt 41 krever. Hvitvaskingsloven § 29 tjener ikke i seg selv som supplerende behandlingsgrunnlag, men åpner for at hvitvaskingslovens og -forskriftens forpliktelser kan tjene som supplerende rettsgrunnlag til GDPR artikkel 6 (1)

[68] Se kapittel 2.1.2.
[69] EMK artikkel 8 (2); Grunnloven § 102; EU-Charteret artikkel 52 (1).
[70] Se kapittel 2.1.2.
[71] Konfidensielle samtaler med tre banker av varierende størrelse (06.09.2024, 22.10.2024, 23.10.2024); Konfidensiell samtale med Datatilsynet (03.10.2024).

bokstav c. Hvorvidt rapporteringspliktige kan behandle personopplysninger må dermed vurderes i relasjon til hvitvaskingslovens og hvitvaskingsforskriftens konkrete forpliktelser.

Dersom forpliktelsene etter hvitvaskingsloven og hvitvaskingsforskriften skal kunne tjene som supplerende behandlingsgrunnlag, krever GDPR artikkel 6 (1) bokstav c at behandlingen er «nødvendig» for å oppfylle forpliktelsen(e). Nødvendighetsvilkåret forstås som et vilkår om at «formålet med behandlingen ikke med rimelighet kan oppfylles på annen måte».[72] Et tilsvarende nødvendighetskrav følger ikke av hvitvaskingsloven § 29, men bestemmelsen avgrenser behandling av personopplysninger til behandlinger «for å oppfylle forpliktelser». Hvitvaskingsloven gir ikke uttrykk for å erstatte nødvendighetskravet i GDPR artikkel 6, men at rapporteringspliktige bare kan behandle personopplysninger etter hvitvaskingslovens formål. Der formålet med behandlingen er hvitvaskingsbekjempelse, vil hvitvaskingsloven kunne gi grunnlag for behandling.[73] Behandling for andre formål er dermed ikke tillat, en forståelse som underbygges av hvitvaskingslovens forarbeider.[74] Ordlyd og forarbeider tilsier at rapporteringspliktige er forpliktet til en vurdering av om behandlingen av personopplysninger er «nødvendig» for formålet om hvitvaskingsbekjempelse. Dersom personopplysningene anses «nødvendig[e]» for å oppfylle hvitvaskingslovens og -forskriftens forpliktelser, vil artikkel 6 (1) bokstav c sammenholdt med hvitvaskingsloven og forskriften kunne tjene som hjemmelsgrunnlag for inngrep i retten til privatliv og personopplysningsvern.

For kravet om legitimt formål følger det av fjerde hvitvaskingsdirektiv artikkel 43 at formålet om å forebygge hvitvasking og terrorfinansiering skal anses som «matter of public interest» etter GDPR. Artikkelen fastslår at behandling av personopplysninger som ledd i bekjempelsen av hvitvasking er et akseptert formål for å behandle personopplysninger. Så lenge behandling av personopplysninger skjer med formål om å bekjempe hvitvasking, vil hvitvaskingsloven i utgangspunktet kunne gi grunnlag for behandlingen.

I tillegg til kravet om lovlighet og formål, må inngrepet være forholdsmessig sett opp mot formålet med inngrepet. For etterlevelsen av hvitvaskingsregelverkets forpliktelser innebærer dette at behandlingen av personopplysninger må være forholdsmessig sett opp mot formålet om å avdekke og bekjempe hvitvasking. Dersom behandlingen ikke er forholdsmessig for formålet

[72] GDPR fortalepunkt 39.
[73] Fjerde hvitvaskingsdirektiv artikkel 43.
[74] Prop.40 L (2017-2018), side 179.

om å bekjempe hvitvasking, kan inngrepet i retten til privatliv og personopplysningsvern ikke legitimeres.

Ettersom forholdsmessighetsvurderingen innebærer en avveining mellom retten til privatliv og personopplysningsvern på den ene siden og rapporteringspliktiges rett og plikt til hvitvaskingsbekjempelse på den andre siden, oppstår det er spenningsforhold mellom hvitvaskingsregelverket og GDPR. I praksis kan det virke som at hensynet til hvitvaskingsbekjempelse uavkortet veier tyngre enn retten til personvern og privatliv.[75] Det kan stilles spørsmål ved om en slik praksis har rettskildemessige holdepunkter.

Etter personopplysningsloven § 2 (1) andre punktum gjelder ikke loven «når annet er bestemt i eller med hjemmel i lov». Bestemmelsen åpner for at særlovgivning kan presisere eller gjøre unntak fra personopplysningsregelverket. I proposisjonen understreket Justisdepartementet at «forordningen kun kan fravikes i den utstrekning den åpner for det».[76] GDPR artikkel 23 åpner for unntak fra rettighetene i artikkel 12 til 22, dersom begrensninger anses nødvendig for å ivareta viktige samfunnsinteresser.[77] Viktige samfunnsinteresser inkluderer kriminalitetsbekjempelse, offentlig sikkerhet og finansiell sikkerhet.[78] GDPR fortalepunkt 19 klargjør særlovgivningsadgangen, dersom dette er forholdsmessig og nødvendig i et demokratisk samfunn. Begrensninger i GDPR grunnet hvitvaskingsbekjempelse kan anses nødvendig.[79] Medlemsstatenes adgang til spesiallovgivning understrekes ytterligere i GDPR fortalepunkt 73, som stiller krav til at restriksjonene må være i samsvar med kravene som følger av Charteret og EMK. Adgangen til å begrense GDPR-rettighetene må skje innenfor rammene av det som er forholdsmessig, samt respektere de grunnleggende rettighetene i EU-systemet. Avsløringsforbudet i hvitvaskingsloven § 28 er et utslag av medlemsstatenes adgang til å begrense retten til innsyn etter GDPR artikkel 15. Begrensningen av innsynsretten er basert på at lovgiver allerede har foretatt en forholdsmessighetsvurdering som balanserer retten til privatliv og personopplysningsvern mot behovet for å avdekke og forebygge hvitvasking.

I C-37/20 og C-601/20 uttalte EU-domstolen at målet med et offentlig register for reelle rettighetshavere utgjør en «general interest that is capable of justifying even serious

[75] Konfidensielle samtaler med tre banker av varierende størrelse (06.09.2024, 22.10.2024, 23.10.2024); Konfidensiell samtale med Datatilsynet (03.10.2024).
[76] Prop.56 LS (2017-2018), side 210.
[77] GDPR artikkel 23 (1) bokstav a til f.
[78] GDPR artikkel 23 (1) bokstav c til e.
[79] GDPR fortalepunkt 19.

interferences with fundamental rights enshrined in Articles 7 and 8 of the Charter».[80] Inngrep i privatlivet, gjennom behandling av personopplysninger, kan aksepteres der formålet er å bekjempe hvitvasking og terrorfinansiering. Kravene om lovlighet og proporsjonalitet gjelder likevel uavkortet. Domstolen aksepterte at inngrepet var lovlig, men ikke forholdsmessig. At inngrepet ikke var forholdsmessig, ble begrunnet med at offentlig tilgang til registrene ikke var «strictly necessary» for å bekjempe hvitvasking og terrorfinansiering.[81] I tillegg kunne slike registre sette registrerte i en særlig sårbar situasjon, og åpne for blant annet kidnapping, utpressing og vold mot de registrerte.[82] Domstolen anslo at en mulig løsning på problemet var å registrere de som etterspurte tilgang eller begrense utvalget av yrkesgrupper, institusjoner eller personer med tilgang til registeret.[83] Selv om avgjørelsen gjaldt register for reelle rettigheter, illustrer avgjørelsen at antihvitvaskarbeidet ikke gjelder uavkortet og at hensynet til å bekjempe hvitvasking ikke umiddelbart veier tyngre enn hensynet til privatliv og personopplysningsvern.

De konstitusjonelle reglene tilsier også at hvitvaskingsreglene ikke gir blankofullmakt til behandling av personopplysninger. Personvernforordningen bygger på grunnleggende rettigheter EMK artikkel 8, Grunnloven § 102 og EU-Charteret artikkel 7 og 8.[84] Kriminalitetsbekjempelse bygger til en viss grad på retten til sikkerhet etter Charteret artikkel 6, ettersom kriminalitetsbekjempelse har en allmennbeskyttende side. At hvitvaskingsdirektivet bygger på en rettighet etter Charteret, følger imidlertid ikke av direktivet og har begrenset rettskildemessig holdepunkt. En rett til vern mot kriminalitet fremgår heller ikke eksplisitt av EMK eller Charteret. Ettersom GDPR bygger på rettigheter nedfelt i Grunnloven, EMK og Charteret, vil det stride med grunnleggende menneskerettigheter og rettsstatlige prinsipper, dersom hensynet til hvitvaskingsbekjempelse generelt sett tilsidesetter hensynet til privatliv og personopplysningsvern.

I rettsteorien er det tatt til orde for at rapporteringspliktige ved utarbeidelsen av rutiner etter hvitvaskingsloven § 8 må være «oppmerksomme på at hvitvaskingslovens regler utgjør eget behandlingsgrunnlag for personopplysninger». Under henvisning til hvitvaskingsloven § 29 (2) konstateres det at hvitvaskingslovens regler «har forrang innenfor hvitvaskingslovens

[80] *Luxembourg Business Registers* C-37/20 og C-601/20, avsnitt 59.
[81] *Luxembourg Business Registers* C-37/20 og C-601/20, avsnitt 78.
[82] *Luxembourg Business Registers* C-37/20 og C-601/20, avsnitt 79.
[83] *Luxembourg Business Registers* C-37/20 og C-601/20, avsnitt 80.
[84] Se kapittel 2.1.2.

anvendelsesområde».[85] Uttalelsen forstås som at der hvitvaskingsloven gjør unntak fra GDPR, eksempelvis fra innsynsretten i avsløringsforbudet etter lovens § 28, vil hvitvaskingsloven utgjøre behandlingsgrunnlaget. Rettsteorien gir imidlertid ikke holdepunkter for at hensynet til å bekjempe hvitvasking på generelt grunnlag veier tyngre enn hensynet til privatliv og personopplysningsvern.

Ettersom hverken norsk lovgivning eller EU-rett gir uttrykk for at hensynet til å avdekke og bekjempe hvitvasking på generelt grunnlag veier tyngre enn retten til privatliv og personopplysningsvern, må rapporteringspliktige vurdere hvorvidt behandlingen av personopplysninger ved etterlevelsen av hvitvaskingsloven er forholdsmessige.

3.3 Regelverkenes kryssende hensyn

Hvitvaskingsloven og hvitvaskingsforskriften kan gi hjemmelsgrunnlag for behandling av personopplysninger. Inngrep i retten til personopplysningsvern og privatliv ved antihvitvaskingsarbeid bygger på et legitim formål. Spenningsforholdet mellom hvitvaskingsloven og GDPR settes på spissen ved forholdsmessighetsvurderingen, der det problematiske for den rapporteringspliktige vil være balanseringen av hensynet til privatliv og personopplysningsvern og til kriminalitetsbekjempelse. Som følge av spenningsforholdet oppstår spørsmålet om *hvor* i hvitvaskingsloven spenningsforholdet foreligger, og *hvordan* de kryssende hensynene bør balanseres på en mest mulig hensiktsmessig måte.

4. Et spenningsforhold mellom regelverkene?

4.1 Forholdsmessighetsvurderingen

Den nærmere vurderingen av hva som vil være forholdsmessig følger ikke av lovtekst. Forholdsmessighetsvurderingen må vurderes konkret basert på om inngrepet er strengt nødvendig og egnet for å oppnå formålet samt proporsjonalt.[86] Under henvisning til tidligere EU-domstolsavgjørelser uttalte EU-domstolen i C-77/21 avsnitt 49 at prinsippene i GDPR kapittel II og III må overholdes ved enhver behandling av personopplysninger.[87] Ettersom de grunnleggende GDPR-prinsippene i artikkel 5 bygger på retten til privatliv og

[85] Rui mfl. (2021), side 184.
[86] Se bl.a. *S. og Marper mot UK* (2008), avsnitt 118 flg.
[87] *Nemzeti Adatvédelmi és Információszabadság Hatóság,* C-77/21.

personopplysningsvern, tjener prinsippene som skranker for forholdsmessighetsvurderingen. Overholdelse av GDPR-prinsippene i artikkel 5 utgjør dermed en forutsetning for at behandlingen anses forholdsmessig. Dersom behandlingen av personopplysninger strider med grunnprinsippene i artikkel 5 vil inngrepet mangle legitimitet.

Ettersom hvitvaskingslovens forpliktelser kan gi hjemmel for behandlingsgrunnlag og regelverkene bygger på ulike formål og hensyn som nødvendigvis ikke alltid er forenelige, oppstår problemstillingen om balansering av hensynene gjennomgående ved etterlevelsen av hvitvaskingsregelverkets forpliktelser. I *kapittel 4* tar jeg for meg et utvalg av de mest praktiske tilfellene der spørsmålene om spenningsforhold er mest relevante.

