UiO : Det juridiske fakultet

Lagring av personopplysninger etter GDPR, personopplysningsloven og hvitvaskingsloven

Kandidatnummer: 625

Leveringsfrist: 25.11.2021

Antall ord: 17666

Innholdsfortegnelse

1 Innledning

1.1 Tema

EU sin personvernsforordning ((EU) 2016/679) trådte i kraft 2018. Forordningen ble utarbeidet fordi man ønsket å styrke enkeltpersoners kontroll over egne personopplysninger, samt å bidra til å harmonisere regler om vern av personopplysninger innenfor EU/EØS-regionen. [1] Regelverket som blir omtalt som GDPR (General Data Protection Regulation) har bidratt til at mange virksomheter i større grad har måttet innrette og omstille seg for å oppfylle kravene den stiller. Dette innebærer blant annet mer omfattende rutiner både for planlegging av lagring og behandling av personopplysninger. For å skape et insentiv for etterlevelse av regelverket gir GDPR adgang til å gi relativt store bøter for manglende etterlevelse av regelverket.[2] I Norge har vi gjennomført forordning i lov om behandling av personopplysninger av 20.12.2018.

EU sitt fjerde hvitvaskingsdirektiv ((EU) 2015/849) trådte også i kraft i 2018. Som en følge av at dette trådte i kraft, har de nasjonale kravene til hvitvaskingsarbeid blitt strammet opp. Årsakene til dette er flere. Blant annet genererer hvitvasking annen kriminalitet, kan være ødeleggende for et lands økonomiske utvikling og kan være en trussel mot globale finansinstitusjoner og den legale verdensøkonomien. [3] Formålet med kriminalisering av hvitvasking er «å gjøre det lettere å få bakmenn dømt for økonomisk kriminalitet». Dette innebærer «å få befatning med utbytte fra straffbar handling».[4] For å oppnå formålet, har det blitt iverksatt omfattende og strenge krav til undersøkelser av kunder og rapportering i bransjer som kan benyttes til hvitvasking. Manglende etterlevelse av dette regelverket kan også føre til relativt høye bøter for å intensivere etterlevelsen. Direktivet er gjennomført i norsk rett via lov om tiltak mot hvitvasking og terrorfinansiering av 01.06.2018.

Begge reguleringene bærer preg av å være omfattende, kompliserte og ambisiøse i sine formål. I tillegg har begge en risikopreget tilnærming til hvordan de forpliktede skal oppfylle kravene. Denne tilnærmingen gjør at det ligger mye skjønn til de forpliktede når de skal vurdere hva

[1] Justis- og beredskapsdepartementet (2018)
[2] Personopplysningsloven §§ 26 og 30
[3] Rui (2021) s. 34-37
[4] Rui (2021) s. 39

slags tiltak som er nødvendig for å gjennomføre regelverkene. Dette innebærer at de forpliktede bør ha god risikoforståelse i sine vurderinger når de skal etterleve begge regelverkene samtidig. I oppgaven vil man se at dette kan være utfordrende både på grunn av utformingen av enkelte regler og kompleksiteten av regelverkene.

Oppgaven vil derfor dreie seg om de konkrete pliktene til å lagre personopplysninger i hvitvaskingsloven holdt opp mot de generelle reglene for lagring av personopplysninger etter GDPR og personopplysningsloven. Det er i denne krysningen man kan se hvordan risikovurderingene som må foretas kan bidra til at de to regelverkene eventuelt kommer i et spenningsforhold eller bidrar til at de blir harmonisert.

1.2 Rettskildebildet

I vurderingen av personopplysningsregelverket og hvitvaskingsregelverket er det rettskilder av ulike karakterer som spiller inn. I det følgende skal det redegjøres for de helt elementære og mest fremtredende rettskildene i de to regelverkene. Dette er at de begge bygger på rettsakter fra EU og retten til privatliv som utgangspunktet for personvernreglene.

1.2.1 Personvernsforordningen og det fjerde hvitvaskingsdirektivet

GDPR er inkorporert i norsk lovgivning via personopplysningsloven. Forordningen er lagt ved som et vedlegg til loven, og gjelder som norsk rett. Det vil derfor en rekke steder i oppgaven bli henvist direkte til GDPR, siden det er her de fleste av reglene fremkommer. I tillegg til forordningsteksten oppstiller personopplysningsloven en rekke bestemmelser som er særnorske med tanke på å lagre personopplysninger. Vi har for eksempel strengere regler for bruk av uekte kamerautstyr.[5]

EU sitt fjerde hvitvaskingsdirektiv er gjennomført i norsk rett via hvitvaskingsloven. På generelt plan angir direktiver overordnede mål som medlemsstatene skal oppnå. Hva slags form og innhold de nasjonale rettsaktene skal ha er opp til de enkelte statene. Dette innebærer at statene kan sette strengere regler dersom de ser behov for det.[6] I norsk rett er dette gjort enkelte steder

[5] Personopplysningsloven § 31

[6] Lovdata (u.å)

ved gjennomføringen av hvitvaskingsdirektivet, for eksempel ved definisjon av reelle rettighetshavere og politisk eksponerte personer. Se kapittel 4.

1.2.2 Retten til privatliv

Retten til privatliv og derav retten til personopplysningsvern er helt grunnleggende for forståelsen av personopplysningsreglene. Lagring av personopplysninger anses som et inngrep i retten til privatliv. [7] Det varierer hvor stort inngrep som er lovlig å foreta avhengig av hva som er formålet med behandlingen. I dette avsnittet vil det derfor gjøres rede for hva som kreves for å gjøre inngrep i denne rettigheten både generelt og ved behandling av opplysninger etter hvitvaskingsloven.

Retten til privatliv er nedfelt i Grunnloven (Grl.) § 102 og Den europeiske menneskerettighetskonvensjonen (EMK) artikkel 8. Rettigheten favner vidt og retten til personvern utgjør kun en del av den. Helt grunnleggende skal retten til privatliv regulere forholdet mellom stat og borger.[8] For å skape og opprettholde et velfungerende demokrati er det viktig å forhindre at staten får for mye makt over egne borgere. Vi har blitt et mer digitalisert samfunn hvor teknologien stadig gir myndighetene og store kommersielle aktører effektive verktøy for å drive med overvåking og lagring av personopplysninger.[9] Dette med på å utfordre retten til privatliv og spesielt personopplysningsvernet.[10] Det kan dermed sies at retten til personopplysningsvern stadig blir en viktigere del av retten til privatliv.

EMK artikkel 8 sier at enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse, og at inngrep i denne rettigheten kun kan skje på visse vilkår. Retten til vern av personopplysninger fremkommer ikke direkte av teksten, men må innfortolkes.[11] Etter Den europeiske menneskerettighetsdomstolens (EMD) avgjørelser, så vil behandling av personopplysninger være et inngrep i retten til privatliv.[12]

[7] Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland avsnitt 129-138
[8] Skullerud (2019) s. 37
[9] Den europeiske menneskerettighetsdomstolen (2020) s. 7
[10] Ibid. s. 8
[11] Skullerud (2019) s. 37
[12] Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland avsnitt 129-138

Retten til privatliv har i norsk rett grunnlovsvern, jf. Grl. § 102. Dette innebærer at rettigheten skal tillegges betydelig vekt og utgjøre en skranke og sentral verdi ved utforming av regelverk og rettsanvendelse.[13] Bestemmelsen sier at «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integriteten». Personopplysningsvernet må også innfortolkes i denne bestemmelsen. At rettigheten har fått grunnlovsrang innebærer at personopplysningsvernet skal veie tungt når det settes opp mot andre interesser og hensyn som ikke er forankret tilsvarende, jf. lex superiorprinsippet.[14]

Retten til privatliv er ikke en absolutt menneskerettighet.[15] Av EMK artikkel 8 fremkommer det at man kan gjøre inngrep i rettigheten dersom det følger av lov, forfølger et legitimt formål og er nødvendig i et demokratisk samfunn. Høyesterettspraksis sier at Grl. § 102 skal tolkes med samme unntaksadgang, jf. HR-2015- 206-A avsnitt 60.

Adgangen til å gjøre inngrep i retten til privatliv ved lagring av personopplysninger etter hvitvaskingsloven begrunnes i allmenne hensyn. I EMK artikkel 8 er både hensynet til landets økonomi og forebygging av kriminalitet listet opp som legitime formål og begge kan begrunne inngrepet. Hva som er «nødvendig i et demokratisk samfunn» innebærer at man må foreta en forholdsmessighetsvurdering av de motstridende hensyn. I hvitvaskingslovens tilfelle blir dette en avveining mellom den registrertes rett til privatliv mot samfunnets behov for en velfungerende økonomi og forebygging av kriminalitet. Ved vektingen skal det som nevnt legges stor vekt på at retten til privatliv er grunnlovfestet.

Retten til privatliv og personvern er også nedfelt i EU sitt charter om fundamentale rettigheter artikkel 7 og 8. Charteret er ikke tatt inn i EØS-avtalen.[16] Dette medfører at Norge formelt sett ikke er bundet av det. Vernet i charteret anses allikevel som relevant ettersom begge regelverkene som vurderes tar utgangspunkt i EU/EØS-rett. Dessuten er rettighetene i Charteret utformet likt som tilsvarende rettigheter i EMK.[17] Det europeiske personvernrådet (EDPB) har i tillegg som uttalt mål for 2021-2023 å jobbe for at anti hvitvaskings-tiltak er kompatible med

[13] NOU 2009: 1 s. 274
[14] Høgberg (2013) s. 206
[15] GDPR fortalepunkt 4
[16] Stortinget (2020)
[17] Maximillian Schrems v. Data Protection Commissioner avsnitt 97-98

retten til privatliv og personvernbeskyttelse etter charteret, prinsippene om nødvendighet av slike tiltak i et demokratisk samfunn og proporsjonaliteten i tiltakene og rettsakter fra EU-domstolen.[18] Denne målsetningen vil derfor mest sannsynlig være styrende for hva slags påvirkning personvernreglene vil få for hvitvaskingsreglene i årene fremover.

1.3 Begreper

Personvernreglene og hvitvaskingsreglene har enkelte særegne begreper som vil være gjennomgående i oppgaven. Det anses derfor nødvendig å både presisere hva enkelte av de mest sentrale begrepene innebærer, og spesifisere hvordan de vil bli benyttet i oppgaven.

1.3.1 Personvern og personopplysningsvern

Personvern er et særnorsk begrep og det er uenigheter om hva begrepet innebærer. [19] De ulike definisjonene har allikevel til felles at de handler om begreper som «integritet», «menneskeverd» og «sjelelig fred».[20] Innholdet i begrepet handler derfor om noe mer enn retten til å ikke få behandlet personopplysningene sine. Personvernkommisjonen har derfor valgt å skille mellom begrepene «personvern» og «personopplysningsvern». Deres definisjon av personopplysningsvern er følgende: «*Personopplysningsvern dreier seg om regler og standarder for behandling av personopplysninger som har ivaretakelse av personvern som hovedmål. Reglenes formål er å sikre enkeltindivider oversikt og kontroll over behandling av opplysninger om dem selv. Med visse unntak skal enkeltpersoner ha mulighet til å bestemme hva andre skal få vite om hans/hennes personlige forhold*». [21]

Personopplysningsvernet skal dermed sikre at enkeltindivider har kontroll over egne personopplysninger og at eventuell behandling av deres personopplysninger er forutsigbar.