4.2 Hvitvaskingsloven § 17 om forsterkede kundetiltak

4.2.1 Høyrisikokunder

Etter hvitvaskingsloven § 17 (1) plikter rapporteringspliktige å «gjennomføre forsterkede kundetiltak» der det er «høy risiko for hvitvasking». Tiltakene skal iverksettes der det er «høy risiko», og bestemmelsen er dermed et utslag av risikoprinsippet etter § 6.[88] Finanstilsynet anbefaler i veiledningen til hvitvaskingsloven at risikovurderingen bør inneholde en vurdering av iboende risiko, kvaliteten av foretakets tiltak samt restrisiko.[89] Bestemmelsens formål er at rapporteringspliktige skal bruke mer tid og ressurser på kunder som utgjør høy risiko for hvitvasking.[90]

Gjennomføringen av forsterkede kundetiltak innebærer at rapporteringspliktige skal «iverksette ytterligere nødvendige tiltak», jf. (2). Ordlyden «ytterligere» kundetiltak refererer til de alminnelige kundetiltakene i lovens §§ 12 til 15, men er taus om hvilke øvrige tiltak som skal iverksettes. Hvitvaskingsforskriften § 4-9 gir en ikke-uttømmende liste over hvilke momenter som kan indikere høy risiko for hvitvasking, men inneholder ingen liste over hvilke tiltak som skal eller bør iverksettes der risikoen er høy. Hvitvaskingslovens forarbeider tar heller ikke stilling til tiltaksspørsmålet. Ifølge Finanstilsynets veileder må hvilke kundetiltak som skal iverksettes, «vurderes ut fra den konkrete risikoen».[91] Bakgrunnen for at kunden er underlagt forsterkede tiltak «er følgelig førende for *hvilke* forsterkede tiltak som forventes», og «tiltakende må derfor være tilpasset de konkrete risikoene som identifiseres».[92] Veiledningen

[88] Rui mfl. (2021), side 258.
[89] Finanstilsynet (2022), side 11.
[90] Rui mfl. (2021), side 258.
[91] Finanstilsynet (2022), side 55.
[92] Ibid.

nevner informasjon om kunden, herunder yrke og formuesforhold, samt årsaken til planlagte eller gjennomførte transaksjoner.[93]

Hvitvaskingsloven sammenholdt med veiledningen krever dermed at rapporteringspliktige innhenter flere personopplysninger enn ved alminnelige kundetiltak. De anbefalte tiltakene etter veiledningen vil ofte inkludere opplysninger om kundens økonomiske situasjon, skatteopplysninger og reisedokumentasjon. Prinsippene om dataminimering og formålsbegrensning legger tydelig bånd på at banken kun kan innhente informasjon som er strengt nødvendig for å oppnå formålet om hvitvaskingsbekjempelse. Det er kritikkverdig at Finanstilsynets veiledning er taus om forholdet mellom forsterkede kundetiltak og GDPR, ettersom tiltakene indirekte oppfordrer til omfattende behandling av personvernopplysninger.

For å illustrere kan det tenkes en situasjon der en privatkunde med et langvarig kundeforhold i banken plutselig begynner med store kontantinnskudd, opp til 150.000,- NOK i måneden. Banken ser ingen åpenbar forklaring på bankinnskuddene for de tre til fire siste månedene, og iverksetter forsterkede kundetiltak i medhold av § 17. Gjennom lagrede kontoutskrifter i bankens database, offentlige databaser og spørsmål til kunden, innhenter banken omfattende detaljer om kundens private økonomi, herunder alle former for inntekter (eksempelvis fra arbeid, gaver og arv), skatteopplysninger samt tidligere økonomisk aktivitet (som mindre private lån). Dokumentasjon som forklarer kilden til kontantinnskuddene, eksempelvis i form av salgsavtaler for eiendom eller arbeidsavtaler med arbeidsgiver, kan anses som nødvendig for å avdekke hvitvasking. Opplysninger om at kunden har tatt opp et uformelt privat lån av sin onkel for å finansiere kjøp av boligoppussing, vil imidlertid ha begrenset nytteverdi for å avdekke opphavet til kontantinnskuddene. Dataminimeringsprinsippet tilsier at slike personopplysninger ikke kan innhentes, slik at behandling av disse opplysningene vil være uforholdsmessig.

4.2.2 Politisk eksponerte personer og deres nære familiemedlemmer og kjente medarbeidere

Selv om risikovurderingen i utgangspunktet er overlatt til de rapporteringspliktige, har lovgiver i visse situasjoner konstatert at det alltid og uansett skal iverksettes forsterkede kundetiltak. Hvitvaskingsloven § 18 er et utslag av dette, og fastslår at det skal gjennomføres forsterkede kundetiltak overfor politisk eksponerte personer (PEP). Hvitvaskingsloven § 2 bokstav f

[93] Ibid.

definerer en PEP som en som «innehar eller har innehatt en stilling eller et verv som» nevnt i bokstav f punkt 1 til 8. Eksempelvis nevnes statsoverhode, styremedlemmer i sentralbanken og ambassadører.

I tillegg til kravet om forsterkede kundetiltak overfor PEP, skal rapporteringspliktige iverksette forsterkede tiltak overfor nære familiemedlemmer og kjente medarbeidere til PEP.[94] Legaldefinisjonen av nære familiemedlemmer og kjente medarbeidere følger av hvitvaskingsloven § 2 g og h. For å ha grunnlag for forsterkede kundetiltak overfor nære familiemedlemmer, krever hvitvaskingsloven § 12 (4) at rapporteringspliktige har «systemer for å avgjøre om kunde, personer som handle på vegne av kunden eller er gitt disposisjonsrett [...] er nært familiemedlem» av PEP. Bestemmelsen stiller et kartleggingskrav til hvorvidt personer med fullmakt eller disposisjonsrett utgjør nært familiemedlem eller kjent medarbeider av PEP. Kravet er en nasjonal regel som går vesentlig lenger enn det som følger av fjerde hvitvaskingsdirektiv, ettersom direktivet kun krever kartlegging av kunden og reelle rettighetshavere.[95] Fjerde hvitvaskingsdirektiv er et minimumsdirektiv, slik at EØS-statene kan vedta strengere regler enn hva direktivet krever.[96] Selv om direktivet er et minimumsdirektiv, bør medlemsstaten påvise et klart behov for innføringen av en strengere regel. I forarbeidene foreslo utvalget at loven skulle samsvare med fjerde hvitvaskingsdirektiv, slik at det kun skal kartlegges hvorvidt kunden eller reell rettighetshaver er PEP. Departementet endret utvalgets forslag, men ga ingen begrunnelse for endringen.[97] Når direktivavviket medfører en betydelig utvidelse av personkretsen som får sine personopplysninger behandlet, er det kritikkverdig at departementet foreslo den omfattende utvidelsen uten å begrunne endringen eller drøfte regelens forhold til personopplysningsvernet. Dessuten medfører kartleggingsplikten et betydelig merarbeid for norske rapporteringspliktige, noe som vil kunne stride med risikoprinsippet.[98]

Som en del av «systemer for å avgjøre» om det eksisterer PEP-er i kundeforholdet, tilbyr private selskaper lister over PEP-er og deres familiemedlemmer.[99] Utvalget uttalte at det per desember 2016 ikke eksisterte noen offentlig PEP-lister.[100] Tilsvarende gjelder per desember 2024. Departementet bemerket at offentlige PEP-lister dessuten «ikke vil være tilstrekkelig til å

[94] Hvitvaskingsloven § 18.
[95] Rui mfl. (2021), side 223.
[96] HR-2024-761-A, avsnitt (33).
[97] Prop.40 L (2017-2018), side 77.
[98] Rui mfl. (2021), side 223-224.
[99] Ibid.
[100] NOU 2016:27, side 83.

oppfylle rapporteringspliktiges forpliktelser, fordi en norsk liste nødvendigvis ikke vil inneholde andre enn norske PEP-er».[101] Både lovforarbeidene og Finanstilsynets veiledning konstaterer at det ikke kreves at rapporteringspliktige benytter PEP-lister fra kommersielle aktører.[102] Dessuten har listene ofte begrenset troverdighet, da falske treff og negativ informasjon utgjør mer enn 50% av treffene i rapporteringspliktiges overvåkningssystemer.[103] Dersom ressurser settes til å avklare treffene, vil ressursbruken kunne bidra til ineffektiv hvitvaskingsbekjempelse, og dermed stride med risikoprinsippet.[104] Tross dette er det ikke uvanlig at rapporteringspliktige bruker slike lister, fordi listene til en viss grad kan gi opplysninger om PEP samt deres nære familiemedlemmer og kjente medarbeidere. Bakgrunnen skyldes trolig at konsekvensene av mangelfull kartlegging av en PEP eller manglende etterlevelse av hvitvaskingsloven for PEP-tilfeller, kan medføre alvorlige konsekvenser for banken. Eksempelvis resulterte manglende oppfølging av to namibiske PEP-er at DNB ble etterforsket av Økokrim for straffbare forhold.[105]

Samtidig som PEP-listene kan gi informasjon for å kartlegge PEP-er og deres nærstående, byr bruken på flere GDPR-utfordringer. Innsamlingen av informasjon om familiemedlemmer kan enkelt si noe om familiemedlemmets seksualitet, eksempelvis der en PEP-liste inneholder at en mannlig PEP er gift med en person med et typisk mannlig navn. Tilsvarende kan en PEP-liste inneholde informasjon om fødselsdatoen og nasjonaliteten til en PEP sitt barn, noe som vil kunne gi indikasjoner på barnets etnisitet. Et tredje eksempel er en PEP-liste inneholder informasjon om medlemskap i politiske partier eller deltakelse i politiske demonstrasjoner. Et siste eksempel er der en PEP-liste inneholder detaljer om et familiemedlems kriminalhistorikk, eksempelvis henlagte anklager om seksualforbrytelser. Både seksualitet, etnisitet og politisk orientering anses som spesielle kategorier av personopplysninger etter GDPR artikkel 9. Tilsvarende utgjør informasjon om straffbare forhold sensitive opplysninger etter GDPR artikkel 10. PEP-lister som stammer fra områder utenfor EU kan være akseptert etter annen nasjonal lovgivning, ved at lovgivningen stiller mildere eller ingen krav til behandling av personopplysninger. Bruken av slike utenforstående PEP-lister i Norge, vil imidlertid kunne stride med EUs regler om personopplysningsvern.

[101] Prop.40 L (2017-2018), side 77.
[102] Prop.40 L (2017-2018), side 77; Finanstilsynet (2022), side 62.
[103] Rui mfl. (2021), side 225.
[104] Ibid.
[105] NRK (2019).

Ifølge GDPR artikkel 9 (1) er behandling av slike sensitive personopplysninger forbudt. Behandling av slike sensitive personopplysninger krever sterkere beskyttelse, og er dermed underlagt strengere krav enn alminnelige personopplysninger. Artikkel 9 (2) bokstav g gir imidlertid unntaksadgang, der behandlingen er «nødvendig av hensyn til viktige allmenninteresser, på grunnlag av [nasjonal- eller unionsrett]». Hvorvidt behandlingen er «nødvendig» må sees i forhold til «målet som søkes oppnådd», jf. artikkel 9. I tillegg må behandlingen være forenelig med retten til personopplysningsvernet, og sikre tilstrekkelige tiltak for å verne den registrertes rettigheter og interesser. Når det er «nødvendig for å gjennomføre forpliktelsene i hvitvaskingsloven» kan rapporteringspliktige behandle sensitive personopplysninger etter GDPR artikkel 9, jf. hvitvaskingsforskriften § 6-1. Basert på unntaket i artikkel 9, er det imidlertid ikke tilstrekkelig å vurdere nødvendighetsvilkåret i hvitvaskingsforskriften. I tillegg må den rapporteringspliktige, som også utgjør behandlingsansvarlig, vurdere om kravene om forenelighet med personopplysningsvernet og sikkerhetstiltak etter GDPR artikkel 9 er innfridd. Rapporteringspliktige kan derfor ikke basere nødvendigheten av behandlingen utelukkende på antihvitvaskingsformål.

En annen tenkelig situasjon er der en av bankens kunder er medlem av riksrevisjonens styre, og dermed får PEP-status etter hvitvaskingsloven § 2.[106] Banken iverksetter forsterkede kundetiltak etter § 17 i det PEP-en og hennes ektemann søker om refinansiering av boliglånet. På bakgrunn av at kunden har PEP-status bestemmer banken seg for å samle inn informasjon om hele familien, herunder ektemannens utlegg og økonomiske forpliktelser til noe som viser seg å være psykiatrisk behandling av deres 13 år gamle datter. Banken ber ektemannen om legeerklæring som konstaterer datterens diagnose, medisinske historie og behandlingsplan. I tillegg ber banken om dokumentasjon på utgiftene, herunder kvitteringer og fakturaer for datterens medisiner og behandling på en selvstendig, privat psykiater.

Helseopplysninger utgjør sensitive personopplysninger etter GDPR artikkel 9, og behandling av opplysningene er dermed i utgangspunktet forbudt. For eksemplet med legeerklæring og utleggsdokumentasjon, er det klart at innsamling av detaljert informasjon om diagnose, medisinsk historie og behandlingsplan strider med GDPR artikkel 9. Behandlingen av helseopplysningene har ingen direkte relevans til den økonomiske aktiviteten som eventuelt kan indikere hvitvasking. Slike helseopplysninger vil ikke gi informasjon om kundens økonomiske adferd eller forklare uregelmessige transaksjoner. Manglende sammenheng

[106] Hvitvaskingsloven § 2 (1) bokstav f nr. 5.

mellom økonomisk aktivitet og helseopplysninger, vil følgelig bryte med GDPR's dataminimeringsprinsipp og formålsprinsipp. Førstnevnte prinsipp, fordi innsamlingen av helseopplysningene vil gå vesentlig lenger enn det som er strengt nødvendig for å avdekke hvitvasking. Det eksisterer langt mindre inngripende tiltak for å kartlegge kundens økonomiske forhold. Behandlingen bryter også med formålsprinsippet, ettersom kartlegging av datterens helse ikke er forenelig med å formålet om «sikre kunnskap om kunden» for å avdekke hvitvasking, jf. hvitvaskingsloven § 17 (2) sammenholdt § 1.

Når det gjelder kvitteringene og fakturaene for medisiner og behandling er spørsmålet mer usikkert. Selv om kvitteringene og fakturaene ikke eksplisitt inneholder detaljert informasjon om datterens helsetilstand, vil slike dokumenter kunne gi indikatorer på datterens helsetilstand. Ved tolkningen av GDPR artikkel 9 har EU-domstolen i flere avgjørelser fastslått at bestemmelsen må tolkes vidt.[107] I C-21/23 uttalte domstolen at bestemmelsen ikke kan tolkes på en slik måte at behandling av personopplysninger «that are liable indirectly to reveal sensitive information concerning a natural person» ikke omfattes av bestemmelsen.[108] En tolkning som utelukker indirekte opplysninger, vil uthule vernet etter GDPR artikkel 9. Ettersom kvitteringene og fakturaene kan inneholde navn på medikamenter eller navnet på en institusjon som kun behandler rusmiddelavhengige, vil opplysningene kunne kategoriseres som helseopplysninger. Ved innsamling av slike kvitteringer og fakturaer kan det stilles spørsmål ved hvorvidt kvitteringer og fakturaer for medisiner og behandling er strengt nødvendig for å avdekke hvitvasking. Med mindre det kan vises til en klar sammenheng mellom de innhentede dokumentene og vurderingen av hvitvaskingsrisikoen, er det lite som tilsier at behandling av slike personopplysninger er nødvendige. Tilsvarende vil innhenting tross manglende nødvendighet stride med prinsippet om dataminimering, fordi banken innhenter mer informasjon enn det som er strengt nødvendig. Det vil imidlertid kunne stille seg annerledes, dersom det avdekkes at ektemannen til PEP-en er involvert i større, ujevne transaksjoner og disse kobles til en privat behandlingsinstitusjon.

4.2.3 Grunnkravene i hvitvaskingsloven §§ 12 til 15

I tillegg til å iverksette ytterligere tiltak for høyrisikokunder, krever § 17 at rapporteringspliktige skal «oppfylle kravene til å innhente og bekrefte opplysninger» etter §§ 12 til 15. Der kunden er fysisk person skal rapporteringspliktige innhente og bekrefte kundens identitet ved

[107] *ND v. DR* [GC] C-21/23, avsnitt 81.
[108] *ND v. DR* [GC] C-21/23, avsnitt 82.

«personlig fremmøte ved gyldig legitimasjon», jf. § 12 (2). I henhold til hvitvaskingslovens veiledning er kravet om identitetsbekreftelse «ufravikelig».[109] Dersom identitetsbekreftelse skjer uten personlig oppmøte, skal det etter § 12 «fremlegges ytterligere dokumentasjon eller gjennomføres ytterligere tiltak». Hvitvaskingsforskriften § 4-3 definerer kravene til hva som utgjør gyldig legitimasjon. Hvitvaskingslovens veiledning nevner pass og førerkort som eksempler.[110]

Et scenario der personopplysningshensyn står i spenningsforhold til hvitvaskingsloven, er tilfeller der personer mangler gyldig legitimasjon etter hvitvaskingsforskriften, og samtidig har utfordringer med fysisk oppmøte hos banken. Typisk er det tale om eldre og/eller syke personer, som ikke er underlagt vergemål. For slike tilfeller åpner Finanstilsynet for et «særskilt unntak» med «strengt ansvar» hos rapporteringspliktige, ved at kunden kan fremlegge dokumentasjon på helsetilstand, annen dokumentasjon som underbygger kundens identitet, og dokumentasjon på kundens behov for kundeforholdet. For helsetilstandsdokumentasjonen uttaler Finanstilsynet at legeerklæring om at fremskaffelse av gyldig ID må konstateres å være «reelt umulig», slik at ubeleilighet ved fremskaffelse ikke er tilstrekkelig.[111]

Unntak fra forbudet om å behandle helseopplysninger etter GDPR artikkel 9 kan aksepteres på visse vilkår og vil i større grad anses forholdsmessig der det er høy risiko for hvitvasking. Innsamling av legeerklæring vil dermed i større grad kunne aksepteres der vedkommende utgjør høyrisikokunde. Utfordringen med hvitvaskingsloven § 12 er imidlertid at bestemmelsen gjelder uavhengig av risikoklassifiseringer. Spenningsforholdet mellom regelverkene byr særlig på utfordringer, der det er tale om lavrisikokunder. Innsamling av sensitive personopplysninger vil i slike tilfeller tvilsomt være strengt nødvendig for å avdekke hvitvasking. I kriminalitetsbildet er det lite som tilsier at eldre, syke mennesker er den bankkundegruppen som utgjør størst hvitvaskingsrisiko, heller tvert imot. Å innhente legeerklæringer som konstaterer helsetilstanden til en kunde som ikke utgjør høy risiko for hvitvasking, vil dermed i liten grad kunne anses forholdsmessig.

Unntaksregelen for legitimering krever omfattende dokumentasjon. Den overnevnte tilnærming kan fremstå meningsløs for rapporteringspliktige, og vil i ytterste konsekvens stride med risikoprinsippet. Å bruke tid og ressurser på å innhente omfattende dokumentasjon som kan

[109] Finanstilsynet (2022), side 28.
[110] Ibid.
[111] Finanstilsynet (2022), side 33.

bekrefte lavrisikokunders identitet, fremstår lite forenelig med risikoprinsippet. Konsekvensen blir at ressursene ikke plasseres der det er et reelt behov for å avdekke hvitvasking. Prioriteringen medfører at etterlevelsen av både GDPR og hvitvaskingsregelverket blir undergravet.

4.3 Hvitvaskingsloven § 25 om undersøkelsesplikten

Hvitvaskingsloven § 25 fastslår at dersom rapporteringspliktige «avdekker forhold som kan indikere» tilknytning til hvitvasking, «skal det foretas nærmere undersøkelser». Som navnet på bestemmelsen «undersøkelsesplikt» og ordlyden «skal» tilsier, er det tale om en plikt til å foreta undersøkelser. I likhet med lovens § 17 setter ordlyden ingen grenser for hvilke undersøkelser som kan eller skal gjøres, slik at ordlyden isolert sett tilsier at banken har fri adgang til innsamling, vurdering, bruk, og lagring av informasjon om kunden og kundeforholdet. Hvitvaskingsloven § 25 har imidlertid svært nær tilknytning til lovens kapittel 4 om kundetiltak og løpende oppfølging. Kapittelet begrenser seg til rapporteringspliktiges kunder og kundeforhold, slik at reelle hensyn og systemorienterte sammenhenger tilsier at tilsvarende begrensning gjelder for undersøkelsesplikten etter § 25. Praktiske hensyn og risikoprinsippet taler for det samme, ettersom en vid undersøkelsesplikt vil kreve omfattende tids- og ressursbruk. En for bred undersøkelsesplikt vil heller ikke fremstå rimelig overfor de rapporteringspliktige, og vil kunne virke ineffektivt etter lovens formål. Ved å stille svært omfattende krav til innsamling og vurdering av informasjon om bankens kunder og kundeforhold, vil kravene kunne gå på bekostning av risikoprinsippet.

Ordlyden «kan indikere» tilsier en lav terskel for når undersøkelsesplikten inntrer. Hvitvaskingsloven (2009) ble revidert fra mistankekrav til indikasjonskrav, fordi det norske systemet forutsetter at undersøkelsesplikten inntrer før plikten til å rapportere. Lovutvalget uttalte i denne sammenheng at det er «naturlig at terskelen for rapportering er noe høyere enn for [undersøkelsesplikten]», og at «fokuset for de rapporteringspliktige må være at avvik fra normal kundeadferd utløser undersøkelsesplikt».[112] Både ordlyden og lovforarbeidene tyder på at det skal svært lite til før banken er pliktig til å behandle opplysninger om kunden, herunder personopplysninger. I et GDPR-perspektiv tilsier den lave terskelen for undersøkelsesplikten at det bør utvises ekstra varsomhet ved behandlingen av personopplysninger. Når det er lav terskel for å behandle informasjon, må det stilles strengere krav til at informasjonen som innhentes er

[112] NOU 2016:27, side 113.

strengt nødvendig. Av hensyn til kundenes personopplysningsvern, bør ikke behandlingen av personopplysninger skje ukritisk, tross hvitvaskingslovens lave terskel.

Hva som utgjør innholdet av «nærmere undersøkelser» reiser spørsmål om bankens undersøkelsesplikt overfor tredjepersoner. Bestemmelsens (2) bokstav d tydeliggjør at undersøkelsesplikten i en viss grad også omfatter tredjepersoner, ettersom undersøkelsesplikten alltid inntrer når «en transaksjon [foretas] fra person i et land eller område som ikke har tilfredsstillende tiltak mot hvitvasking». I rettsteorien er det reist spørsmål ved om undersøkelsesplikten også inntrer der rapporteringspliktige avdekker forhold som kan indikere hvitvasking, men hvor tilknytningen mellom kunden og transaksjonen er svak eller fraværende.[113] Et eksempel er der banken får informasjon om at en tredjeperson, som bankkunden har et forretningsforhold med, muligens er mistenkt for korrupsjon i et datterselskap i utlandet. Skulle datterselskapet være lokalisert i Belgia og bankkunden ikke har noen forbindelse til datterselskapet, er det mindre nødvendig å undersøke forholdene. Motsetningsvis vil nødvendigheten av å undersøke nærmere være svært mye større, dersom datterselskapet er lokalisert i Dubai og bankkunden har bistått datterselskapet i et prosjekt.

I GDPR-sammenheng oppstår spørsmålet om innhenting av opplysninger for disse forholdene er «nødvendige». I relasjon til Belgia-eksempelet tilsier dataminimeringsprinsippet at informasjonsinnhenting ikke er nødvendig. Dette kan begrunnes i at bankkunden ikke har noen direkte kobling til forholdene og tredjepersonens situasjon. Fraværet av nødvendig behandling styrkes når det er tale om et datterselskap lokalisert i et «stabilt og trygt» EU-land. Det foreligger ingen rapporteringsplikt overfor tredjepersoner i medhold av hvitvaskingsloven, men rapporteringspliktige kan selvsagt rapportere forholdene til politiet, dersom de selv ønsker.[114] Manglende rapporteringsplikt for slike forhold tilsier at behandling av personopplysninger ikke er nødvendig. Samtidig gir bestemmelsen uttrykk for en lav terskel, og med god grunn. Når det allerede foreligger indikasjoner på hvitvasking, står man ett steg lenger inn i kjernen av formålet om å bekjempe hvitvasking. Har man først kommet til det punktet at det foreligger indikasjoner på hvitvasking, vil rapporteringspliktige være berettiget til å behandle personopplysninger. I tråd med risikoprinsippet bør det begrenses hvor mye som kan kreves av rapporteringspliktige,

[113] Rui mfl. (2021), side 302-303.
[114] Ibid.

ettersom iverksettelse av undersøkelser ved svak tilknytning vil være tid- og ressurskrevende for de rapporteringspliktige.[115]

Et annet praktisk eksempel er rapporteringspliktiges bruk av sanksjonslister. Hvitvaskingsloven § 38 og hvitvaskingsforskriften § 7-3 pålegger rapporteringspliktige å ha elektroniske overvåkningssystemer for «å identifisere personer som er underlagt sanksjoner».[116] Plikten gjelder overfor listeførte personer og foretak etter EUs og FNs sanksjonslister.[117] Dersom rapporteringspliktige får treff i sanksjonslistene, må rapporteringspliktige iverksette undersøkelser etter hvitvaskingsloven § 25. At plikten utløses ved treff, skyldes at slike lister kan gi indikasjon på hvitvasking. Bruken av sanksjonslister fra andre land og institusjoner forekommer ofte, spesielt amerikanske lister. Utfordringen med lister utenfor EU og EØS, er at slike lister kan inneholde personopplysninger i større omfang enn det GDPR-reglene og tilhørende særlovgivning åpner for. Eksempelvis kan listene inneholde informasjon om at vedkommende er dømt for seksual- eller voldsforbrytelser. Opplysninger om «straffedom» er underlagt spesiell beskyttelse etter GDPR artikkel 10, og forutsetter at behandling av opplysningene har hjemmel i forskrift.[118] Ettersom EUs og FNs sanksjonslister er inntatt i sanksjonsloven med tilhørende forskrifter, har behandling av personopplysninger fra disse listene tilstrekkelig hjemmelsgrunnlag. I tillegg presiserer hvitvaskingsforskriften § 6-1 at personopplysninger som nevnt i GDPR artikkel 10 kan behandles, dersom dette er «nødvendig for å gjennomføre forpliktelsene i hvitvaskingsloven med forskrift». Plikten til å screene kundemassen og transaksjoner mot EUs og FNs lister følger av hvitvaskingsforskriften § 7-3, og er presisert i Finanstilsynets veileder punkt 8.1. Behandling av personopplysninger hentet fra sanksjonslister av EU, FN og Norge har dermed tilstrekkelig hjemmel. Hjemmelsspørsmålet stiller seg imidlertid annerledes, dersom en amerikansk eller annen tredjelands sanksjonsliste eksempelvis inneholder informasjon om en person som er dømt for voldsutøvelse. For hvitvaskingsregelverket følger det ingen plikt til å screene mot øvrige sanksjonslister, og ettersom slike lister ikke er inkludert i sanksjonsloven eller tilhørende bestemmelser, er det usikkert hvorvidt behandlingen av personopplysninger i denne sammenheng har tilstrekkelig hjemmel. Hvis dette ikke er tilfellet, vil bruken av slike lister stride med prinsippet om lovlighet etter GDPR artikkel 5 (1) bokstav a.