Både begrepet personopplysningsvern og personvern blir benyttet i oppgaven. Når sistnevnte nevnes er det snakk om personvern i form av personopplysningsvern.

[18] European Data Protection Board (2020)
[19] Skullerud (2019) s. 55
[20] NOU 2009:1 s. 30
[21] Dokument 16 (2011–2012) s. 172

1.3.2 Personopplysninger

«Personopplysninger» er legaldefinert i artikkel 4 nr. 1 som «enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet». For eksempel vil et personnummer gi opplysninger om den fysiske personen er mann eller kvinne, transaksjonsopplysninger kan gi opplysninger om en persons økonomi og hvor en person pleier å handle dagligvarer og et navn kan si noe om en persons opprinnelse eller religion.

I relasjon til hvitvaskingsloven så er det en rekke ulike personopplysninger som samles inn. Først og fremst er det opplysninger som er spesifikt angitt i bestemmelsene om kundetiltak, jf. hvitvaskingsloven §§ 12 og 13. Andre opplysninger av mer variert art må imidlertid også lagres etter mer skjønnsmessige vurderinger.

Stort sett vil det henvises til «personopplysninger» generelt og ikke spesifikke typer personopplysninger i denne oppgaven. Enkelte steder vil det allikevel presiseres konkrete opplysninger når det er klart hvilke som skal lagres eller når det uklart om det er adgang til å behandle konkrete opplysninger.

1.3.3 Rapporteringspliktig og behandlingsansvarlig

Hvem som er rapporteringspliktig etter hvitvaskingsloven følger av § 4 første, annet og tredje ledd, jf. § 2 bokstav c. Loven gjelder for finansielle rapporteringspliktige som banker, betalingsforetak, forsikringsselskaper og verdipapirforetak. Og for ikke-finansielle aktører som revisorer, regnskapsførere, advokater, eiendomsmeglere og tilbydere av spilltjenester. Det er derfor stor variasjon i hvem som er rapporteringspliktig. Dette vil gi ulike forutsetninger på ulike vis for å etterleve begge regelverk.

En behandlingsansvarlig kan være både en fysisk og en juridisk person. Behandlingsansvarlig har ansvaret for at behandlingen av personopplysninger skjer i henhold til kravene som

personopplysningsloven og GDPR oppstiller.[22] Det kan foreligge et felles behandlingsansvar mellom flere behandlingsansvarlige.[23] Ofte kan det også være uklart om en juridisk person er en behandlingsansvarlig eller en databehandler.[24] Denne distinksjonen utdypes ikke nærmere, siden det i denne oppgaven kun vil bli redegjort for behandlingsansvarliges plikter.

Ved etterlevelse av hvitvaskingsloven vil de som er forpliktet stort sett få rollen som både behandlingsansvarlig og rapporteringspliktig. I oppgaven kommer stort sett rapporteringspliktig til å bli brukt når det er snakk om rollen både som rapporteringspliktig og behandlingsansvarlig. Ellers så blir behandlingsansvarlig brukt ved redegjørelse av generelle personopplysningsregler.

1.4 Problemstilling

GDPR og personopplysningsloven oppstiller generelle regler for hvordan personopplysninger skal behandles og lagres. Reglene gjelder for alle typer behandling av personopplysninger som faller inn under regelverkets virkeområde. [25] Det kan gis nasjonale lover som angir en spesiell type behandling av personopplysninger og som medfører at de generelle kravene må vike, jf. lex specialis-prinsippet.[26] Disse spesielle behandlingsoppleggene må allikevel være innenfor rammene som forordningen stiller, jf. trinnhøydeprinsippet.[27] Systemet i personvernreglene tar dermed høyde for at de generelle reglene ikke passer i alle situasjoner hvor personopplysninger behandles, og at det finnes behov for spesialregulering. Allikevel skal forordningen sikre at lagring av personopplysninger alltid skjer innenfor gitte rammer som er veloverveide med tanke på den registrertes grunnleggende rettigheter og friheter.

Hvitvaskingslovens kapittel 6 regulerer hvordan rapporteringspliktige skal behandle personopplysninger ved oppfyllelse av lovens forpliktelser. Disse forpliktelsene dreier seg i stor grad om å lagre personopplysninger om kunder. I § 29 om forholdet til personopplysningsloven fremkommer det i andre ledd at «Personopplysningsloven gjelder ved rapporteringspliktiges

[22] GDPR art. 24
[23] Schartum (2020) s. 62
[24] Schartum (2020) s. 63
[25] Skullerud (2019) s. 41
[26] l.c.
[27] l.c.

behandling av personopplysninger etter loven her med mindre annet fremgår av bestemmelser gitt i eller i medhold av loven». Dette innebærer at rapporteringspliktige alltid må følge de generelle reglene i GDPR og personopplysningsloven ved lagring av personopplysninger, med mindre det er gitt eksplisitte unntak i loven. Unntakene må allikevel være innenfor rammene som forordningen stiller, som nevnt ovenfor.

Paragraf 30 første ledd, første punktum pålegger rapporteringspliktige en plikt til å lagre opplysninger i en viss tid. Bestemmelsen lyder som følgende: «*Rapporteringspliktige skal registrere og lagre opplysninger og dokumenter som er innhentet og utarbeidet i forbindelse med tiltak etter §§ 9 til 26, i fem år etter at kundeforholdet ble avsluttet eller transaksjonen ble gjennomført*».

Bestemmelsene i §§ 9 til 26 er bestemmelser om kundetiltak, oppfølging av opplysninger fremskaffet som følge av kundetiltak og rapporteringsplikt for rapporteringspliktige. Årsaken til lagringsplikten er at rapporteringspliktige må kunne vise til at de har foretatt de nødvendige vurderingene og iverksatt de nødvendige tiltakene de er forpliktet til etter hvitvaskingsloven.[28] Opplysningene bidrar også direkte til å oppfylle selve hovedformålet med hvitvaskingsloven som er å fremskaffe etterretningsinformasjon.[29]

Hvitvaskingsloven forutsetter dermed behandling av personopplysninger. Som nevnt har EDPB satt som mål frem til 2023 å harmonisere hvitvaskingsregelverket bedre med de grunnleggende rettighetene i EU Charteret. Dette målet viser en oppfatning om at hvitvaskingsreglene ikke oppfyller kravene som personopplysningsreglene stiller og er i uoverensstemmelse med menneskerettighetene. I denne oppgaven vil det gjøres en sammenligning av de to regelverkene for å se om denne presumsjonen stemmer.

Problemstillingen for denne oppgaven er om det foreligger et spenningsforhold mellom hvitvaskingsloven og personopplysningsreglene.

[28] Rui (2021) s. 356

[29] Ibid. s. 55

1.5 Håndhevelse av regelverkene

Både personvernreglene og hvitvaskingsreglene fungerer slik at det er de rapporteringspliktige og behandlingsansvarlige som selv må vurdere egen etterlevelse av reglene.[30] [31] Dette forutsetter at EU og EØS-statene har aktive tilsynsmyndigheter både når det gjelder å føre tilsyn og gi veiledning. I Norge er det henholdsvis Datatilsynet og Finnstilsynet som driver med dette.

Manglende eller mangelfull etterlevelse av begge regelverkene kan sanksjoneres med økonomiske sanksjoner, jf. hvitvaskingsloven § 49 og personopplysningsloven §§ 26 og 30. I tillegg kan resultatet av dette også innebære økt risiko for omdømmetap. Det kan trolig være utfordrende å sette seg inn i regelverkene hver for seg og i kombinasjon med hverandre. Siden sanksjonene kan være relativt store, så er det ikke umulig at rapporteringspliktige velger seg ett av regelverkene dersom de oppleves «umulige» å harmonisere. Muligheten for å bli sanksjonert kan dermed tenkes å ha stor praktisk betydning for etterlevelse av regelverkene.

2 Risikobaserte regelverk

Både hvitvaskingsloven og GDPR er risikobaserte regelverk. Slike regelverk er en kontrast til regelbaserte regelverk som baserer seg på konkrete terskler og hvor myndighetene har «risikoen» for vurderingene i reglene. [32] I dette kapittelet vil det bli redegjort hvor hva slags risiko man snakker om i relasjon til de to ulike regelverkene. Det er viktig å ha forståelse av disse vurderingene, fordi de har direkte betydning for hvordan regelverkenes formål skal ivaretas. Risikoen er derfor styrende for hvilke tiltak som må iverksettes og hvordan man skal tolke ulike bestemmelser.

Det vil derfor gjøres rede for hvordan risikotilnærmingene i de to ulike regelverkene er ment å fungere for å optimalisere de overordnede formålene. Ettersom de to formålene kan trekke i ulike retninger, vil det deretter vurderes hvordan rapporteringspliktige bør håndtere risikoene i begge regelverkene samtidig.

[30] Skullerud (2019) s. 176
[31] Rui (2021) s. 138
[32] l.c.

2.1 Prinsippet om risikobasert tilnærming i hvitvaskingsloven

I hvitvaskingsloven er det risikoen for at hvitvasking og terrorfinansiering skal skje man ønsker å kartlegge. Dette følger av formålet med loven som er «å forebygge og avdekke hvitvasking og terrorfinansiering», jf. hvitvaskingsloven § 1 første ledd. Andre ledd angir overordnet hvordan dette skal gjøres: «Tiltakene i loven skal beskytte det finansielle og økonomiske systemet samt samfunnet som helhet ved å forebygge og avdekke at rapporteringspliktige brukes eller forsøkes brukt som ledd i hvitvasking eller terrorfinansiering».

Av lovkommentarene fremkommer det mer konkret at formålet er å forebygge og avdekke hvitvasking og terrorfinansiering «ved å pålegge rapporteringspliktige å gjøre seg kjent med sine kunder, overvåke dem, undersøke indikasjoner på hvitvasking og terrorfinansiering, og å rapportere mistanke om slik virksomhet til myndighetenes enhet for finansiell etterretning». Oppsummert er dermed det overordnede formålet at rapporteringspliktige skal skaffe etterretningsinformasjon.[33]

Et spørsmål som oppstår ved tolkningen av andre ledd i formålsbestemesen er hvorvidt rapporteringspliktige er forpliktet til å redusere risikoen for at hvitvasking og terrorfinansiering skal skje.[34] Å redusere risikoen vil blant annet kunne innebære at kunder som utgjør en høy risiko for hvitvasking må ekskluderes. Dette vil kunne komme i strid med kravet om «financial inclusion», finansavtaleloven § 14(1) og forsikringsavtaleloven §§ 3-10, 12-12 og 12-9.[35] I tillegg kan det være i direkte strid med lovens formål dersom man skal ekskluderer kunder som utgjør høy risiko. Dette vil gjøre at man ikke får undersøkt, overvåket og rapportert disse til myndighetene.[36] Man kan derfor ikke si at det er krav om at rapporteringspliktige skal redusere risikoen.