[115] Ibid.
[116] Finanstilsynet (2022), side 96.
[117] Finanstilsynet (2022), side 98.
[118] Personopplysningsloven § 7 smh. § 9.

I rettsteorien er det trukket fram at hjemmelsspørsmålet skaper en særlig utfordring for norske rapporteringspliktige.[119] Utfordringene innebærer at mange rapporteringspliktige, spesielt banker, er avhengig av å etterleve amerikanske sanksjonslister for å kunne handle i amerikanske dollar og med amerikanske aktører. Forbud mot bruk av sanksjonslister på grunn av GDPR medfører dermed inngripende konsekvenser for bankene.[120] Når GDPR tar sikte på å beskytte en rettferdig og forholdsmessig behandling av personopplysninger, er det liten grunn til å tro at regelverket var ment å legge bånd på norsk næringslivs mulighet til å handle med internasjonale aktører. En slik forståelse underbygges av at Datatilsynet ved flere anledninger har gitt midlertidige tillatelser for behandling av artikkel 10-opplysninger.[121]

Hvorvidt det skal foretas nærmere undersøkelser er opp til den rapporteringspliktige, basert på den risikovurderingen banken har foretatt av kunden. Det er bankene som må utforme maler for risikoklassifisering og foreta risikovurderinger av egne kunder. Myndighetene har i begrenset grad laget formelle, konkrete regler om hvordan klassifiseringen skal gjøres. Hvitvaskingsloven med forskrift gir ingen uttømmende liste, og Finanstilsynets veiledning sier lite konkret om klassifiseringene. Dette medfører at bankenes risikovurderinger og -klassifiseringer har en tendens til å utformes i et subjektiv format, fremfor at risikovurderingene baseres på objektive kriterier gitt eller veiledet fra myndighetene. Resultatet gjør at en kunde kan flagges som høyrisikokunde hos bank A, og som middelsrisikokunde hos bank B. Manglende felleskriterier medfører en risiko for at enkelte banker kan ta i bruk for eksempel etnisk profilering, noe som strider med både GDPR og likestillings- og diskrimineringsloven. Selv om etnisk profilering ikke er et kjent problem i Norge, er det likevel utbredt at personer har underbevisste forventninger og antagelser til mennesker som er annerledes enn seg selv, uavhengig av om det gjelder etnisitet, kjønn, religion, seksualitet eller politikk. Manglende felleskriterier for etterlevelse av hvitvaskingsregelverket åpner for at personer med annen bakgrunn kan få brukt sine personopplysninger mot seg. I tillegg har Det europeiske datatilsynet (EDPS) uttalt at behandling av personopplysninger knyttet til seksualitet og etnisitet bør være forbudt ved behandling med formål om hvitvaskingsbekjempelse.[122]

[119] Clausen og Munte-Kaas (2020).
[120] Ibid.
[121] Ibid.
[122] EDPS Opinion 12/2021, punkt 16.

4.4 Hvitvaskingsloven § 26 om rapporteringsplikten

Dersom det avdekkes «forhold som gir grunnlag for mistanke om hvitvasking [...] skal rapporteringspliktige oversende opplysninger til Økokrim om forholdene», jf. hvitvaskingsloven § 26 (1) første punktum. Bestemmelsen gir uttrykk for at rapporteringspliktige skal sende MT-rapport ved «mistanke» om hvitvasking. Rapporteringspliktige skal også «oversende andre nødvendige opplysninger» etter forespørsel fra Økokrim, jf. andre punktum. Oversendelse etter forespørsel gjelder uavhengig av om den rapporteringspliktige allerede har sendt MT-rapport til Økokrim.[123] Forarbeidene gir anvisning til at rapporteringsplikten har en lav terskel, uten at magefølelse eller vage holdepunkter er tilstrekkelig.[124] Det er «opplysninger [...] om forholdene» som skal oversendes fra banken til Økokrim, og det må dermed skilles mellom opplysninger av generell karakter og personopplysninger. Generelle opplysninger omfattes ikke av GDPR-regelverket, og kan oversendes til Økokrim uten nærmere ettertanke. Ordlyden «opplysninger [...] om forholdene» angir en begrensning av hvilke opplysninger, herunder personopplysninger, som kan oversendes. At den oversendte informasjonen må gjelde «forholdene», henviser til «forhold som gir grunnlag for mistanke om hvitvasking». Etter bestemmelsens ordlyd har rapporteringspliktige som utgangspunkt kun lovhjemmel til å oversende personopplysninger som inngår i de «forhold som gir grunnlag for mistanke om hvitvasking». I tråd med dataminimeringsprinsippet har rapporteringspliktige kun adgang til å oversende informasjon om forhold som gir mistankegrunnlag. Dersom banken oversender kundens transaksjonshistorikk for de siste fem årene, selv om det kun er transaksjoner fra de siste åtte månedene som har gitt grunnlag for mistanke om hvitvasking, vil oversendelsen kunne stride med dataminimeringsprinsippet.

I lys av at personopplysninger om eksempelvis religion utgjør sensitive personopplysninger etter GDPR artikkel 9 (1), kan det reises spørsmål ved den lave terskelen for rapportering til Økokrim. Dersom rapportering skjer basert på svak eller generell mistanke om at visse trossamfunn eller institusjoner er «mistenkelige», uten konkrete holdepunkter, vil rapporteringen utfordre forholdsmessighetskravet. Dette innebærer at behandling av sensitive opplysninger som navn og religionstilknytning uten tilstrekkelig holdepunkter vil stride med dataminimeringsprinsippet. En lav terskel og et forventningspress om streng etterlevelse av

[123] Hvitvaskingsloven § 26 (1) andre punktum.
[124] Prop.40 L (2017-2018), side 102.

hvitvaskingsloven, kan resultere i en praksis med overrapportering uten at forholdene nødvendigvis utgjør reelle grunnlag for mistanke.

I forlengelsen av eksempelet med bruk av sanksjonslister og PEP-lister ved etterlevelsen av hvitvaskingslovens §§ 17 og 25, vil den negative informasjonen som listene inneholder også kunne utgjøre brudd på GDPR ved etterlevelsen av rapporteringsplikten. Oversendelse basert på utdaterte lister medfører at personopplysningene som lagres hos Økokrim er uriktige. En slik praktisering vil stride med GDPRs prinsipper om rettferdighet og riktighet.[125]

Økokrims tilgang på opplysninger om mistenkelige forhold består av en passiv og aktiv tilgang. For Økokrims passive tilgang kan det stilles spørsmål ved om det overrapporteres, fordi bankene er redde for overtredelsesgebyrer fra Finanstilsynet. Praksis der en etterlever hvitvaskingsloven «ekstra godt» vil ikke stå i forenlighet med kravet til forholdsmessighet etter GDPR, ettersom behandlingen av personopplysninger ikke er strengt nødvendig. Tilsvarende problematikk gjelder i en viss utstrekning for Økokrims aktive tilgang på opplysninger. Forarbeidene fastslår uttrykkelig at «mistenkelig» ikke bare kan baseres på mageføelse eller antakelser. EDPS har likevel gitt uttrykk for en bekymring om at «mistenkelige forhold»-kravet åpner for en praksis der innsamlingen og oversendelsen av data ikke utgjør en del av en målrettet etterforskning, men en taktikk som heller ligner på datagruvedrift.[126] Resultatet blir at myndighetene behandler personopplysninger i større omfang enn det som er strengt nødvendig, fordi dataene potensielt kan være nyttige i fremtiden. Myndighetene innhenter dermed data basert på relevans fremfor behov. En slik praksis vil stride med både dataminimeringsprinsippet og formålsprinsippet, fordi behandlingen av personopplysninger ikke er nødvendig for å avdekke hvitvasking.

4.5 Hvitvaskingsloven § 31 (3) om utveksling av opplysninger

Hvitvaskingsloven § 31 (3) har ingen tilsvarende artikkel i direktivet, og utgjør en særnorsk regel. Bestemmelsen fastslår at visse rapporteringspliktige «kan uten hinder av taushetsplikt utveksle nødvendige kundeopplysninger seg imellom når det anses nødvendig som ledd i nærmere undersøkelser etter § 25».[127] Bestemmelsen gir nærmere bestemte rapporteringspliktige adgang til å dele opplysninger seg imellom, deriblant banker, uten at delingen bryter med avsløringsforbudet i hvitvaskingsloven § 28. Informasjonsutvekslingen

[125] GDPR artikkel 6 bokstav a og d.
[126] EDPS Opinion 1/2017, punkt 52.
[127] Hvitvaskingsloven § 4 (1) bokstav a til c og j

skal begrenses til «nødvendige kundeopplysninger» når det anses «nødvendig som ledd i nærmere undersøkelser». Hva som anses nødvendig og tidspunktet for når delingen er nødvendig må vurderes konkret.[128] Finanstilsynets veiledning konstaterer at utveksling forutsetter at «undersøkelsene er pågående» og at den forespørrende må ha et «særskilt grunnlag for forespørselen i pågående undersøkelser».[129]

Videreføringen av den særnorske regelen var omdiskutert av lovutvalget grunnet risikoen for personverninngrepet slik deling kunne medføre. Lovutvalget uttalte at det kunne reises spørsmål ved om lovforslaget ga «tilstrekkelig hjemmel etter personopplysningsloven», ettersom fjerde hvitvaskingsdirektiv kun inneholdt én regel om utlevering av opplysninger fra rapporteringspliktige «innad i konsern».[130] Tross anbefalinger fra utvalget om å fjerne regelen om opplysningsutveksling, konstaterte departementet at det var «forsvarlig å videreføre adgangen».[131] Departementet begrunnet videreføringen med at det ikke var «grunnlag for å hevde at fjerde hvitvaskingsdirektiv [var] til hinder for denne type utveksling».[132] Når norsk regulering går lenger i adgangen til å behandle personopplysninger enn det som fremgår av hvitvaskingsdirektivet, er det kritikkverdig at departementet ikke tok stilling til lovutvalgets spørsmål. Det kan imidlertid ikke kreves at rapporteringspliktige frastår å benytte delingsadgangen for å oppnå direktivkonform fortolkning, når hvitvaskingsloven uttrykkelig åpner for slik opplysningsutveksling.[133]

I høringsrunden uttalte Finans Norge at «det ikke er gitt at det er et større personverninngrep at kundeopplysninger utveksles mellom rapporteringspliktige, enn at opplysningene utveksles med Økokrim».[134] Opplysningsdeling med Økokrim skjer på grunnlag av «mistanke» etter hvitvaskingsloven § 26, og kan medføre alvorlige konsekvenser for den rapporterte, i form av etterforskning eller tvangstiltak. Deling med Økokrim kan oppleves som mer inngripende enn deling mellom rapporteringspliktige, fordi delingen ikke skjer som ledd i forebygging, men potensiell straffeforfølgelse. Samtidig utgjør Økokrim en konkret institusjon, mens de nevnte rapporteringspliktige i § 4 utgjør et vesentlig bredere spekter av aktører. Spredningen av personopplysninger kan dermed foretas i mye større omfang ved deling mellom rapporteringspliktige enn med Økokrim, og gir i mindre grad forutberegnelighet for

[128] Finanstilsynet (2022), side 93.
[129] Ibid.
[130] NOU 2016:27, side 143.
[131] Prop.40 L (2017-2018), side 110.
[132] Ibid.
[133] Rui mfl. (2021), side 371-372.
[134] Prop.40 L (2017-2018), side 110.

bankkunden av hensyn til hvem som har tilgang på personopplysningene. Det er kritikkverdig at departementet ikke har vurdert dette aspektet.

Samtidig vil en svært liberal delingsadgang potensielt resultere i masseovervåkning over bankkunder. Av hensyn til prinsippene om formålsbegrensning og dataminimering, er det dermed avgjørende hvorvidt utvekslingen av opplysninger er forholdsmessige. Dersom en bank utveksler informasjon om enhver kunde som utgjør middels eller høy hvitvaskingsrisiko, uavhengig av hvor sterk indikasjonene på hvitvasking er, vil delingen åpenbart være uforholdsmessig og stride med GDPR.

Deling av informasjon kan dessuten utfordre riktighetsprinsippet. I likhet med rapporteringsplikten kan deling av personopplysninger basert på PEP-lister eller sanksjonslister by på utfordringer knyttet til GDPR. Eksempelvis vil deling av informasjon basert på utdaterte lister medføre deling av uriktige personopplysninger. Delingen vil i slike tilfeller stride med riktighetsprinsippet.[135] Manglende oppdateringer av informasjon eller bruk av utdatert opplysninger kan medføre at banker deler antagelser basert på feilaktig informasjon, og dermed deler opplysninger om forhold som ikke utgjør betydelig hvitvaskingsrisiko. Dersom en bank deler feilaktige opplysninger om en bankkunde med en annen rapporteringspliktig, kan delingen medføre alvorlige konsekvenser for den registrerte. EDPB har i denne sammenheng påpekt at slik datadeling kan forverre praksisen med «de-risking», en praksis der banker velger å avslutte eller begrense forretningsforbindelser med høyrisikokunder.[136] Resultatet blir at delingsadgangen mellom banker øker risikoen for uberettiget ekskludering fra banktjenester. Ekskluderingen kan medføre alvorlige juridiske konsekvenser for den registrerte. Eksempelvis kan den registrerte få vanskeligheter med å åpne eller få tilgang til egne konti, benytte betalingsmidler, få kreditt eller nektes tilgang til andre finansielle tjenester.

Dersom en rapporteringspliktig deler kundedata med en annen rapporteringspliktig og mottakeren videreformidler informasjonen til tredjepart(er) uten samtykke eller hjemmel i lov, vil behandlingen stride med GDPR. Eksempelvis, hvis en rapporteringspliktig som mottar data om en mistenkelig kunde, videreformidler denne informasjonen til en tredjepart som ikke er rapporteringspliktig uten et gyldig formål, er dette et klart brudd på GDPR. Det er likevel usikkert hvor problematisk eksemplet er i praksis, ettersom rapporteringspliktige er underlagt et strengt avsløringsforbud etter hvitvaskingsloven § 28. Det er rimelig å anta at

[135] GDPR artikkel 5 (1) bokstav d.
[136] EDPB Letter (2023), side 3.

rapporteringspliktige i en banks hvitvaskingsavdeling ikke deler informasjon om kundene, fordi brudd på avsløringsforbudet kan medføre alvorlige konsekvenser for både banken og bankens ansatte. Banken kan ilegges overtredelsesgebyr etter hvitvaskingsloven § 49, mens ansatte kan straffesanksjoneres etter § 51. Selv om delingsadgangen antageligvis ikke er problematisk i praksis, er det likevel bemerkelsesverdig at lovbestemmelsen strider med GDPR og samtidig åpner for brudd på GDPR.

EU-Rådet foreslo en tilsvarende bestemmelse i EUs hvitvaskingsregelverk, som det som følger av hvitvaskingsloven § 31 (3). EDPB stilte seg svært kritisk til forslaget, og uttalte at de foreslåtte reguleringene ikke var forholdsmessige i forhold til de målene som etterstrebes.[137] Tilsynet argumenterte for at en omfattende delingsadgang mellom rapporteringspliktige ville medføre en svært omfattende databehandling, som ville resultere i masseovervåking av private aktører.[138] Bekjempelse av kriminalitet i all hovedsak er en offentlig oppgave. Av hensyn til personopplysningers sensitive natur og konsekvensene for involverte individer, bør private aktørers bidrag til kriminalitetsbekjempelse være strengt begrenset samt grundig begrunnet.

Selv om informasjonsdeling utvilsomt er en essensiell del av antihvitvaskingsarbeidet, er det grunn til å revurdere den norske særregelen, særlig sett i lys av EUs AML-pakke. Den nye hvitvaskingsforordningen fortalepunkt 146 til 152 oppfordrer til informasjonsdeling mellom kompetente myndigheter og rapporteringspliktige, under forutsetning om ivaretakelse av retten til personopplysningsvern. Samtidig fastslår forordningens artikkel 75 at medlemmer av partnerskap for informasjonsdeling kan utveksle opplysninger, der det er strengt nødvendig for å overholde forpliktelsene om kundetiltak etter forordningens kapittel III.[139] Informasjonsdelingen må samsvare med grunnleggende rettigheter, og partnerskapets medlemmer må verifisere at partnerskapet har mekanismer som sikrer gjennomføring av DPIA.[140] Artikkelen inneholder ytterligere flere krav for ivaretakelse av retten til personopplysningsvern, og vil trolig gi grunnlag for en mer avbalansert delingsregel enn dagens bestemmelse.

Hverken sjette hvitvaskingsdirektiv eller hvitvaskingsforordningen i «AML-pakken» gir uttrykkelige regler om frivillig informasjonsdeling mellom kriminalitetsbekjempende myndigheter, tilsynsmyndigheter og kredittinstitusjoner. En slik regel er imidlertid allerede

[137] Ibid.
[138] Ibid.
[139] Forordning 2024/1624 (Hvitvaskingsforordningen) artikkel 75 (1).
[140] Hvitvaskingsforordningen, artikkel 75 (1) og (2).

inntatt i den svenske penningtvättslagen.[141] Samarbeidsadgangen er begrenset til å gjelde alvorlig hvitvasking, til ikke å gå lenger enn det som er nødvendig av hensyn til hvitvaskingsbekjempelse og til at det tiltenkte resultatet ved informasjonsdelingen står i et rimelig forhold til de ulemper som kan antas å oppstå for berørte enkeltindivider.[142] Informasjonsdeling forutsetter følgelig at samarbeidspartene gjennomfører konkrete forholdsmessighetsvurderinger før informasjonen kan deles. Løsningen synes å tilrettelegge for bedre vurderingsgrunnlag for rapporteringspliktige, og kan tjene som inspirasjon for en norsk regel. I lys av den overnevnte diskusjonen og en etterspurt utredning til EU, krever problematikken rundt strategisk, frivillig informasjonsdeling at lovgiver vurderer hvordan den nye forordningen skal implementeres i norsk lovgivning.[143]

4.6 Begrensninger i innsynsretten

En sentral side av personopplysningsvernet er innsynsretten i GDPR artikkel 15. Etter bestemmelsen har den registrerte rett til innsyn i forhold knyttet til behandlingen av personopplysninger, slik som formålet med behandlingen og berørte kategorier av personopplysninger.[144] Bestemmelsens formål er at «den registrerte skal kunne skaffe seg relevant informasjon om behandlingen, og verifisere at den skjer i overensstemmelse med [forordningens krav]».[145] Som en del av innsynsretten, har den registrerte krav på informasjon om retten til å kreve uriktige eller overflødige opplysninger korrigert eller slettet.[146] Innsynsretten bygger dermed i stor grad på prinsippet om lovlighet, rettferdighet og åpenhet samt riktighetsprinsippet. Som utgangspunkt har bankkunder krav på innsyn i de behandlingsprosessene som banken foretar, når banken behandler kundens personopplysninger.

Imidlertid kan innsynsretten begrenses på visse vilkår etter GDPR artikkel 23. Slik begrensning fremgår av hvitvaskingsloven § 32 (1) som fastslår at «rapporteringspliktige ikke skal gi innsyn» i opplysninger omfattet av undersøkelsesplikten og rapporteringsplikten, eller «andre opplysninger som kan vanskeliggjøre overholdelse av denne loven, etterforskning eller lignende undersøkelser». Begrensningen er essensiell for lovformålet om å produsere

[141] Penningtvättslagen, 4a kap 1 §.
[142] Penningtvättslagen 4a kap 2 §.
[143] Vogel mfl. (2024), side 36.
[144] GDPR artikkel 15 (1) bokstav a og b.
[145] Skullerud mfl. (2018), side 137.
[146] GDPR artikkel 15 (1) bokstav e.

etterretningsinformasjon, ettersom omfattende innsynsrett kan skade etterforskningen eller føre til omgåelse av hvitvaskingsregelverket.

Utformingen av risikoklassifiseringer og gjennomføringen av risikovurderinger er hovedsakelig overlatt til bankene.[147] En slik løsning kan by på utfordringer knyttet til prinsippene om åpenhet og riktighet. Manglende åpenhet utgjør en usikkerhet for kundene, ved at kunden ikke kan være sikker på hvilken form for opptreden som vil anses mistenkelig. Kundene vil heller ikke få vite hvilke omstendigheter som medfører at personopplysningene deres blir overført til Økokrim, skattemyndighetene eller andre kompetente myndigheter. EU-domstolen har uttalt at innsynsretten etter GDPR artikkel 15 (1) bokstav c krever at utøvelsen av rettigheten må gjøres på en slik måte at det mulig for den registrerte å etterprøve hvorvidt vedkommendes personopplysninger er korrekte og behandles lovlig.[148] Manglende åpenhet overfor kunder, knyttet til risikovurderinger og risikoklassifisering, kan anses problematisk med tanke på GDPRs krav til åpenhet. Grunnet avsløringsforbudet har dessuten Datatilsynet begrenset mulighet til å etterprøve bankenes vurderinger.[149] Selv om fraværet av felleskriterier i liten grad er forenelig med åpenhetsprinsippet, vil klare felleskriterier bidra til at kundetiltak i mindre grad baseres på risikovurderinger av de rapporteringspliktige. Imidlertid utgjør manglende åpenhet kjernen av avsløringsforbudet, ettersom hensynet til effektiv bekjempelse og etterforskning av hvitvasking krever at kunden ikke er klar over at vedkommende mistenkes. Den lave terskelen for å nekte innsyn i straffesaker,[150] tilsier ytterligere at GDPR ikke kan legge særlig strenge føringer for innsynsretten rundt behandlingen av personopplysninger som ledd i antihvitvaskingsarbeidet. Det ville blitt vesentlig enklere for hvitvaskere å omgå bankenes systemer, dersom myndighetene utgir offentlige, konkrete veiledninger for når bankene må iverksette tiltak og rapportere til Økokrim.

Ettersom hvitvaskingsloven § 32 om unntak fra innsynsretten også gjelder «andre opplysninger som kan vanskeliggjøre overholdelse av denne loven, etterforskning eller lignende undersøkelser», medfører begrensningen at hvitvaskingsloven gjennomgående står i et spenningsforhold til GDPR-prinsippene om åpenhet og riktighet.

[147] Se kapittel 4.3.
[148] C-154/21, *RW mot Österreichische Post AG,* avsnitt 37.
[149] Se kapittel 5.7.
[150] Straffeprosessloven § 242 (1).

5. Tiltak for harmonisering av dagens regelverk

5.1 Innledende

Som illustrert er det ikke mulig å fastsette en konkret grense for hvilke personopplysninger som alltid eller aldri kan innhentes ved etterlevelse av hvitvaskingsloven. Den manglende muligheten til å fastsette en absolutt grense er en naturlig følge av flere forhold. For det første, at de to regelverkene er risikobaserte og at ingen av reglene har eksplisitt forrang over det andre. De vage formuleringene av prinsippene for databehandling bidrar til en fleksibel anvendelse av GDPR samtidig som det vanskeliggjør fastsettelsen av en konkret grense for behandling. Når GDPR krever at behandlingsansvarlig foretar konkrete forholdsmessighetsvurderinger ved enhver behandling av personopplysninger, vil det være umulig å fastsette én bestemt grense. Alt håp om et harmonisert regelverk er imidlertid ikke tapt av denne grunn.

5.2 Kunnskap og ressursbruk

At de to regelverkene er både kompliserte og omfangsrike, forutsetter at rapporteringspliktige har god og inngående kunnskap om begge fagfelt. Med fagfolk som har forståelse for regelverkene, både isolert og i en kontekstuell sammenheng, vil det være enklere for rapporteringspliktige å forholde seg til lovreglene. For å unngå misforståelser og uriktig etterlevelse av regelverkene, vil inngående kunnskap om lovområdene være en viktig forutsetning. I lys av at regelverkene står i et spenningsforhold og at begge regelverkene forutsetter risikovurderinger og rutiner for å innfri lovkravene, tilsier rettskildene at rapporteringspliktige må ha økt kompetanse om GDPR. En viktig prioritering for bankene må dermed være å sikre at de ansatte med ansvar for antihvitvaskingsarbeidet har tilfredsstillende kunnskap om både hvitvaskingsregelverket og GDPR. Ytterligere vil tilstrekkelig ressursbruk være et viktig tiltak. Dagens hvitvaskingsregelverk krever at bankene er aktive i sitt arbeid, og når hvitvaskingsreglene krever inngående vurderinger av bankens kundemasse er det sentralt at banken har tilstrekkelig med ressurser for å håndtere kundemassen.