I hvitvaskingsloven er risikoprinsippet et grunnleggende prinsipp som innebærer at rapporteringspliktige skal ha en risikobasert tilnærming når tiltakene i loven iverksettes. Dette kommer direkte til uttrykk i lovens § 6. [37]

[33] Rui (2021) s. 55
[34] Ibid. s. 57
[35] Rui (2021) s. 58
[36] l.c.
[37] Rui (2021) s. 138

Finanstilsynets rundskriv til hvitvaskingsloven sier at «Risikoklassifiseringen må bygge på generelle vurderinger fra virksomhetens risikovurdering og konkrete forhold tilknyttet den enkelte kunde».[38]

Den rapporteringspliktige må derfor først og fremst danne en forståelse av hvordan egen virksomhet kan benyttes til hvitvasking og terrorfinansiering, jf. § 7 om virksomhetsinnrettet risikostyring.[39] Dette innebærer hvordan foretakets egen virksomhet, virksomhetens produkter, tjenester og kundeforhold, ulike type kunder og kundegrupper og geografiske forhold kan utgjøre en risiko for hvitvasking.[40] I rundskrivet står det at den generelle risikovurderingen består av minimum fire komponenter.[41] Dette er for det første å ha kunnskap om hva hvitvasking og terrorfinansiering er. Kunnskapen danner et utgangspunkt for forståelsen av hvordan egen virksomhet kan benyttes til denne typen kriminalitet. For det andre ha kjennskap om sin egen virksomhet og kartlegge hva slags risiko som kan kyttes til ulike produkter, tjenester og transaksjoner. Dette gjelder også før nye produkter, tjenester og teknologi lanseres.[42] For det tredje må bedriftens distribusjonskanaler vurderes. Her kan for eksempel innledende kundetiltak av distributører som ikke er bundet av hvitvaskingsregelverket eller nettbaserte løsninger for kundeopprettelse og kundetiltak utgjøre en risiko. For det fjerde må rapporteringspliktige kjenne til hvem de forholder seg til. Dette innebærer hvem kunden, reelle rettighetshavere og andre som handler på vegne av kunden er. Informasjon om disse menneskene og deres tilknytning både geografisk og bransjemessig er dermed nødvendig og kan gi mye informasjon om risiko.

Som følge av den generelle vurderingen så deles vanligvis risikoen inn i lav, middels og høy.[43] Hva som konkret kan anses som relevante momenter for denne klassifiseringen følger av hvitvaskingsforskriften §§ 4-6 og 4-9. I disse forskriftsbestemmelsene oppstilles det typiske karakteristikker som kan tilsi lav eller økt risiko for hvitvasking. Dette kan for eksempel være at en kunde har tilknytning til et land med enten høyt eller lavt korrupsjonsnivå, har en transparent og lett forståelig selskapsstruktur eller en veldig innviklet og unødvendig kompleks

[38] Finanstilsynet (27. juni 2019) s. 14
[39] Rui (2021) s. 149
[40] Finanstilsynet (27. juni 2019) s. 10
[41] l.c.
[42] l.c.
[43] Rui (2021) s. 191

selskapsstruktur. De virksomhetsinnrettede vurderingene er som regel generelle og innebærer ikke personopplysninger.[44] De er heller med på å danne utgangspunktet for hva slags kundetiltak som må iverksettes for en konkret kunde, jf. § 9 andre ledd.[45]

Den rapporteringspliktige må gjennomføre kundetiltak før kundeforholdet etableres eller før utførelsen av en transaksjon, jf. § 11 første ledd. For å kunne kartlegge hvilken risiko en konkret kunde utgjør, så innebærer kundetiltak krav om at den rapporteringspliktige må ha kunnskap om hvem kunden er. Dette er et grunnleggende prinsipp i arbeidet mot hvitvasking og omtales som «know your costumer»-prinsippet (heretter KYC).[46] KYC innebærer at de rapporteringspliktige må innhente og lagre spesifikk informasjon om kunden. Denne informasjonen danner utgangspunktet for den løpende overvåkningen underveis i kundeforholdet, jf. § 24. Overvåkingen innebærer at den rapporteringspliktige følger opp om informasjonen kunden har gitt innledningsvis i kundeforholdet stemmer overens med faktisk oppførsel.

I hvilken grad kundetiltak skal iverksettes bestemmes dermed av hvilken risiko for hvitvasking og terrorfinansiering kunden anses å utgjøre. Dette innebærer lagring av flere opplysninger og større grad av overvåking når risikoen for hvitvasking er høy.

Det følger av hvitvaskingsloven § 6 at man skal ha en risikobasert tilnærming også til registrering og lagring av personopplysninger etter § 30. [47] Dette innebærer at det er større adgang til å lagre opplysninger når det er høyere risiko for hvitvasking, og motsatt ved lav risiko. Ifølge forarbeidene er det imidlertid mindre rom for en slik tilnærming etter § 30 enn ved gjennomføring av kundetiltak. [48]

Myndighetene er også forpliktet av risikoprinsippet ved gjennomføringen av hvitvaskingsreglene.[49] Dette innebærer blant annet at regler og retningslinjer må utformes basert på en «fornuftig avveining mellom ønsket om å regulere og å respektere den selvreguleringen som

[44] Rui (2021) s. 171
[45] Ibid. s. 174
[46] Ot.prp. nr. 72 (2002-2003) s. 71
[47] Rui (2021) s.356
[48] Ot.prp. nr. 3 (2008-2009) s. 49
[49] Rui (2020) s.143

risikoprinsippet legger opp til».[50] Tilsyn må også gjennomføres risikobasert. Tilsynsmyndighetene kan ikke bruke én standard for tilsynelatende like rapporteringspliktige, men må foreta mer konkrete vurderinger for hver enkelt rapporteringspliktig.[51]

2.2 Risikovurderinger i GDPR

I GDPR og personopplysningsloven er *det risikoen for at de grunnleggende rettighetene til de registrerte skal bli krenket* den behandlingsansvarlige må vurdere. [52] Dette følger av GDPR art. 1 nr. 2 som sier at forordningen skal sikre «vern av fysiske personers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger».

Lagring av personopplysninger anses som et inngrep i retten til privatliv, se punkt 1.2.2, og det vil alltid foreligge en viss risiko for de registrertes grunnleggende rettigheter når lagring skjer. Den behandlingsansvarlige er dermed forpliktet til å iverksette risikoreduserende tiltak for å gjøre risikoen akseptabel, men de har ikke plikt til å fjerne den fullstendig.[53] Tiltakene som skal iverksettes er i hovedsak tekniske og organisatoriske tiltak, jf. art. 24, 25(1), 28(1), (3)(e) og (4) og 32 (1). Fortalen nevner disse tiltakene ofte, men presiseres ikke hva de innebærer.[54] Ifølge Schartum så må innholdet baseres på en tolkning av samsvarsanalyser og formålsbetraktninger.[55] Dette innebærer en samlet vurdering av alle tiltak i forordningen, og hva som samlet sett gir best tolkningsresultat. Hans konklusjon er at «teknisk» forstås som «enhver teknisk fremgangsmåte, herunder bruk av teknologi i den forbindelse». «Organisatorisk» kan forstås som «noe som gjelder struktur og det å ordne, uten at det er gitt noen forutsetning om hva som skal organiseres». [56] Han er deretter forsiktig med å gi for spesifikke eksempler og poengterer at begge begrepene er vide og åpner opp for flere tiltak man kan konkretisere mer nøyaktig. Det er også andre kategorier tiltak som kan være veldig aktuelle, eksempelvis juridiske, økonomiske og pedagogiske tiltak. Eksempler på konkrete å øke kunnskapen om personopplysningsvern, ha rutiner for håndtering av personopplysninger, ha klar ansvarsfordeling for personvern og ha

[50] Rui (2021) s. 143
[51] l.c.
[52] Schartum (2020) s. 237
[53] Ibid. s. 240
[54] Ibid. s. 242
[55] Ibid. s. 244
[56] Schartum (2020) s. 245

klart for seg de overordnede rammene for behandlingen.[57] Selv om tiltak kan variere, er det et krav om at de tiltakene om er valgt skal være «effektive».[58]

Forordningen sier ingenting om hva som kreves av omfang og faglig nivå når det gjelder risikovurderingene. [59] Et fellestrekk mellom bestemmelsene som setter krav til risikovurderinger er at de tar sikte på risiko i relasjon til bestemmelser i forordningen.[60] Ifølge Schartum må utgangspunktet derfor trolig være at «risikovurderingen skal omfatte alle bestemmelser som den behandlingsansvarlige har forpliktelse til å etterleve».[61]

Artikkel 24, 25, 32 og 35 er helt sentrale bestemmelser om den behandlingsansvarliges plikter og inneholder overordnede krav til risikovurdering. [62] [63] Artikkel 24, 25 og 32 stiller krav til hvordan selve behandlingsopplegget skal være. Det må derfor gjennomføres en risikovurdering *før* man starter behandling av opplysninger etter disse bestemmelsene.[64] Dersom vurderingene etter disse bestemmelsene tilsier at det foreligger høy risiko, må man iverksette risikovurdering etter art. 35.[65]

I artikkel 24 som handler om den behandlingsansvarliges ansvar foreligger det en plikt til å iverksette tiltak for å sikre og vise at behandlingen skjer i overensstemmelse med kravene i forordningen. [66] Ved vurderingen av hva som kreves av tiltak, må det gjennomføres en forholdsmessighetsvurdering. Dette innebærer at jo større konsekvenser og risiko for de registrertes rettigheter og friheter, jo mer omfattende og strengere tiltak må til enn ved mindre inngripende og mindre omfattende behandlingsaktiviteter.[67] Ved vurderingen så må man ta hensyn til opplysningenes art, spesielt om det gjelder behandling av særlige kategorier av personopplysninger. I tillegg må det vurderes om formålet med behandlingen vil få stor betydning for den

[57] Datatilsynet (2018)
[58] Fortalepunkt 74
[59] Schartum (2020) s. 238
[60] Ibid. s. 239
[61] Ibid. s. 239
[62] Skullerud (2019) s.176
[63] Schartum (2020) s. 237
[64] Ibid. s. 238
[65] Ibid. s. 276
[66] Skullerud (2019) s. 274
[67] l.c.

registrerte ved at den resulterer i en beslutning eller innebærer overvåking. [68] Videre påpeker lovkommentarene at for virksomheter som er bundet av flere regelverk og som har rutiner for gjennomføring av risikovurderingen på ett forretningsområde, så kan disse utvides til å også inkludere risiko knyttet til personvern. Målsettingen bør være at internkontrollen som skal utøves etter artikkel 24 integreres i virksomhetens prosesser.[69] For eksempel kan en virksomhetsinnrettet risikovurdering etter hvitvaskingsloven, også inkludere risikovurdering knyttet til personvern.

Artikkel 25 handler om krav til innebygd personvern og personvern som standardinnstilling. Denne plikten gjelder uavhengig av risiko ved behandlingen, men foreliggende risiko vil allikevel være førende for hvilke tiltak som den behandlingsansvarlige plikter å iverksette i det enkelte tilfellet.[70] Det skal etableres tekniske og organisatoriske tiltak for å sikre en effektiv gjennomføring av prinsippene for vern av personopplysninger.[71] Dataminimeringsprinsippet, prinsippet om riktighet og lagrinsbegrensningsprinsippet fremheves som godt egnet til å kunne ivaretas gjennom tekniske tiltak.[72]

Artikkel 32 handler om sikkerhet ved behandlingen av personopplysninger. Bestemmelsen oppstiller ingen konkrete krav til sikkerhetstiltak, men angir hovedprinsipper. [73] Overordnet stilles det krav til egnet sikkerhetsnivå. Hva som anses som et egnet sikkerhetsnivå må vurderes av den behandlingsansvarlige. Videre må det iverksettes tiltak om bringer risikoen ved behandlingen ned på et tilfredsstillende nivå.[74] Ved denne vurderingen skal det tas hensyn til den tekniske utviklingen, kostnaden ved tiltakene, behandlingens art, omfang, formål og sammenhengen det utføres i og hvilke typer opplysninger som inngår i behandlingen, jf. Art. 32 nr. 1. Det gis videre forslag om fire konkrete sikkerhetstiltak som bør vurderes, jf. Art. 32 nr. 2 bokstav a-d. I art. 32 nr. 1 så vises det til en risikobasert tilnærming hvor sikkerhetsnivået og tiltakene skal stå i et rimelig forhold til den aktuelle risiko ved behandlingen.[75] Denne tilnærmingen

[68] Schartum (2020) s. 274-275
[69] Ibid. s. 275
[70] Ibid. s. 280
[71] Ibid. s. 281
[72] Ibid. s. 281
[73] Ibid. s. 307
[74] Ibid. s. 208
[75] Skullerud (2019) s. 312

krever at det gjennomføres risikovurderinger av behandlingen, jf. Art. 32. nr. 2. [76] Den rådende standard for informasjonssikkerhet er ISO 27001.[77] Denne legger opp til at behandlingsansvarlig skal ha en risikobasert tilnærming når sikkerhetstiltakene planlegges, gjennomføres og evalueres.

GDPR artikkel 35 pålegger behandlingsansvarlige å gjennomføre en vurdering av hvilke konsekvenser en planlagt behandling av personopplysninger vil få for rettighetene og frihetene til de registrerte. En slik vurdering kan resultere i at behandlingen endres eller at man ikke skal behandle opplysninger i det hele tatt.[78] Denne vurderingen skiller seg fra risikovurderingene i de andre nevnte bestemmelsene, ettersom disse vurderingene har som formål «å fastsette hva som er tilfredsstillende nivå av organisatoriske og tekniske sikkerhetstiltak for en behandling av personopplysninger».[79] I disse bestemmelsene tar man også hensyn til virksomhetens interesser og perspektiv ved risikovurderingene, men ved konsekvensvurderingen så er det den registrertes perspektiv som er i fokus.[80] Selv om ordlyden i art 35 tilsier at en konsekvensvurdering kun skal gjennomføres når «det er sannsynlig at en type behandling» vil medføre høy risiko for de registrertes rettigheter og friheter, er det klart at lignende vurderinger også må skje ved behandlinger som ikke nødvendigvis utgjør en høy risiko, jf. art. 24.[81] Ifølge Schartum innebærer dermed ikke art. 35 en ny og separat risikovurdering.

Av art. 5 nr. 2 jf. art. 5 nr. 1 bokstav f kan det innfortolkes et krav om at risikovurderinger skal være dokumentert og etterprøvbare.[82] Når risikovurderingene skal gjennomføres må ses i sammenheng med kravene i art. 24, 25 og 32. Dette innebærer at det bør være et mål at risikovurderingene skal få reell innflytelse på systemer og løsninger som etableres.[83] Risikovurderinger bør gjennomføres også etter at det er etablert behandling, og spesielt hvis det skjer endringer av betydning for risikoen.[84]

---

[76] Skullerud (2019) s. 312
[77] l.c.
[78] Skullerud (2019) s. 326
[79] l.c.
[80] l.c.
[81] Jarbekk (2021) art. 35 note 1
[82] Skullerud (2019) s. 312
[83] Skullerud (2019) s. 313
[84] l.c.

2.3 Vurdering av innholdet i rapporteringspliktiges plikt til å vurdere risiko i hvitvaskingsloven og GDPR og personopplysningsloven

Redegjørelsen ovenfor gjør det klart at den rapporteringspliktige har en plikt til å vurdere risiko i begge regelverk. Risikoene er imidlertid ulike, og dette gjør det de kan de trekke i forskjellige retninger. Etter hvitvaskingsloven fremstår kravet noe mer klart og håndfast enn i GDPR. Dette har nok sammenheng med at det er regulert i et eget kapittel, jf. kapittel 3. Mens i GDPR følger det mer av systemet i reguleringen, og risikovurderingene varierer derfor noe etter hvilken bestemmelse det er snakk om. Dette gjør at innholdet i vurderingene kan fremstå mer «utilgjengelige».

Rapporteringspliktige skal ha en risikobasert tilnærming til lagring av personopplysninger. Dette innebærer at når risikoen for hvitvasking er høy, så vil det også være større adgang til å lagre personopplysninger. Et større omfang av og mer inngripende lagring kan bidra til økt risiko for de registrertes rettigheter. Høy risiko for hvitvasking og dermed større omfang av lagring av personopplysninger kan dermed føre til at personopplysningsreglene samtidig stiller krav til risikoreduserende tiltak.

I redegjørelsen av GDPR art. 24 så fremkommer det at det bør være en målsetting at internkontrollen som skal utøves integreres i virksomhetens prosesser.[85] Rapporteringspliktige bør dermed i den virksomhetsinnerettede risikovurderingen etter hvitvaskingsloven, også vurdere hva slags risiko virksomhetens behandling av personopplysninger utgjør. Dette vil gi rapporteringspliktig en overordnet oversikt over hva slags personverstiltak som bør iverksettes etter den varierende risikoen for hvitvasking. Det som er viktig er dermed å finne ut hva som konkret leder til økt risiko ved de ulike behandlingen, og deretter hva slags tiltak eller hvilket nivå av tiltak som kreves for å få risikonivået ned på et egnet nivå. Og om risikonivået er såpass høyt at behandlingen er ulovlig, jf. GDPR art. 35. Sistnevnte alternativ kan være problematisk ettersom at det er viktig å få gjennomført kundetiltak når risikoen for hvitvasking er høy.

[85] Skullerud (2019) s. 275

Trolig vil en slik samlet risikovurdering bidra til at virksomheten på et grunnleggende nivå har tiltak som skaper et godt personopplysningsvern ved utførelsen av bestemte kundetiltak. Dette skaper oversikt over hvilke situasjoner og scenarioer som krever ulike tiltak etter begge regelverkene, og sammenhengen mellom de to risikovurderingene kommer tydeligere frem. I tillegg bør risiko selvsagt alltid vurderes konkret i ulike tilfeller, men trolig vil ressurser sette grenser for hvor langt dette er mulig å gjennomføre.

3 Generelle og spesielle krav til lagring av personopplysninger etter GDPR, personopplysningsloven og hvitvaskingsloven

Som redegjort for i kapittel 1.4, så gjelder både generelle og mer spesielle krav til lagring av personopplysninger etter hvitvaskingsloven. I denne delen av oppgaven vil det gjøres rede for når de generelle personvernreglene kommer til anvendelse, de helt grunnleggende kravene om behandlingsgrunnlag og – formål ved lagring av personopplysninger, grunnleggende personvernsprinsipper og de registrertes rettigheter. Løpende vil det bli gjort rede for hvordan dette er regulert i hvitvaskingsloven og drøftes hvordan loven i enkelte tilfeller gir mer spesialtilpassede regler. Dette vil gi et bedre grunnlag for å forstå hvordan regelverkene virker sammen og eventuelt er i et spenningsforhold.

3.1 Når kommer personvernregelverket til anvendelse?

Det er ikke fullstendig overlapp mellom personopplysningsreglene og hvitvaskingsreglene. Det vil derfor kort redegjøres for når personopplysningsreglene generelt kommer til anvendelse. Og når de komme til anvendelse ved etterlevelse av hvitvaskingsloven.

Personopplysningsloven § 2 sier at «Loven og personvernforordningen gjelder ved helt eller delvis automatisert behandling av personopplysninger og ved ikke-automatisert behandling av personopplysninger som inngår i eller skal inngå i et register». Teksten en identisk med teksten i forordningens artikkel 2 nr. 1.

Ut ifra den vide formuleringen så vil reglene i utgangspunktet gjelde for «enhver informasjonsmengde, elektronisk eller fysisk, som er systematisert eller behandles på en slik måte at det er

mulig å gjenfinne personopplysninger». [86] Hva som er en personopplysning, er redegjort for i kapittel 1.3.2.

«Behandling» er i artikkel 4 nr. 2 definert som «enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registering organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller andre former for tilintetgjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring».

Listen er ikke uttømmende, og det er svært lite som skal til for at en handling anses som behandling av personopplysninger. Ut ifra lovkommentarene er man bundet av reglene så å si med en gang man er i befatning med personopplysninger.[87]

Behandling som er helt eller delvis «automatisert» gjelder behandling med lite eller ingen menneskelig involvering og som utføres eller kontrolleres av en maskin.[88] «Ikke-automatisert» behandling utføres av mennesker. Dette kan for eksempel være notater som lagres i et register.

3.1.1 Når kommer personvernregelverket til anvendelse ved etterleves av hvitvaskingsloven?

De personopplysningene som lagres etter hvitvaskingsloven er i hovedsak opplysninger som samles inn ved gjennomføring av kundetiltak. Ettersom formålet med å gjennomføre kundetiltak er å identifisere kunden eller reelle rettighetshavere, så innebærer dette at alle opplysninger som blir samlet i tilknytning til dette er opplysninger «om en identifisert eller identifiserbar fysisk person («den registrerte»)», jf. GDPR art. 4 nr. 1.

Av § 29 (1) så fremkommer det som nevnt at «Rapporteringspliktige kan behandle personopplysninger for å oppfylle forpliktelser i loven her eller forskrifter gitt i medhold av loven». Det er dermed ved de forpliktelsene som forutsetter eller pålegger rapporteringspliktige å behandle personopplysninger som personopplysningsreglene gjelder for. Det er dermed ikke total, men ganske stor overlapp mellom de to regelverkene

[86] Skullerud (2019) s. 138
[87] Skullerud (2019) s. 153
[88] Jarbekk (2021) artikkel 2, note 2

3.2 Behandlingsgrunnlag og formål

For å kunne lovlig behandle personopplysninger må den behandlingsansvarlige oppfylle kravene som følger av personopplysningsloven og personvernsforordningen. Overordnet så må man fastsette et formål med behandlingen og ha et rettslig grunnlag for å behandle personopplysninger, jf. GDPR artikkel 5 (1) b, 6 og 9. Siden det aktuelle behandlingsgrunnlaget i hvitvaskingsloven følger av lov, vil det kun gjøres rede for kravene til behandlingsgrunnlag som følger av lov.