5.3 Interne retningslinjer og rutiner

For å sikre etterlevelse av både hvitvaskingsregelverket og GDPR er det avgjørende at virksomheter har etablerte interne retningslinjer og gode rutiner for risikovurdering og håndtering av risikoer. Dette er essensielt for å harmonisere de to regelverkene, da begge krever grundige risikovurderinger, men på ulike områder.

Hvitvaskingsloven § 8 krever at rapporteringspliktige «skal ha oppdaterte rutiner» for å sikre at virksomheten oppfyller bestemmelsene i loven og tilhørende forskrift. Ettersom rettskildene krever overholdelse av GDPR ved etterlevelsen av hvitvaskingslovens forpliktelser, må rutinekravet i hvitvaskingsloven § 8 forstås som også å omfatte rutiner for GDPR. Departementet konkluderte tilsvarende i proposisjonen, og presiserte at bestemmelsen skal «dekke behandlingen av personopplysninger siden rutinene skal beskrive rapporteringspliktiges oppfyllelse av lovens forpliktelser».[151] Tross fravær av uttrykkelig krav om rutiner, forutsetter flere av bestemmelsene i GDPR at behandlingsansvarlig har utformet og innarbeidet rutiner for alle trinn i prosessen om behandlingen av personopplysninger.[152] I tråd med hvitvaskingsloven § 8 bør rapporteringspliktige innarbeide rutiner som gir anvisning på hvilke vurderinger som skal gjøres konkret opp mot GDPR ved behandling av personopplysninger for å etterleve hvitvaskingsregelverket.

Interne retningslinjer og rutiner bidrar til å skape struktur og forutsigbarhet for hvordan virksomheten skal håndtere risikoer ved hvitvasking og behandling av personopplysninger. Uten retningslinjer risikerer man inkonsistente tilnærminger som kan føre til brudd på regelverkene. Samtidig sikrer klare, dokumenterte prosedyrer for risikovurderinger at virksomhetens ansatte har en felles forståelse av hvordan risiko skal identifiseres, vurderes og håndteres. Dette gir en systematisk og enhetlig tilnærming, som reduserer sannsynligheten for at kritiske risikoer går ubemerket. Når det gjelder hvitvasking, må virksomheter ha rutiner for å identifisere og vurdere risikoer basert på faktorer som kundeprofiler, transaksjonsmønstre og geografiske områder. Dette krever grundige risikoklassifiseringer, slik at nødvendige tiltak kan iverksettes, som overvåking av mistenkelige transaksjoner og tilpasning av kundekontrolltiltak etter risikonivå. Samtidig krever GDPR-regelverket at personopplysningsvernet ivaretas gjennom for eksempel DPIA. Dette sikrer at virksomheter iverksetter beskyttelsestiltak for å minimere risiko, slik som anonymisering av data eller strenge tilgangskontroller.

I tillegg er god dokumentasjon avgjørende for begge regelverkene. Når risikovurderinger, risikoklassifiseringer og DPIA-er er godt dokumentert, kan virksomheten vise til at nødvendige vurderinger og tiltak er gjennomført i tråd med regelverkene. Dokumentasjon gir virksomheten mulighet til å gjennomgå og forbedre sine prosesser over tid, basert på endrede risikoforhold eller nye regulatoriske krav. Rutiner for regelmessig oppfølging og revisjon er også viktig for å

[151] Prop.40 L (2017-2018), side 56.
[152] GDPR artikkel 5, 24 og 30-34.

sikre at virksomhetens retningslinjer forblir relevante og effektive. Utdaterte rutiner kan svekke virksomhetens evne til en effektiv risikohåndtering, uavhengig av om det gjelder personopplysningsvern eller antihvitvasking. Ved å revidere risikovurderinger og DPIA-er kontinuerlig, kan virksomheten tilpasse tiltak etter behov og sikre tilstrekkelig etterlevelse av lovens krav.

5.4 Garantier for informasjonssikkerhet og forbrukerperspektivet

Ifølge EU-domstolen krever Charteret artikkel 8 effektiv beskyttelse mot risikoen for misbruk og enhver ulovlig tilgang til og bruk av data.[153] Regler som griper inn i artikkel 8 må dermed være tydelig formulert, spesifikt tilpasset den omfattende datamengden, ta hensyn til dataenes sensitive natur, samt beskytte mot risikoen for ulovlig tilgang.[154] Fortalene til både fjerde og sjette hvitvaskingsdirektiv erklærer at direktivene respekterer den grunnleggende retten til personopplysningsvern og anvender proporsjonalitetsprinsippet.[155] Direktivene inneholder også noen spesifikke garantier for databeskyttelse, for eksempel artikkel 41 i fjerde hvitvaskingsdirektiv om at behandling av personopplysninger bare kan behandles for å bekjempe hvitvasking og terrorfinansiering, og artikkel 48 (2) som krever at ansatte som arbeider for de kompetente myndighetene har høy profesjonell standard, også når det gjelder «standards of confidentiality and data protection».

Imidlertid inneholder hverken fjerde hvitvaskingsdirektiv eller hvitvaskingsloven eksplisitte garantier for informasjonssikkerhet eller rettigheter for de registrerte. EDPS uttalte i denne sammenheng at tilsynet var positive til direktivets gjentatte referanser til behovet for å respektere personvernreglene ved etterlevelsen av hvitvaskingsreglene. Tilsynet understreket imidlertid også en bekymring for at disse henvisningene ikke ble tilstrekkelig etterlevd i praksis.[156] Fraværet av etablerte rettigheter gir inntrykk av at tilnærmingen i hvitvaskingsdirektivene er å utforske mulige unntak fra personvernkravene, fremfor å positivt etablere rettighetene.[157] Innføring av lovpålagte garantier for informasjonssikkerhet kan bidra til at etterlevelsen i GDPR ikke kun skjer på papiret, men også i praksis.

I dagens samfunn er de fleste avhengig av å være bankkunde. All lønnsutbetaling går digitalt, det er vanskelig å ta ut penger med mindre man har bankkort, betaling av regninger skjer

[153] *Digital Rights Ireland* [GC] C-293/12 og C-594/12, avsnitt 66.
[154] Ibid.
[155] Fjerde hvitvaskingsdirektiv fortalepunkt 43; sjette hvitvaskingsdirektiv fortalepunkt 21.
[156] EDPS Opinion 1/2017, punkt 40-41.
[157] Artikkel 29-gruppen Opinion 14/2011, side 3-4.

digitalt, og kjøp av bolig eller formuesgoder av større verdi uten bankkonto er praktisk umulig. Dagens regelverk legger dermed opp til at kundene må akseptere «overvåkingen» eller ikke ha et bankforhold overhodet. Dette innebærer at alle som bruker banktjenester automatisk underlegges behandling av personopplysninger. Situasjonen skaper en maktubalanse mellom forbrukeren og banken som rapporteringspliktig, ettersom forbrukeren har ingen reell valgmulighet til å nekte behandling av personopplysninger. Forbrukeren står dermed i en sårbar posisjon, noe som forsterkes av bankenes plikt til å rapportere mistenkelige aktiviteter i henhold til hvitvaskingsregelverket. Harmoniseringstiltak bør derfor inkludere garantier for datasikkerhet, særlig når bankene håndterer sensitive personopplysninger. Dette kan innebære en lovbestemt plikt til implementering av strenge rutiner for behandling av særlige kategorier av personopplysninger, slik som helseinformasjon, politisk orientering eller etnisk bakgrunn, noe som allerede kreves etter GDPR. En slik harmonisering vil samtidig redusere den systemiske maktubalansen og styrke forbrukerens rettigheter.

5.5 Lovbestemt plikt til rutiner for antihvitvask og personvernbeskyttelse

Hvitvaskingsforskriften § 6-1 fastslår at rapporteringspliktige «må ha rutiner for behandling av personopplysninger» omfattet av GDPR artikkel 9 og 10. Ved utformingen av hvitvaskingsforskriften § 6-1 uttalte Datatilsynet at det burde vurderes «om den foreslåtte plikten til å ha en rutine for en slik behandling er tilstrekkelig tiltak for å sikre de registrertes rettigheter».[158] Tilsynet begrunnet behovet med at det i likhet med plikten til rutiner, risikohåndtering og kravene til hvitvaskingstiltak etter hvitvaskingsloven §§ 6 til 8, bør kunne stilles liknende krav til behandling av personopplysninger. Finanstilsynet uttalte at det var behov for en klar hjemmel for behandling av særlige kategorier, men anså det ikke hensiktsmessig å gi en avgrenset og uttømmende liste for hvilke kategorier av personopplysninger og når i kundeforholdet man kan behandle disse.[159] Etter Finanstilsynets vurdering ville det være «for byrdefullt for de rapporteringspliktige å utrede behovet i forkant av hver gang særlige kategorier innhentes og behandles».[160] Av hensyn til et effektivt regelverk bør det utvises forsiktighet med å være svært restriktiv ved etterlevelsen av GDPR.

[158] Høringssvar fra Datatilsynet (2020), side 4.
[159] Høringsnotat fra Finanstilsynet (2019), side 42.
[160] Ibid.

5.6 Begrensning av skjønnsvurderinger

Det nåværende hvitvaskingsregelverket innebærer at rapporteringspliktige er helt eller delvis overlatt til å foreta skjønnsvurderinger, et naturlig utslag av risikoprinsippet. En risikotilnærming gir stor fleksibilitet og åpner for at rapporteringspliktige kan prioritere ressurser der hvitvaskingsrisikoen er størst. Som illustrert bærer dagens hvitvaskingsregelverk et gjennomgående preg av å ikke ha hensyntatt eller være samkjørt med GDPR-reglene. Resultatet synes å skylde at hvitvaskingsloven åpner for stort skjønn hos de rapporteringspliktige, og de fravikende delene av hvitvaskingsloven fra hvitvaskingsdirektivet medfører risikoprinsippet ikke gjennomføres i sin helhet. Kombinasjonen av fravikende nasjonal rett og stort skjønnsmessig rom for rapporteringspliktige kan være problematisk, fordi det åpner for ulik praksis hos de ulike bankene. At bankene ikke nødvendigvis ligger på samme linje, kan bidra til «bank-shopping» blant hvitvaskerne samt utfordringer knyttet til utveksling av opplysninger etter hvitvaskingsloven § 31 (3). Når Finanstilsynet i tillegg håndhever regelverket svært strengt, risikerer man overrapportering. En bred skjønnsmessig lovgivning kan dermed resultere i en ineffektiv hvitvaskingsbekjempelse, som samtidig bryter med GDPRs forholdsmessighetsprinsipp.

En mulig løsning er å innføre retningslinjer eller standardiserte prosedyrer som begrenser rapporteringspliktiges skjønnsmessige vurderinger. På den måten kan man sikre en mer ensartet tilnærming blant de rapporteringspliktige samt redusere risikoen for unødvendig behandling av personopplysninger. En mer ensartet tilnærming vil også bidra til å motvirke «bank-shopping», der hvitvaskere aktivt utnytter banker som mangler gode antihvitvaskingsrutiner.

Samtidig må lovgiver og relevante tilsyn være oppmerksomme på at hvitvaskingsregelverket er risikobasert. For spesifikke regler kan virke ineffektivt for antihvitvaskingsarbeidet. Innenfor ethvert fagfelt der det foretas inngrep, vil skjønnsvurderinger i stor grad baseres på faktum. Ettersom den juridiske løsningen baseres på en konkret proporsjonalitetsvurdering i det konkrete tilfellet, kan ikke lovgiver legge for strenge føringer for hvordan problemstillingen skal løses i praksis. Regler og retningslinjer som begrenser og presiserer rapporteringspliktiges skjønnsvurderinger, må ta høyde for at hvitvaskingsloven og GDPR er risikobaserte regelverk som forutsetter proporsjonalitetsvurderinger.

5.7 Tilsyn og veiledning for antihvitvask og personvern

En stor utfordring med dagens regelverk er at bankene opplever å bli dratt mellom to regelverk, med to tilsyn på begge sider av kniveggen. Kombinasjonen av kompliserte regelverk og fravær av samkjørte veiledninger fra Datatilsynet og Finanstilsynet om forholdet mellom GDPR og hvitvaskingsloven, gjør det utfordrende for rapporteringspliktige å foreta veloverveide forholdsmessighetsvurderinger. Spenningsforholdet er i liten grad vurdert i hvitvaskingslovens forarbeider og Finanstilsynets veileder. En mulig løsning er tydeligere veiledning fra Finanstilsynet som aktivt bidrar til avklaring av GDPR-problematikk for rapporteringspliktige. Sjette hvitvaskingsdirektiv oppfordrer til en slik løsning, ettersom fortalen understreker viktigheten av at hvitvaskingslovens tilsynsmyndigheter er oppmerksomme på veiledninger og publikasjoner utstedt av databeskyttelsesmyndigheter.[161] Fortalen oppfordrer ytterligere til at informasjon fra databeskyttelsesmyndighetene inkluderes i kommunikasjonen til de rapporteringspliktige institusjonene.[162] Ved at Finanstilsynet tydeliggjør forholdet mellom regelverkene gjennom veiledning og tilsyn, vil rapporteringspliktige i større grad kunne foreta avbalanserte forholdsmessighetsvurderinger ved behandling av personopplysninger i antihvitvaskingsarbeidet.