3.2.1 Behandlingsformål

I GDPR art. 5 nr. 1 bokstav (b) fremkommer det at personopplysninger skal «samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene».

Dette kravet har en sentral betydning for de rettslige rammene rundt behandlingen av personopplysninger. I forordningen er kravet til formål formulert både som et prinsipp, men også fremhevet som et grunnleggende krav til lovlig behandling av personopplysninger. [89] Når man angir formålet med behandlingen, så vil dette i noen grad være bestemmende for hva som kan utgjøre et lovlig behandlingsgrunnlag, se kapittel 3.2.3. Det har også betydning for prinsippene om dataminimering, lagringsbegrensning og opplysningskvalitet ettersom disse prinsippene tar utgangspunkt i hva som er formålet med den aktuelle behandlingen.[90]

Et formål må være konkret utformet. Dette innebærer at det må egne seg til å vurdere om opplysningene er nødvendige og om behandlingen skjer i samsvar med GDPR sine bestemmelser. Det skal ikke være tvil om hva som er formålet og det må være berettiget. Dette innebærer at det ikke må være i uoverensstemmelse med andre regelverk og det må følge de generelle samfunnskravene. Formålet må også være saklig begrunnet i den behandlingsansvarliges virksomhet. Dette innebærer at formålet må stå i samsvar med hva man kan forvente at virksomheten samler inn opplysninger til.[91]

[89] Schartum (2020) s. 91
[90] l.c.
[91] Skullerud (2019) s. 173

3.2.2 Behandlingsformål i hvitvaskingsloven

I hvitvaskingsloven er det overordnede formålet for behandling av personopplysninger «å forebygge og avdekke hvitvasking og terrorfinansiering», jf. § 1. Dette innebærer at alle opplysninger som behandles og lagres for å oppfylle lovens forpliktelser må tjene til å forebygge og avdekke hvitvasking og terrorfinansiering. Formålet er ganske vidt og det kan tenkes at det tidvis kan være krevende for de rapporteringspliktige å vurdere hva som faller inn under formålet og ikke.

Datatilsynet har avgitt et høringssvar hvor de stiller seg noe kritisk til reglene for personopplysningsbehandling i hvitvaskingsloven, spesielt med tanke på behandling av særlige kategorier. Dette har også en side til formålsbegrensningsprinsippet. Datatilsynet skriver i høringssvaret at for å oppnå de to grunnprinsippene om proporsjonalitet og dataminimering, nærmere om dette i kapittel 3.3, etter GDPR, så bør det presiseres hvilke opplysninger man kan behandle til hvilke formål, og hvor man ikke kan behandle bestemte type av opplysninger. [92] En følge av dette vil trolig være større bevissthet rundt hvilke opplysninger som tjener til å oppfylle formålet og ikke.

Behandlingsformålet vil i hvitvaskingsloven dermed kunne bidra til god veiledning for når og hvor man skal legge ned mest ressurser i hvitvaskingsarbeidet, ettersom tiltakene i hvitvaskingsloven skal være risikobasert, se kapittel 2.1. Når det er høy risiko for hvitvasking, så vil man i større grad være innenfor behandlingens formål. Behandlingsformålet kan derfor anses som et viktig «instrument» når man skal balanserer risikoen i hvitvaskingsloven og personopplysningsreglene med hverandre.

3.2.3 Behandlingsgrunnlag

Artikkel 6 i GDPR sier at adgang til å behandle «alminnelige» personopplysninger må være basert på et formelt grunnlag. Dette kan overordnet være samtykke fra de registrerte, jf. bokstav a i bestemmelsen eller spesifikke «nødvendige» grunner som følger av forordningen, jf. bokstav

[92] Datatilsynet (2020) s. 3

b-f. [93] Det sikreste grunnlaget følger ifølge Schartum av lov.[94] Her vil det kun gjøres rede for behandlingsgrunnlag etter bokstav c, fordi det er dette alternativet som er relevant for oppgavens problemstilling.

Bokstav c i forordningen sier at behandling er lovlig dersom «behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige». Det kreves etter artikkel 6 nr. 3 at det i tillegg må foreligge hjemmel i nasjonal rett eller unionsretten. [95] I fortalens punkt 41 så utdypes dette med at det ikke er krav til en formell lov vedtatt av et parlament. Det presiseres at «Nevnte rettslige grunnlag eller lovgivningsmessige tiltak bør imidlertid være tydelig og presist, og anvendelsen av det bør være forutsigbar for personer som omfattes av det, i samsvar med rettspraksisen til Den europeiske unions domstol («Domstolen») og Den europeiske menneskerettighetsdomstol».

Behandling av særlige kategorier av personopplysninger er i utgangspunktet forbudt, jf. GDPR artikkel 9 nr. 1. Årsaken til dette er at behandling av disse kan medføre en særlig høy risiko for de registrertes rettigheter, og trenger derfor et særskilt vern.[96] «Særlige kategorier» er personopplysninger om «rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering». Denne listen er uttømmende, men de ulike kategoriene er veldig åpne og dette medfører at det kan bli vanskelig å vurdere om en opplysning rammes av forbudet. [97] Eksempler på vanskelige vurderinger kan være å vurdere om tilhørighet i en terrororganisasjon sier noe om ens religion eller politiske oppfatning, om et bilde av en person som bærer et religiøst hodeplagg sier noe om dens religion eller om et bilde kan si noe om en persons legning, helseforhold eller etisk tilhørighet.[98]

[93] Schartum (2020) s. 110
[94] Ibid. s. 111
[95] Jarbekk (2021) art. 6 note 9
[96] Skullerud (2019) s. 207
[97] Schartum (2020) s. 134
[98] Skullerud (2019) s. 207

I nr. 2 gjøres det unntak fra forbudet dersom vilkårene i bokstav a til j er oppfylt. Ved å oppfylle de konkrete vilkårene i unntakene foreligger det dermed behandlingsgrunnlag for å behandle personopplysningen. I vårt tilfelle er det bokstav g om «allmenne interesser» som er aktuelt ettersom å forebygge og avdekke hvitvasking og terrorfinansiering anses som viktige allmenne interesser.[99]

Bestemmelsen krever at behandlingen er «nødvendig» av hensyn til «viktige allmenne interesser» og på grunnlag av nasjonal rett. Det er trolig strengere krav til klarere hjemmel etter § 9 enn etter § 6.[100] Det må også foretas en forholdsmessighetsvurdering.[101] Viktigheten vil avhenge av den konkrete situasjonen og det forutsettes at bruken av dette unntaket er i samsvar med prinsippet om lovlighet, rettferdighet og åpenhet i artikkel 5(1) a, se kapittel 3.3. [102] Årsaken til at prinsippet er spesielt viktig er at formuleringen «viktige allmenne interesser» er vid og dermed åpen for tolkning, samtidig som at unntaket kan være potensielt inngripende.[103]

Det er et krav om at behandlingen må være «nødvendig» både etter artikkel 6 g 9. Kravet angir noe den «behandlingsansvarlige ønsker eller er forpliktet til å oppnå» ved behandlingen.[104] Kravet virker som å peke mot behandlingsformålet. Men ifølge Schartum så er det ikke meningen at man skal innfortolke et krav tilsvarende kravet til formål etter artikkel 5 første ledd, bokstav b. Det påpekes allikevel at minst ett av formålene som er satt for den enkelte behandlingen bør være i tråd med det overordnede formålet.[105] Dette viser at logisk sett så bør det være en sammenheng mellom behandlingsgrunnlag og -formål for at behandlingen skal være lovlig.

Artikkel 10 angir kravene for behandling av personopplysninger om straffedommer og lovovertredelser. I norsk rett gir personopplysningsloven § 11 hjemmel for slik behandling. Bestemmelsen oppstiller de samme kravene som artikkel 9 stiller til særlige kategorier av opplysninger. I tillegg til at vilkårene i denne bestemmelsen må være oppfylt, så må det også foreligge behandlingsgrunnlag etter artikkel 6.[106] Bestemmelsen sier at i utgangspunktet skal

[99] Hvitvaskingsdirektivet artikkel 43
[100] Skullerud (2019) s. 207
[101] Schartum (2020) s. 139
[102] l.c.
[103] l.c.
[104] Schartum (2020) s. 126
[105] l.c.
[106] Skullerud (2019) s. 217

personopplysninger om straffedommer og lovovertredelser være «under en offentlig myndighets kontroll».[107] Det er allikevel anledning til å behandle denne typen opplysninger når det er tillatt etter nasjonal rett, og det er gitt nødvendige garantier for registrertes rettigheter og friheter.

3.2.4 Behandlingsgrunnlag i hvitvaskingsloven

Når det kommer til hvitvaskingsloven så fremkommer det rettslige grunnlaget for å behandle alminnelige personopplysninger av § 29 første ledd. Bestemmelsen sier at «Rapporteringspliktige kan behandle personopplysninger for å oppfylle forpliktelser i loven her eller forskrifter gitt i medhold av loven». Rekkevidden for behandlingsgrunnlaget vil her være styrt av formålet med behandlingen, som er å avsløre og forebygge hvitvasking.

Andre ledd angir at grunnlag for å behandle «sensitive opplysninger» kan fastsettes i forskrift. Definisjonen «sensitive opplysninger» ble byttet ut med «særlige kategorier» da GDPR trådte i kraft, og begrepet i hvitvaskingsloven skal forstås i tråd med forordningen.[108] I hvitvaskingsforskriften § 6-1 så gis det adgang til å behandle «personopplysninger omfattet av personvernforordningen artikkel 9 og 10 når det er nødvendig for å gjennomføre forpliktelsene i hvitvaskingsloven med forskrift». Denne bestemmelsen gir dermed adgang til å behandle både særlige kategorier og opplysninger om straffedommer og lovovertredelse.

I høringsrundene til «Endringer i hvitvaskingsregelverket (lov og forskrift) – EUs femte hvitvaskingsdirektiv mv.»[109] så har Datatilsynet inngitt et høringssvar hvor de mener at det bør stilles klarere krav til hvordan rapporteringspliktige skal behandle særlige kategorier av personopplysninger. De mener at forslaget som er utarbeidet ikke favner godt nok om kravene som stilles til slik behandling[110] Og det trengs tydeligere bestemmelser for når man kan behandle hvilke typer av særlige opplysninger, særlig med tanke på at det er de rapporteringspliktige selv som skal vurdere når det er nødvendig å behandle disse. [111]

[107] Schartum (2020) s. 149
[108] Rui (2021) s. 355
[109] Finanstilsynet (2019)
[110] Datatilsynet (2020) s. 2
[111] Datatilsynet (2020) s. 3

Det kan dermed argumenteres for at rekkevidden til å behandle særlige kategorier i dagens hvitvaskingslov og – forskrift ikke verner godt nok om de registrertes grunnleggende rettigheter og friheter. Som redegjørelsen viser, er det i utgangspunktet forbudt å behandle særlige kategorier. For å kunne gjøre dette må det oppstilles veloverveide krav som gir forutsigbar behandling for de registrerte. Datatilsynet nevner at det trolig ikke er nødvendig å ha anledning til å behandle opplysninger om rasemessig opprinnelse, fagforeningsmedlemskap, genetiske opplysninger, helseopplysninger eller en persons seksuelle forhold eller orientering i antihvitvaskingsarbeid.[112] At behandlingsansvarlige dermed kan behandle slike opplysninger på bakgrunn av egne vurderinger fremstår lite veloverveid og uforutsigbar holdt opp mot de kravene GDPR stiller. I kapittel 4.3 kommer det et eksempel hvor denne problemstillingen er aktuell.

3.3 Grunnleggende prinsipper for lagring av personopplysninger

Dette kapittelet tar for seg de grunnleggende prinsippene for behandling av personopplysninger, jf. GDPR artikkel 5. Disse prinsippene gir føringer for hvordan behandling skal skje og har stor betydning for tolkning av andre bestemmelser i forordningen.[113] Prinsippene er ganske skjønnsmessige, har vide formuleringer og de konkrete innholdene er ikke fastlagt enda. Dette innebærer at de gir veiledninger av mer prinsipiell betydning og at de i enkelte tilfeller veier mindre dersom de veies mot andre konkurrerende hensyn. [114] Prinsippet om formålsbegrensning vil ikke bli behandlet her siden det allerede er behandlet i kapittel 3.2.1.

Lovlighet, rettferdighet og åpenhet

I bokstav (a) stilles det krav til at personopplysninger skal behandles lovlig, rettferdig og gjennomsiktig «med hensyn til den registrerte». At personopplysninger skal behandles «lovlig» viser først og fremst til de krav som rettsordenen stiller.[115] Det må foreligge et rettslig grunnlag som gir adgang til lagring av personopplysninger, men behandlingen må også være i overensstemmelse med omkringliggende rett som for eksempel EU-rett og menneskerettighetene.[116]

[112] Datatilsynet (2020) s. 3
[113] Schartum (2020) s. 87
[114] l.c.
[115] Schartum (2020) s. 89
[116] l.c.

At behandlingen må være «rettferdig» innebærer at den registrerte må oppfatte den som rimelig og naturlig med tanke på formålet med innsamlingen[117] og at motstridende interesser skal avveies på en forholdsmessig måte.[118]

Kravet til åpen eller transparent behandling handler om at den registrerte lett skal kunne få forståelse for at personopplysninger blir behandlet og hvordan dette foregår. Dette bidrar til at registrerte enklere kan håndheve rettighetene sine. [119] Kravet innebærer også at den registrerte skal få all den informasjonen som er relevant for å forstå hva behandlingen går ut på, hvilke regler som gjelder og hvordan dette praktiseres.[120]

Dataminimering

I bokstav (c) er det krav om at opplysningene skal være «adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for».

At personopplysninger skal være adekvate peker tilbake til formålet med behandlingen. Med dette som utgangspunkt skal det ikke lagres for mange opplysninger, men det skal være mange nok opplysninger til å oppnå formålet med behandlingen.[121]

Relevanskriteriet har også sammenheng med formålet. Opplysningene som innhentes skal være relevante for å oppnå formålet. Det er rettslig relevante opplysningen det siktes til i denne sammenhengen.[122] Dersom det er snakk om opplysninger som ikke følger av rettslige forhold, så må man begrense til opplysninger som er saklig relevante. [123] Av fortalens punkt 39 kan man lese at dette gjelder når «behandlingen ikke med rimelighet kan oppfylles på en annen måte».

Videre så skal opplysningene «begrenses til det som er nødvendig». Dette kravet må også holdes opp mot formålsbegrensningen. Vurderingen man må foreta for enhver opplysning er om

[117] Skullerud (2019) s. 173
[118] Schartum (2020) s. 89
[119] Skullerud (2019) s. 173
[120] Schartum (2020) s. 90
[121] Ibid. s. 92
[122] Schartum (2020) s. 92
[123] l.c.

man klarer seg uten den. [124] Dersom man kommer til at man har behov for en opplysning, må man videre vurdere hvor lenge man har behov for den og hvor detaljert den trenger å være.[125]

Ved vurderingen av nødvendigheten så må man også se på om andre opplysninger av mindre inngripende art for den registrerte kan gjøre samme nytte. Den registrerte skal ikke kunne identifiseres eller eksponerer i større grad enn nødvendig. [126]

Riktigheten

I bokstav (d) fremkommer det krav om at personopplysninger skal «være korrekte og om nødvendig oppdaterte; det må treffes ethvert rimelig tiltak for å sikre at personopplysninger som er uriktige med hensyn til formålene de behandles for, uten opphold slettes eller rettes».

Kravet innebærer at de opplysningene som lagres skal være korrekte. For å oppnå dette kravet kan det være hensiktsmessig å la den registrerte selv ha adgang til opplysningene slik at de eventuelt kan rette de selv.[127] I utgangspunktet handler kravet kun om riktigheten/kvaliteten på personopplysninger. [128] Av dette kravet kan det ifølge Schartum også utledes er krav om behandlingskvalitet. [129]

Lagringsbegrensning

I bokstav (e) stilles det krav om at opplysningene «lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for». Unntaksvis kan de behandles i lengre perioder «dersom de utelukkende vil bli behandlet for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1, forutsatt at det gjennomføres egnede tekniske og organisatoriske tiltak som kreves i henhold til denne forordning for å sikre de registrertes rettigheter og friheter».

[124] Schartum (2020) s.93
[125] l.c.
[126] l.c.
[127] Skullerud (2019) s. 175
[128] Schartum (2020) s. 93
[129] Ibid. s. 94

Dette kravet oppstiller et forbud mot å lagre opplysninger lengre enn nødvendig med tanke på formålet, [130] med unntak for de spesifikke tilfellene nevnt i forordningsteksten. Innholdet i kravet er at opplysningene skal slettes eller anonymiseres når/dersom formålet er oppnådd. [131]

Integritet og konfidensialitet

Personopplysninger skal «behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak» etter bokstav (f).

Dette prinsippet oppstiller et grunnleggende krav til at den behandlingsansvarlige skal sørge for tilstrekkelig sikkerhet for personopplysningene.[132] Overordet må behandlingsansvarlig sørge for at det ikke skjer uautorisert og ulovlig innsyn i opplysningene og beskyttelse mot tap, endring eller ødeleggelse av opplysningene.[133] Ifølge Schartum så må prinsippet ses i sammenheng med kapittel IV avsnitt 2 i GPPR om «Personopplysningssikkerhet».[134] Dette kapittelet oppstiller mer konkrete krav til informasjonssikkerhet.[135]

At prinsippet har fått en selvstendig betydning kan ha sammenheng med den teknologiske utviklingen. Denne har bidratt til at behandling av personopplysninger innebærer en økt risiko for brudd på konfidensialitet, integritet og tilgjengelighet.[136] Av ordlyden «tilstrekkelig» så innebærer imidlertid ikke kravet at behandlingen må være uten risiko, men hensynet til sikring må veies opp mot andre hensyn og behov.[137]

Ansvarlighet

Artikkel 5 nr. 2 oppstiller kravet til ansvarlighet. Den behandlingsansvarlige må kunne påvise at kravene i nr. 1 oppfylles. For å kunne påvise dette bør man ha et godt internkontrollsystem som beskriver hvilke opplysninger som behandles for hvilke formål og hvordan disse

[130] Skullerud (2019) s. 175
[131] l.c.
[132] Skullerud (2019) s. 176
[133] l.c.
[134] Schartum (2020) s. 98
[135] Skullerud (2019) s. 176
[136] l.c.
[137] Schartum (s. 98)

behandles.[138] Dette henger sammen med at man i utgangspunktet ikke trenger godkjenning fra myndighetene for å behandle personopplysninger. I stedet så må man som behandlingsansvarlig selv vurdere om behandlingen er i overensstemmelse med regelverket. Dette betyr at den behandlingsansvarlige har risikoen for eventuelle feilvurderinger.[139] Å dokumentere alle vurderingene man har foretatt er dermed viktig, fordi det er dette datatilsynet etterspør ved tilsyn.[140]

3.3.1 Prinsipper av spesiell betydning ved etterlevelse av hvitvaskingsloven

Enkelte av de grunnleggende prinsippene blir tidvis utfordret mer enn de andre i hvitvaskingsregelverket.[141] Her kommer det er kort forklaring på hvordan de kan utfordres.

Formålsbegrensingsprinsippet

Ettersom formålet til hvitvaskingsloven er styrende for intensiteten på tiltakene, så får formålsbegrensningsprinsippet en helt særegen stilling. Prinsippet har innvirkning på all lagring av personopplysninger ved at de skal tjene til å «å forebygge og avdekke hvitvasking og terrorfinansiering», jf. hvitvaskingsloven § 1. Alle opplysninger som innhentes i forbindelse med kundetiltak skal dermed i prinsippet holdes opp mot formålsbegrensingsprinsippet. Formålsprinsippet blir utfordret ved at hvitvaskingsregelverket enkelte steder legger opp til behandling utover det formålet tillater, og ved at det behandles store mengder opplysninger hvor trolig en del er overflødig.

Dataminimeringsprinsippet

Dataminimeringsprinsippet har også praktisk betydning ved etterlevelse av hvitvaskingsloven ettersom rapporteringspliktige er forpliktet til å innhente store mengder personopplysninger og ofte kan drive med såkalt «ekstra god etterlevelse» («goldplating»). Dette går ut på at rapporteringspliktige overoppfyller kravene i hvitvaskingsloven, og tidvis lagrer flere opplysninger enn hva loven krever.[142] Dette vil være i strid med dataminimeringsprinsippet som skal begrense antall opplysninger til det som er nødvendig med tanke på formålet med behandlingen.

[138] Skullerud (2019) s.176
[139] Schartum (2020) s. 100
[140] Skullerud (2019) s. 176
[141] European Data Protection Board (2021)
[142] Rui (2021) s. 234

Det er rettet kritikk mot hvitvaskingsreglene om at dette prinsippet ikke ivaretas godt nok. [143] Datatilsynet ønsker at det skal spesifiseres bedre i hvitvaskingsreglene hvilke typer opplysninger, for eksempel hvilke særlige kategorier og typer domfellelser, som kan samles inn i relasjon til de ulike tiltakene.[144]

Lagringsbegrensingsprinsippet

Lagringsbegrensningsprinsippet har betydning for den konkrete diskusjonen om hvor lenge opplysninger skal lagres. I hvitvaskingsloven er lagringstiden utvidet, og dette er i direkte klinsj med dette prinsippet.