Dagens hvitvaskingslov setter i stor grad grenser for Datatilsynets mulighet til å føre tilsyn med rapporteringspliktiges behandling av personopplysninger. Avsløringsforbudet i hvitvaskingsloven § 28 gjelder «tredjepersoner», med unntak overfor «rapporteringspliktiges tilsynsmyndighet etter hvitvaskingsregelverket». Ettersom Datatilsynet ikke fører tilsyn med hvitvaskingsloven, tilsier ordlyden at avsløringsforbudet også gjelder overfor Datatilsynet. Lovbestemmelsen synes å praktiseres strengt grunnet myndighetenes inngripende sanksjoneringsadgang. [163] Resultatet er Datatilsynet får svært begrenset innsyn i hvilke personopplysninger som er behandlet og nødvendigheten av behandlingen. Å praktisere avsløringsforbudet strengt overfor Datatilsynet ligger utenfor kjernen av forbudets formål, ettersom det overordnede hensynet er at kunden ikke skal varsles om at vedkommende er under overvåkning for hvitvasking.[164] Selv om det er essensielt å begrense antall personer som har tilgang til vurderingene som foretas, og direktivet og hvitvaskingslovens forarbeider forutsetter

[161] Sjette hvitvaskingsdirektiv fortalepunkt 87.
[162] Ibid.
[163] Konfidensielle samtaler med tre banker av varierende størrelse (06.09.2024, 22.10.2024, 23.10.2024); Konfidensiell samtale med Datatilsynet (03.10.2024).
[164] NOU 2016:27, side 226.

en streng praktisering, bør avsløringsforbudet tolkes innskrenkende overfor Datatilsynet.[165] Tolkningen vil være i tråd med fjerde og sjette hvitvaskingsdirektiv, ettersom fortalene konstaterer at nasjonale databeskyttelsesmyndigheter kun bør involveres der risikovurderingen «has an impact» på kundens personvern.[166] Ettersom direktivene uttrykkelig åpner for at databeskyttelsesmyndigheter kan involveres under visse omstendigheter, bør ikke tolkningen av avsløringsforbudet ukritisk gå på bekostning av kundens personvern. Selv om direktivet åpner for at rapporteringspliktiges avsløringsforbud ikke gjelder overfor Datatilsynet, oppstår spørsmålet om Datatilsynet «arver» bankens avsløringsforbud. Problemstillingen aktualiseres fordi klageren, som part i klagesaken, har innsynsrett etter forvaltningsloven § 18. Selv om forvaltningsloven § 19 (2) bokstav b åpner for skjønnsbaserte unntak, er løsningen usikker. For å tydeliggjøre Datatilsynets mulighet til å føre effektivt tilsyn med rapporteringspliktige, bør lovgiver vurdere et lovbestemt unntak for Datatilsynet. Eksempelvis kan unntakslisten i hvitvaskingsloven § 28 uttrykkelig inkludere Datatilsynet, eller det kan innføres en tilsvarende regel som i politiregisterloven § 59 (2) , jf. § 54 (3), der Datatilsynet etter begjæring kan nekte innsyn.

Et mer omfattende tiltak, men potensielt effektivt, er å etablere felles tilsyn bestående av en andel fra Datatilsynet og en andel fra Finanstilsynet. Et felles tilsyn vil kunne forbedre samarbeidet mellom Finanstilsynet og Datatilsynet samt sikre en mer enhetlig tilnærming til utfordringene som oppstår i grenseområdet mellom hvitvaskingsforebygging og informasjonsbeskyttelse. Løsningen vil gi rapporteringspliktige tydeligere veiledning, redusere dobbeltarbeid og styrke ressursutnyttelsen.

6. Avsluttende betraktninger

Hvitvasking og terrorfinansiering medfører betydelige negative konsekvenser for samfunnet, særlig for velferdsstaten. Bekjempelsen av slik kriminalitet er dermed en svært viktig prioritering. Samtidig utgjør personopplysningsvernet og informasjonssikkerhet essensielle mursteinbrikker i et fritt, tillitsfullt og demokratisk samfunn. En god balansegang mellom hensynene og regelverkene er dermed avgjørende for å sikre en demokratisk og fri velferdsstat.

[165] Fjerde hvitvaskingsdirektiv fortalepunkt 46; NOU 2016:27, side 226.
[166] Fjerde hvitvaskingsdirektiv fortalepunkt 24; Sjette hvitvaskingsdirektiv fortalepunkt 12.

Hvitvaskingsregelverket er svært vidt og delvis uklart formulert når det gjelder hvilken informasjon rapporteringspliktige kan innhente, en naturlig følge av at regelverket er risikobasert. Både lovens enkeltforpliktelser og regelverket som helhet medfører at rapporteringspliktige kan behandle et svært stort omfang av personopplysninger. Å behandle personopplysninger om hvitvaskere er essensielt for en effektiv bekjempelse av hvitvasking. Selv om hvitvasking er et alvorlig samfunnsproblem, må det være adgang til å kritisere den omfattende behandlingsadgangen som dagens hvitvaskingslov og -forskrift åpner for. Spesielt når regelverket tilsynelatende ikke fungerer slik man ønsket i praksis. I Stortingsmelding 15 (2023-2024) påpekes flere praktiske utfordringer, herunder stigende antall MT-rapporter, flere henleggelser, vedvarende lavt antall straffesaker samt lav kapasitet og manglende nødvendig spesialistkunnskap i politiet.[167]

Finanstilsynets sviende pisk har tilsynelatende bidratt til en praksis, der hvitvaskingsregelverket blir hardt prioritert i bankvesenet, ofte på bekostning av personvernet. En nevneverdig utfordring i denne sammenheng er «goldplating», et fenomen der rapporteringspliktige etterlever hvitvaskingsloven «ekstra godt». Resultatet av at rapporteringspliktige overoppfyller hvitvaskingsloven i frykt for Finanstilsynets sanksjoner, er at rapporteringspliktig går lenger enn det som nødvendig.[168] I GDPR-sammenheng innebærer dette at bankene behandler personopplysninger i større omfang enn det som er nødvendig. I lys av menneskerettighetene er det problematisk at dagens regelverk ikke produserer etterretningsinformasjon av verdi, samtidig som regelverket er sterkt inngripende i personvern- og privatlivretten. Når dagens regelverk fremstår ineffektiv i praksis, kan det reises spørsmål ved den frihet som den øvrige, og ellers største, delen av befolkningen må akseptere å få innskrenket. Hvor mye må den redelige borgeren akseptere å bli overvåket og få sine personopplysninger behandlet, når hvitvaskingsregelverket i begrenset grad fungerer i praksis?

Dagens utfordringer viser nødvendigheten av å revurdere regelverket for forholdet mellom regelverkene og hvordan offentlige myndigheter og rapporteringspliktige skal avveie hensynet til kriminalitetsbekjempelse mot. Tross EDPBs skepsis til økt informasjonsdeling, synes «AML-pakken» å inneholde konturer av at EU allerede har foretatt avveininger på enkelte områder. Som nevnt i *kapittel 4.5* oppfordrer forordningen til økt informasjonsdeling mellom offentlige myndigheter og finansinstitusjoner under forutsetning om ivaretakelse av GDPR

[167] Meld. St. 15 (2023-2024), side 27-28, 43 og 93.
[168] Rui mfl. (2021), side 234.

samt retten til personopplysningsvern og privatliv. I tillegg anbefaler hvitvaskingsdirektivet at medlemsstatene innsetter en Fundamental Rights Officer i Financial Intelligence Unit, for å fremme enkeltpersoners grunnleggende rettigheter.[169] «AML-pakken» vil utvilsomt kreve endringer i norsk lovgivning og trolig bidra til et mer veloverveid og oversiktlig regelverk for rapporteringspliktige.

[169] Sjette hvitvaskingsdirektiv fortalepunkt 65.

Referanseliste

Lover og forskrifter

Norge

1814	Lov 17. mai 1814 Kongerikets Norges Grunnlov (Grunnloven)
1967	Lov 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven)
1978	Lov 9. juni 1978 nr. 48 om personregistre m.m. (personregisterloven, opphevet)
1981	Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven)
1988	Lov 10. juni 1988 nr. 40 om finansieringsvirksomhet og finansinstitusjoner (finansieringsvirksomhetsloven, opphevet)
1992	Lov 27. november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det Europeiske økonomiske samarbeidsområde (EØS) mv. (EØS-loven)
2000	Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven (2000), opphevet)
2005	Lov 20. mai 2005 om straff (straffeloven)
2009	Lov 6. mars 2009 nr. 11 om tiltak mot hvitvasking og terrorfinansiering mv. (opphevet)
2009	Forskrift 13. mars 2009 nr. 302 om tiltak mot hvitvasking og terrorfinansiering mv. (opphevet)

2010	Lov 28. mai 2010 nr. 16 om behandling av personopplysninger i politiet og påtalemyndigheten (politiregisterloven)
2017	Lov 16. juni 2017 nr. 51 om likestilling og forbud mot diskriminering (likestillings- og diskrimineringsloven)
2018	Lov 1. juni 2018 nr. 23 om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsloven)
2018	Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven)
FOR-2018-09-14-1324	Forskrift om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsforskriften)

Utenlandske lover

2017 (Sverige)	Lag (2017:630) om åtgärder mot penningstvätt och finansiering av terrorism (penningtvättslagen)

Internasjonale konvensjoner, traktater og direktiver

Konvensjoner og traktater

Den europeiske menneskerettighets-konvensjonen	Konvensjonen om beskyttelse av menneskerettighetene og de grunnleggende friheter, Roma 4. november 1950, (Den europeiske menneskerettighetskonvensjonen)
FNs konvensjon om sivile og politiske rettigheter	FNs konvensjon 16. september 1966 om sivile og politiske rettigheter (FNs konvensjon om sivile og politiske rettigheter)
EØS-avtalen	Avtale om Det europeiske samarbeidsområdet med tilhørende protokoller, Oporto 2. mai 1992 (EØS- avtalen)

EUs Charter om grunnleggende rettigheter	Charter of Fundamental Rights of the European Union, 2012/C 326/02, 26. October 2012 (EUs Charter om grunnleggende rettigheter)
Traktaten om den Europeiske Unions virkemåte	Treaty on the Functioning of the European Union, Consolidated version 2016, EN 2016/C 202/01 (TFEU)

EU direktiver, forordninger, mv.

Direktiv 95/46/EF	Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (personopplysningsdirektivet)
Direktiv 2005/60/EF	Europaparlaments- og rådsdirektiv 2005/60/EF av 26. oktober 2005 om tiltak for å hindre at det finansielle systemet benyttes til hvitvasking og finansiering av terrorisme (tredje hvitvaskingsdirektiv)
Direktiv 2015/849	Europaparlaments- og rådsdirektiv 2015/849 av 20. mai 2015 om forebygging av bruk av det finansielle systemet med formål om hvitvasking eller terrorfinansiering mv. (fjerde hvitvaskingsdirektiv)
Forordning 2016/679	Europaparlaments- og rådsdirektiv (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (GDPR eller personvernforordningen)
Direktiv 2024/1640	Europaparlaments- og rådsdirektiv (EU) 2024/1640 av 31. mai 2024 om ordninger som medlemsstatene skal innføre for å hindre at finanssystemet brukes til hvitvasking av penger eller finansiering av terrorisme (sjette hvitvaskingsdirektiv)

Forordning 2024/1624	Europaparlaments- og rådsforordning (EU) 2024/1624 av 31. mai 2024 om tiltak for å hindre at finanssystemet brukes til hvitvasking av penger eller finansiering av terrorisme (hvitvaskingsforordning)

Forarbeider, offentlige dokumenter, rundskriv, retningslinjer, mv.