Riktighet

Prinsippet om riktighet kommer først og fremst i spenning når rapporteringspliktige innhenter opplysninger fra tredjeparter og screener mot ulike typer «watchlists». Innhenting av opplysninger fra disse, kan bidra til større risiko for de registrertes rettigheter ettersom man ikke alltid har oversikt over hvilke typer opplysninger disse inneholder, og i hvilken grad disse er korrekte. Ettersom registrertes krav på innsyn og retting av personopplysninger, se kapittel 3.4, er begrenset, kan dette bidra til at rapporteringspliktige må iverksette ytterligere tiltak for å sikre riktigheten.

3.4 De registrertes rettigheter

De registrerte har fått en del rettigheter i personvernsregelverket som skal gjøre det enklere å få kontroll over egne opplysninger og få håndhevet rettighetene sine. I hvitvaskingsloven har noen av disse rettighetene blitt begrenset, fordi de vil forhindre oppnåelse av lovens formål. I dette delkapittelet skal det kort gjøres rede for noen av de mest sentrale rettighetene, hvordan man generelt kan begrense rettighetene og hvordan rettighetene ivaretas i hvitvaskingsregelverket.

Forordningen inneholder bestemmelser som skal sikre åpenhet og gjennomsiktighet ovenfor den registrerte personen.[145] Dette innebærer blant annet at den behandlingsansvarlige skal gi

[143] European Data Protection Board (2021)
[144] Datatilsynet (2020) s. 3
[145] Schartum (2020) s. 157

informasjon til den registrerte om behandlingen og at den registrerte får rett til å kreve innsyn i opplysninger.[146]

Det er i hovedsak artikkel 13,14 og 15 i forordningen som er aktuelle. Av disse kan det utledes at de registrerte skal få informasjon om kontaktopplysninger til den behandlingsansvarlige og eventuelt personvernombud og databehandlere mv., om formål og behandlingsgrunnlag for behandlingen. Dette er nødvendig for at den registrerte skal få mulighet til å håndheve rettighetene sine.[147] Det kan kreves innsyn i opplysninger, kategorier av opplysninger og kilder opplysningene er hentet fra. Uavhengig av hvem opplysningene er hentet inn fra, så skal det gis informasjon om lagringstid.[148]

Når det gjelder lagringstid er hovedregelen at personopplysninger skal slettes når de ikke lenger er «nødvendige for formålet som de ble samlet inn eller behandlet for», jf. GDPR art. 17 nr. 1 bokstav a). Dette er i samsvar med lagringsbegrensningsprinsippet som oppstiller et forbud mot å lagre opplysninger lengre enn det som er nødvendig med tanke på formålet. [149]

Etter art. 23 i forordningen kan man begrense de registrertes rettigheter i nasjonal rett. En forutsetning er at man samtidig «overholder det vesentligste i de grunnleggende rettighetene og frihetene og er […] nødvendig og forholdsmessig tiltak i et demokratisk samfunn». Paragraf 16 i personopplysningsloven gir adgang til dette for å ivareta hensyn som nevnt i bestemmelsens første ledd a-f.

3.4.1 Ivaretakelse av de registrertes rettigheter i hvitvaskingsloven

Ettersom hovedformålet med hvitvaskingsloven er å skaffe etterretningsinformasjon til myndighetene, så krever dette at hvitvaskingsloven enkelte steder må begrense de registrertes rettigheter for å oppfylle formålet. Som nevnt i kapittelet over er det en forutsetning for å kunne begrense rettighetene at det vesentligste i de grunnleggende rettighetene og frihetene til de registrerte er ivaretatt.

[146] Schartum (2020) s. 157
[147] Ibid. s. 164
[148] Ibid. s. 168
[149] Skullerud (2019) s. 175

I personopplysningsloven er det anledning til å begrense retten til innsyn for opplysninger som «det er påkrevd å hemmeligholde av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger», jf. første ledd bokstav b. Retten til innsyn er derfor begrenset i hvitvaskingsloven § 32. Dette har sammenheng med avsløringsforbudet i § 28 hvor ett av hovedformålene er å forhindre at eventuell straffeforfølgning vanskeliggjøres.[150] Det er dermed begrenset hva slags informasjon den rapporteringspliktige kan gi og hva han kan spørre kunden om for ikke å skape mistanke om undersøkelser.[151]

Det gjøres også unntak fra retten til å kreve personopplysninger slettet. Dette kan utledes av den rapporteringspliktiges plikt til å lagre opplysninger «fem år etter at kundeforholdet ble avsluttet eller transaksjonen ble gjennomført», jf. hvitvaskingsloven § 30 første ledd første punktum. Ved forsterkede kundetiltak ved avslutningen av kundeforholdet, så er lagringsplikten på ti år, jf. hvitvaskingsforskriften § 6-4.

Oppsummert kan man si at begrensningene i hvitvaskingsloven er nødvendige for å få oppfylt lovens formål. Forutsetningen for inngrep gjør seg allikevel gjeldende og innebærer at det uansett skal foreligge et tilstrekkelig vern av de registrertes grunnleggende rettigheter. Dette viser at begrensningene skaper et spenningsforhold til personopplysningsreglene. Om det er iverksatt kompenserende tiltak i hvitvaskingsloven er uklart. Om det er gjort så ivaretar trolig ikke disse de registrerte godt nok. Dette vil vi se eksempler på i neste kapittel.

4 Regler i hvitvaskingsloven som skaper et spenningsforhold til personvernreglene

Hvitvaskingsloven har bestemmelser som definerer hvilke personer den rapporteringspliktige er forpliktet til å innhente opplysninger om og i hvilken grad kundetiltak skal iverksettes. Enkelte av disse reglene er utformet relativt firkantet og skaper lite rom for risikobasert tilnærming. Dette bidrar til at hvitvaskingsloven enkelte steder kommer i et tydelig spenningsforhold med GDPR. Det skal derfor i det følgende gjøres rede for hvordan reglene om reelle rettighetshavere, politisk eksponerte personer og sanksjonsregelverket definerer hvem det skal innhentes opplysninger om og hvordan utformingen av disse reglene utfordrer personvernreglene.

[150] Rui (2021) s. 373

[151] Ibid. s. 344

4.1 Hvitvaskingsloven §§ 13 og 14 om reelle rettighetshavere

Paragraf 13 og 14 i hvitvaskingsloven angir når rapporteringspliktige skal innhente informasjon om reelle rettighetshavere og hvem som defineres som reell rettighetshaver i hvitvaskingsloven. Vurderingene i disse bestemmelsene vil være styrende for hvilke kundetiltak rapporteringspliktige må iverksette og dermed hva slags og hvor mange personopplysninger som må innhentes om de som regnes som reelle rettighetshavere.

Hvitvaskingsloven § 13 første ledd angir hvilke opplysninger som skal innhentes når kunden er en «juridisk person». Juridiske personer er ifølge lovkommentarene alle typer selskaper inkludert enkeltmannsforetak og stiftelse.[152] Videre er det en rekke juridiske arrangementer som ikke omfattes av definisjonen, men som allikevel skal anses som et subjekt etter hvitvaskingsloven. Disse arrangementene er for eksempel sameier, dødsbo under skifte, konkursbo, lag, foreninger, kommuner, fylkeskommuner, statsforetak, offentlige finansielle foretak og kommunale foretak.[153] Bestemmelsen gjelder også for utenlandske kunder som ikke er juridiske personer.[154]

Av hvitvaskingsloven § 13 første ledd, tredje punktum følger det at rapporteringspliktige må gjennomføre «egnede tiltak for å forstå eierskaps- og kontrollstrukturen i kunden». Denne plikten kan ses på som et utslag av KYC-prinsippet. Årsaken til at disse tiltakene skal gjennomføres er at forståelse for og kunnskap om selskapet gjør det enklere å oppdage mistenkelig aktivitet.[155] I tillegg blir det enklere å identifisere «reelle rettighetshavere», ettersom komplekse og uvanlige selskapsstrukturer kan være godt egnet for å skjule disse. [156]

Paragraf 2 bokstav e definerer en reell rettighetshaver som en «fysisk person som i siste instans eier eller kontrollerer kunden, eller som en transaksjon eller aktivitet gjennomføres på vegne av». I juridiske personer er det ikke nødvendigvis åpenbart hvem som eier eller kontrollerer selskapet. Det kan dermed være krevende å finne ut hvem som er reell rettighetshaver eller om

[152] Rui (2021) s. 214
[153] Ibid s. 214-215
[154] Rui (2021) s. 215
[155] l.c.
[156] Rui (2021) s. 216

det hele tatt finnes en i selskapet. [157] I § 14 er det gitt en bestemmelse som nærmere definerer hva som skal vurderes for å anse en fysisk person som en reell rettighetshaver for juridiske personer.

Det som overordnet må vurderes når man skal avgjøre reelt eierskap er «hvilke personer som har slik myndighet og kontroll at personen enten direkte eller indirekte kan kontrollere, styre eller påvirke kunden eller kundens midler, eventuelt selv er berettiget til midlene».[158] Denne vurderingsnormen er viktig å ha klart for seg, ettersom reglene er komplisert utformet og ikke nødvendigvis fanger opp det de opprinnelig er ment for.[159]

Først og fremst utvides personkretsen i første ledd første punktum. Bestemmelsen sier at det er en «fysisk person som alene eller sammen nære familiemedlemmer» som er reell rettighetshaver dersom videre vilkår er oppfylt. Dette betyr at dersom en person sammen med nære familiemedlemmer har kontroll over en kunde, så er man reell rettighetshaver. Årsaken til at man i norske regler har utvidet kretsen slik er at det skal forhindre omgåelse av reglene.[160] I lovkommentarene løftes dette frem som problematisk. [161] Det påpekes at utvidelsen ikke er forenlig med direktivets mål om like regler for antihvitvaskingsarbeid i EU/EØS-området og det bidrar til merarbeid for rapporteringspliktige. [162] Forfatterne konkluderer med at man bør ha en risikobasert tilnærming til undersøkelse av nære familiemedlemmer.

4.1.1 Direkte kontroll

Første ledd første punktum bokstav a pålegger den rapporteringspliktige å avgjøre om det er en «fysisk person alene eller sammen med nære familiemedlemmer» som eier «direkte eller indirekte» mer enn «25% av eierandelene (eks. aksjer, eierposter, andeler)» i en juridisk person. Ordlyden indikerer at dette er en absolutt terskel og dersom du eier mer enn 25% er du automatisk en reell rettighetshaver. Finanstilsynets rundskriv taler for at bestemmelsen skal forstås i samsvar med ordlyden.[163] Lovkommentaren problematisere dette. Forfatterne mener en slik

[157] Rui (2021) s. 216
[158] Tax Justice Network (2018) s.64
[159] Rui (2021) s. 232
[160] Prop. 40 L (2017–2018) s. 74
[161] Rui (2021) s. 230
[162] Rui (2021) s. 230
[163] Finanstilsynet (2019) s.33

forståelse ikke er forenlig med direktivet og at uttalelser i forarbeidene taler for at vurderingen her skal vær risikobasert, jf. § 6.[164] Å legge til grunn at alle som eier mer enn 25 % er reelle rettighetshavere vil kunne være i strid med det overordnede formålet med bestemmelsen som er å finne hvem som faktisk har kontroll over den juridiske personen, se vurderingstemaet ovenfor. Konsekvensen av å legge denne forståelsen til grunn er at man ikke ender opp med korrekt informasjon om hvem som faktisk har kontroll over den juridiske personen. Det er ikke slik at alle, alene eller sammen med familie, som har 25% eller mer av aksjene i et selskap kontrollerer det. En slik praktisering vil derfor bidra til at det blir mange flere registrerte enn nødvendig i rapporteringspliktiges antihvitvaskingsarbeid. Dette vil være er i strid med personopplysningsreglene.