Norge

NOU 1974:22	NOU 1974:22 Persondata og personvern
NOU 1975:10	NOU 1975:10 Offentlige persondatasystem og personvern
NOU 1997:19	NOU 1997:19 Et bedre personvern – forslag til lov om behandling av personopplysninger
Innst.O.nr.51 (1999-2000)	Innst. O. nr. 51 (1999-2000) Innstilling fra justiskomiteen om lov om behandling av personopplysninger (personopplysningsloven)
Ot.prp.nr.72 (2002-2003)	Ot.prp.nr.72 (2002-2003) Lov om tiltak mot hvitvasking av utbytte fra straffbare handlinger mv. (hvitvaskingsloven)
Prop.40 L (2017–2018)	Prop.40 L (2017–2018) Lov om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsloven)
NOU 2015:12	NOU 2015: 12 Ny lovgivning om tiltak mot hvitvasking og terrorfinansiering Første delutredning
NOU 2016:27	NOU 2016: 27 Ny lovgivning om tiltak mot hvitvasking og terrorfinansiering II Andre delutredning
Prop.56 LS (2017-2018)	Prop.56 LS (2017-2018) Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til

	deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen
Høringsnotat fra Finanstilsynet (2019)	Høringsnotat (2019), *Høringsnotat – forslag til endringer i hvitvaskingsloven og hvitvaskingsforskriften*, [Høringsnotat], 1. november 2019, (hentet fra Regjeringen.no: https://www.regjeringen.no/contentassets/56fe59758a8f41979c0b2979e2835410/horingsnotat-hvitvaskingsforskrift-2019-master-v11-endelig-2194816.pdf)
Høringssvar fra Datatilsynet (2020)	Datatilsynet (2022), *Høring - Endringer i hvitvaskingsregelverket (lov og forskrift) – EUs femte hvitvaskingsdirektiv mv. – Finansdepartementet*, [Høringssvar], 20. mars 2020, (hentet fra Regjeringen.no: https://www.regjeringen.no/no/dokumenter/horing--endringer-i-hvitvaskingsregelverket-lov-og-forskrift--eus-femte-hvitvaskingsdirektiv-mv/id2683265/?uid=bdca72ad-585e-42d9-9ac5-b938eb241470)
Finanstilsynet (2022)	Finanstilsynet (2022), *Veiledning til Hvitvaskingsloven* (Nr. 4/2022), [Rundskriv] (hentet fra Finanstilsynets hjemmesider: https://www.finanstilsynet.no/4ac1a7/contentassets/7b1a60634567430796fc36ea9b1ae3ac/rundskriv-4-2022-veileder-til-hvitvaskingsloven.pdf)
Prop.74 LS (2023–2024)	Prop. 74 LS (2023–2024) Endringer i finansmarkedslovgivningen (samleproposisjon) og samtykke til godkjenning av fire beslutninger i EØS-komiteen om innlemmelse i EØS-avtalen av rettsakter på finansmarkedsområdet

Internasjonale veiledninger, rapporter, arbeidsdokumenter mv.

OECD Guidelines (1980)	OECD Publishing, *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Paris, 23. September 1980,(https://www.oecd-ilibrary.org/docserver/9789264196391-en.pdf?expires=1726733213&id=id&accname=ocid194730&checksum=20B46A8011CAA29AE847BCFF7FBF4E60, sist besøkt 19. september 2024)
Artikkel 29-gruppen Opinion 14/2011	Article 29 Data Protection Working Group, *Opinion on data protection issues related to the prevention of money laundering and terrorist financing*, Adopted on 13 June 2014, WP 186, (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp186_en.pdf, sist besøkt 25. september 2024)
Official Journal of the European Union, 2012/C 192/05	Official Journal of the European Union, 2012/C 192/05
EDPS Opinion 1/2017	European Data Protection Supervisor, Opinion 1/2017, EDPS Opinion on Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC (https://www.edps.europa.eu/sites/default/files/publication/17-02-02_opinion_aml_en.pdf, sist besøkt 16. oktober 2024).
Artikkel 29-gruppen (2017/2018)	Article 29 Data Protection Working Group, *Guidelines on transparency under regulation 2016/697*, Adopted on 29 November 2017, as last revised and adopted on 11 April 2018, WP 260, (https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_en.pdf, sist besøkt 19. september 2024)

EDPB Recommendations 02/2020	European Data Protection Board, *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, 10. november 2020, (https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf, sist besøkt 19. september)
EDPS Opinion 12/2021	European Data Protection Supervisor, Opinion 12/2021, EDPS Opinion on the anti-money laundering and countering the financing of terrorism (AML/CFT) package of legislative proposals, 22. september 2021, (https://www.edps.europa.eu/system/files/2021-09/21-09-22_edps-opinion-aml_en.pdf, sist besøkt 29. november 2024)
EDPB Letter (2023)	European Data Protection Board, *EDPB letter to the European Parliament, the Council and the European Comission on data sharing for AML/CFT purposes in light of the Council´s mandate for negotiations*, 28. mars 2023 (https://www.edpb.europa.eu/system/files/2023-04/edpb_letter_out2023-0015_aml_cft_ep_en.pdf, sist besøkt 4. september 2024)

Rettspraksis

Norge

Rt-1991-616

Rt-1996-1114

Rt-2006-466

Rt-2012-2039

Rt-2013-143

Rt-2014-976

Rt-2015-93

Rt-2015-833

HR-2016-831-U

HR-2021-966-A

HR-2024-761-A

EU-domstolen

Digital Rights Ireland [GC] C-293/12 og C-594/12	Dom av 8. april 2014 [GC], *Digital Rights Ireland,* C-293/12 og C-594/12, ECLI:EU:C:2014:238
Peter Nowak [C5] C-434/16	Dom av 20. april 2017 [C5], *Peter Nowak v. Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:994
Patrick Breyer [C5], C-582/14	Dom av 19. oktober 2016, *Patrick Breyer v. Bundesrepublik Deutsvhland*, C-582/14, ECLI:EU:C:2016:779
Nemzeti Adatvédelmi és Információszabadság Hatóság, [C5] C-77/21	Dom av 20. oktober 2022 [C5], *Nemzeti Adatvédelmi és Információszabadság Hatóság,* C-77/21, ECLI:EU:C:2022:805
Luxembourg Business Registers [GC] C-37/20 og C-601/20	Dom av 22. november 2022 [GC], *Luxembourg Business Registers*, C-37/20 og C-601/20, ECLI:EU:C:2022:912
Österreichische Post AG [C5] C-154/21	Dom av 12. januar 2023 [C5], *Österreichische Post AG*, C-154/21, ECLI:EU:C:2023:3
ND v. DR [GC] C-21/23	Dom av 4. oktober 2024 [GC], *ND. v. DR*, C-21/23, ECLI:EU:C:2024:846

Den europeiske menneskerettighetsdomstolen (EMD)

Olsson mot Sverige (1988)	Olsson mot Sverige [J], no. 10465/83, (1988) ECHR:1988:0324JUD001046583.

Üner mot Nederland (1999)	Üner mot Nederland [J], no. 46410/99, (1999), ECHR:1999:1018JUD004641099.
S. og Marper mot UK (2008)	S. og Marper mot UK [GC], no. 30562/04 og 30566/04, (2008), ECHR:2008:1204JUD003056204.
Mockutė mot Litauen (2018)	Mockutė mot Litauen [J], no. 66490/09, (2018) ECHR:2018:0227JUD0066490/09.

Litteratur (alfabetisk)

Bergseng Skullerud mfl. (2018)	Bergseng Skullerud, Åse Marie, Rønnevik, Cecilie, Skorstad, Jørgen og Engh Pellerud, Marius, *Personvernforordningen (GDPR)*, *Kommentarutgave* (Oslo, 2018).
Clausen og Munte-Kaas (2020)	Clausen, Christopher Sparre-Enger og Munte-Kaas, Hugo-A. B, *Personvern og tiltak mot hvitvasking: – Særlig om screening mot sanksjonslister*, Lov&Data 2020 nr. 1 s. 20-22, (https://lovdata.no/pro/#document/JUS/lod-2020-141-20?searchResultContext=1667&rowNumber=1&totalHits=1, hentet fra Lovdata.no)
Fredriksen (2013)	Fredriksen, Halvard H., *Betydningen av EUs pakt om grunnleggende rettigheter for EØS-retten*, Jussens Venner vol. 48, utg. 6 (2013) side 371-399, (https://doi.org/10.18261/ISSN1504-3126-2013-06-01, hentet fra Idunn.no).
Høgberg (2008)	Høgberg, Alf Petter og Stridbeck, Ulf (red.), *Hvitvasking* (Oslo, 2008)

Rui (2012)	Rui, Jon Petter, *Hvitvasking: Fenomenet, regelverket, nye strategier* (Oslo, 2012)
Rui mfl. (2021)	Rui, Jon Petter, Holm Ringen, Gunnar og Frivold Rørholt, Kristine, *Hvitvaskingsloven, lovkommentar* (Oslo, 2021)
Rui mfl. (2024)	Rui, Jon Petter, Holm Ringen, Gunnar og Frivold Rørholt, Kristine, *Hvitvaskingsloven, lovkommentar* (Oslo, 2024, hentet fra Juridika).
Schartum (2020)	Schartum, Dag Wiese, *Personvernforordningen – en lærebok* (Bergen, 2020)
Schartum og Bygrave (2004)	Schartum, Dag Wiese og Bygrave, Lee A., *Personvern i informasjonssamfunnet,* 1.utgave (Bergen, 2004)
Schartum og Bygrave (2016)	Schartum, Dag Wiese og Bygrave, Lee A., *Personvern i informasjonssamfunnet,* 3.utgave (Bergen, 2016)
Vogel mfl. (2020)	Vogel, Benjamin og Maillart, Jean-Baptiste (eds.), *National and International Anti-Money Laundering Law – Developing the Architecture of Criminal Justice, Regulation and Data Protection*, 1. utgave (United Kingdom, 2020)
Vogel mfl. (2024)	Vogel, Benjamin og Lassalle, Maxime (mfl.), *Developing Public-Private Information Sharing to Strengthen the Fight against Money Laundering and Terrorism Financing*, februar 2024 (Hentet fra eucrim sine hjemmesider: https://eucrim.eu/media/articles_pdf/Vogel_Lassalle_Partfin_Recommendations-2.pdf)
Wessel-Aas og Ødegaard (2018)	Wessel-Aas, Jon og Ødegaard, Magnus, *Personvern*: *Publisering og behandling av personopplysninger*, (Oslo, 2018)

Avisartikler, innlegg, statistikk, rapporter, mv. (etter publiseringsdato)

Justis- og beredskapsdepartementet (2018)	Justis- og beredskapsdepartementet, *Ny personopplysningslov og EUs personvernforordning,* 20. juli 2018, (https://www.regjeringen.no/no/tema/lov-og-rett/innsikt/ny-personopplysningslov/id2592984/, sist besøkt 17. september 2024).
DN (2018)	DN, *Nordea meldt til Økokrim,* 17. oktober 2018, (https://www.dn.no/marked/okokrim/bill-browder/norge/nordea-meldt-til-okokrim/2-1-449728, sist besøkt 19. september 2024).
NRK (2018)	NRK, *Facebook saksøkt etter Cambridge Analytica-skandalen*, 19. desember 2018 (https://www.nrk.no/kultur/facebook-saksokt-etter-cambridge-analytica-skandalen-1.14349224, sist besøkt 24. oktober 2024)
E24 (2019)	E24, *Kobles til hvitvasking av 6,8 milliarder kroner*, 4. mars 2019, (https://e24.no/boers-og-finans/i/Xwv6dn/finsk-dokumentar-68-milliarder-i-mistenkelige-transaksjon-er-sluset-gjennom-nordea-kontoer, sist besøkt 19. september).
Datatilsynet (2019)	Datatilsynet, *Det Europeiske personvernrådet,* 3. mai 2019 (https://www.datatilsynet.no/regelverk-og-verktoy/internasjonalt/personvernradet/, sist besøkt 27. august 2024).
Økokrim (2019)	Økokrim, *Hva er MT-rapporter? Hva gjør EFE?*, 3. juli 2019, (https://www.okokrim.no/hva-er-mt-rapporter-hva-gjoer-efe.6233505-411472.html, sist besøkt 30. august 2024).
NRK (2019)	NRK, *Økokrim har startet etterforskning av DNB*, 28. november 2019, (https://www.nrk.no/norge/okokrim-har-startet-etterforskning-av-dnb-1.14800033, sist besøkt

Økokrim (2021) Økokrim, *Hvitvasking*, 16. september 2021 (https://www.okokrim.no/hvitvasking.422268.no.html, sist besøkt 11. september 2024).

Stortinget (2024) Stortinget, *EU-domstolen: generell og vilkårlig datalagring er ulovlig*, 8. oktober 2020 (https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/EU-EOS-informasjon/EU-EOS-nytt/2020/eueos-nytt---8.-oktober-2020/eu-domstolen-generell-og-vilkarlig-datalagring-er-ulovlig/, sist besøkt 19.september 2024).

Økokrim Økokrim, *Enhet for finansiell etterretning – Årsrapport 2023*, 19. mars 2024 (https://img8.custompublish.com/getfile.php/5282401.2528.twzwatjwppziua/Årsrapport%2B2023-klar.pdf?return=www.okokrim.no, sist besøkt 4. september 2024).

European Council (2024) European Council, *Anti-money laundering: Council adopts package of rules*, 30.mai 2024 (https://www.consilium.europa.eu/en/press/press-releases/2024/05/30/anti-money-laundering-council-adopts-package-of-rules/, sist besøkt 4. september 2024).

SSB (2024) Statistisk sentralbyrå, *Anmeldte lovbrudd og ofre*, 31. mai 2024 (https://www.ssb.no/sosiale-forhold-og-kriminalitet/kriminalitet-og-rettsvesen/statistikk/anmeldte-lovbrudd-og-ofre, sist besøkt 23. august 2024).

UNODC (u.d.) United Nations Office on Drugs and Crime (UNOCD), *Money Laundering*, ukjent dato, (https://www.unodc.org/unodc/en/money-laundering/overview.html, sist besøkt 18. August 2024)