Bestemmelsens første ledd, første punktum, bokstav b sier at rapporteringspliktige skal avgjøre om det er «fysiske personer, alene eller sammen med nære familiemedlemmer» som «på grunn av aksjer andeler eller medlemskap kontrollerer mer enn 25% av det totale antallet stemmer i den juridiske personen eller sammenslutningen». Dersom dette er tilfellet kan det være en *indikasjon* på reelt eierskap, [165] og innebærer ikke at personen automatisk regnes som en reell rettighetshaver.[166] Rapporteringspliktig må her vurdere hva eierskap av ulike aksjer i et selskap har å si for innflytelsen på stemmene. Informasjon kan hentes både fra aksjeeierboken og regnskapsdokumenter.[167]

Bestemmelsens første ledd første punktum bokstav c sier at rapporteringspliktige skal avgjøre om «fysiske personer, alene eller sammen med nære familiemedlemmer» har «rett til å utpeke eller avsette mer enn halvparten av den juridiske personens eller sammenslutningens styremedlemmer eller tilsvarende». Her vil eierandel eller stemmerettigheter på 50 % eller mer være en sterk indikasjon på reelt eierskap. Men som i bokstav a og b så vil ikke dette automatisk indikere at reelt eierskap er tilfellet.[168]

Bokstav a, b og c gir dermed indikasjoner på hvem som er reelle eiere. Dette innebærer at rapporteringspliktige må bruke mye skjønn i sine vurderinger. Det er trolig praksis for at disse

[164] Rui (2021) s. 232
[165] Rui (2021) s. 235
[166] l.c.
[167] l.c.
[168] Rui (2021) s. 236

stort sett blir standardiserte, noe som bidrar til registrering av personer som ikke har reelt eierskap. [169]

Bestemmelsens første ledd første punktum bokstav d sier at rapporteringspliktige skal avgjøre om «det er fysiske personer, alene eller sammen med nære familiemedlemmer» som «på grunn av avtale med eiere, medlemmer, den juridiske personen eller sammenslutningen, vedtekter eller tilsvarende, kan utøve kontroll i samsvar med bokstav a, b eller c». Dette kriterier er materielt, og innebærer at dersom vilkårene her er oppfylt, så anses personen som reell rettighetshaver.[170]

Bestemmelsens første ledd første punktum bokstav e sier at rapporteringspliktige skal avgjøre om «det er fysiske personer, alene eller sammen med nære familiemedlemmer» som «på annen måte utøver kontroll over den juridiske personen eller sammenslutningen». Ifølge lovkommentarene er denne bestemmelsen en omskrivning av § 2 bokstav e, og går verken lengre eller kortere enn denne. [171]

4.1.2 Indirekte kontroll

I bestemmelsens første ledd annet punktum angis hvem som er reelle rettighetshavere ved indirekte kontroll over en juridisk person.[172] Med indirekte kontroll menes «at reelle rettighetshavere ikke bare kan finnes i selskapet som vil bli kunde, men også i bakenforliggende selskaper som har eierandeler i selskapet som vil bli kunde».[173]

Bestemmelsen sier «Dersom en eller flere fysiske personer gjennom kontroll over en eller flere juridiske personer, stiftelser, utenlandske juridiske arrangementer eller andre sammenslutninger utøver kontroll over en annen juridisk person eller sammenslutning på en måte som angitt i første ledd» så anses den for å utøve kontroll over den stiftelsen elle juridiske personen som ønsker å bli eller er kunde. Bestemmelsen peker først tilbake til første ledd, første punktum, bokstav a til e som angir hvem som skal anses som reelle rettighetshavere ved direkte kontroll.

[169] Rui (2021) s. 233
[170] Rui (2021) s. 233
[171] Rui (2021) s. 237
[172] l.c.
[173] l.c.

Dermed bestemmes det at dersom det foreligger et direkte eierskap i et selskap (C) som har kontroll over et annet selskap (B), og det sistnevnte selskapet har kontroll over det selskapet som ønsker å bli kunde (A), så vil den reelle rettighetshaveren i C også bli regnet som å ha kontroll over A. Dette betyr at dersom en person sammen med nære familiemedlemmer eier 25, 1 % av aksjene i selskap C, så kan denne altså regnes som å ha kontroll over A.

Bestemmelsen er kritisert i lovkommentarene. [174] I lovkommentarene argumenteres det for at loven og forarbeidene er i uoverensstemmelsen med direktivet.[175] Og at det er gode grunner for at man skal fravike disse til tross for at alminnelige rettskildeprinsipper tilsier at det skal mye til for at dette kan gjøres. I direktivets artikkel 3(6)(a)(i) angis vurderingstemaet som å være «hvilken kontroll den fysiske personen har over kunden ved sitt indirekte eierskap».[176] Dette vurderingstemaet gjenspeiles ikke i bestemmelsen slik den er nå. Årsaken til kritikken er at forfatterne mener at både loven og forarbeidene er i direkte strid med direktivet. Selve formålet med å identifisere reelle rettighetshavere/fysiske personer som i realiteten eier eller kontrollerer kunden blir undergravd når de norske reglene er utformet som de er. [177] Som man ser av eksempelet ovenfor så skal man ikke ha en stor eierandel i et bakenforliggende selskap før man regnes som reell rettighetshavet for en kunde. Man får dermed verken identifisert de som faktisk er reelle rettighetshavere, i tillegg til at det registreres mennesker som ikke har noe kontroll over selskapet.[178]

I andre punktum fremkommer det krav om at opplysningene om reelle rettighetshavere «entydig» skal identifisere dem. Det kan gjøres unntak for dette i fjerde punktum dersom rapporteringspliktige etter å ha gjennomført «alle rimelige tiltak» mener det ikke finnes noen reell rettighetshaver, eller at det er tvil om at de som er identifisert er reelle rettighetshaver. Når det gjelder spørsmålet om hvor mye tids- og ressursbruk den rapporteringspliktig må legge ned for å bekrefte identitet, så sier lovkommentarene at for å finne ut dette må disse to reglene ses i sammenheng.[179] Det er dermed betydelig tids- og ressursbruk som må nedlegges, fordi

[174] Rui (2021) s. 239
[175] l.c.
[176] Rui (2021) s. 239.
[177] Rui (2021) s. 242.
[178] l.c.
[179] Rui (2021) s. 219.

unntaksbestemmelsen er snever. [180] Videre påpekes det at selv om forarbeidene mener at de rapporteringspliktige skal ha en risikobasert tilnærming til identifisering,[181] så er ikke dette praktisk mulig. Uansett risiko, må man følge kravet som loven oppstiller som er å gjennomføre «alle rimelige tiltak».[182]

I tredje punktum kreves det gjennomførelse av «egnede tiltak» for å bekrefte reelle rettighetshaveres identitet. Ordlyden kan tilsi at dette innebærer en risikobasert tilnærming hvor det i enkelte tilfeller kan være tilstrekkelig å kun spørre kunden eller den reelle rettighetshaveren om identitet. I Prop. 40 L (2017-2018) punkt 5.4.6.3 fremkommer det at det ikke er tilstrekkelig å kun spørre kunden. Informasjonen må også bekreftes av «egne opplysninger». Det er åpent hva dette uttrykket innebærer. Lovkommentarene antar at det holder å verifisere opplysningene opp mot offentlige registre om eierforhold og eventuelt aksjonæravtaler, og andre underliggende avtaler om at en fysisk person eier eller kontrollerer kunden.[183] Dersom det foreligger høy risiko må man vurdere om det er nødvendig å innhente flere opplysninger om reell rettighetshaver enn kun identitet.[184]

Den 1. november i år trådte lov om register over reelle rettighetshavere delvis i kraft. Forhåpentligvis skal denne bidra til å forenkle prosessen med å kartlegge reelle rettighetshavere. Hvitvaskingsloven og denne loven opererer med noe ulike definisjoner. Den nye loven krever ikke identifisering av nære familiemedlemmer og kravene til eierandel er høyere for å anse noen for å ha indirekte kontroll over en kunde.[185] Hvitvaskingsloven har dermed en strengere tilnærming, som gjør at rapporteringspliktige fortsatt må gjennomføre alle vurderingene som nevnt ovenfor på selvstendig grunnlag.

4.1.3 Hvordan utfordrer reglene om reelle rettighetshavere personvernreglene?

Redegjørelsen viser at det er omfattende og noe kompliserte krav til hvordan rapporteringspliktige skal identifisere reelle rettighetshavere. I tillegg er reglene utformet slik at de pålegger

[180] NOU 2016: 27 s. 83.

[181] Prop. 40 L (2017-2018) s. 72.

[182] Rui (2021) s. 219.

[183] Rui (2021) s. 220

[184] Ibid. s. 221

[185] Personlig kommunikasjon i samtale med Gunnar Holm Ringen, advokat og statsautorisert revisor i PWC 10. november 2021.

rapporteringspliktige å definere mennesker som ikke har avgjørende kontroll over kunden som reelle rettighetshavere. Dette innebærer at en del av de som regnes som reelle rettighetshavere etter hvitvaskingsloven, ikke nødvendigvis utgjør noen risiko for hvitvasking i relasjon til rapporteringspliktiges kunder. Når disse personene ikke har anledning til å hvitvaske penger via kunden, så vil ikke opplysninger om denne personen kunne tjene som etterretningsinformasjon. Å lagre personopplysninger om disse vil dermed være ulovlig, siden rapporteringspliktige ikke har tilstrekkelig behandlingsgrunnlag.

Rekkevidden av behandlingsgrunnlaget i hvitvaskingsloven begrenses til å oppfylle lovens forpliktelser. Disse forpliktelsene har alle som formål «å forebygge og avdekke hvitvasking og terrorfinansiering», jf. § 1. Det kan dermed tenkes at definisjonsbestemmelsene heller ikke tjener til å oppfylle hvitvaskingslovens formål. De skaper unødvendig merarbeid for de rapporteringspliktige når de må innhente opplysninger om mennesker som er «irrelevante» i deres hvitvaskingsarbeid.

Den største og mest alvorlige personvernkonsekvensen er dermed at enkelte som har en eierandel i et selskap uten reell innflytelse og deres nære familiemedlemmer, får behandlet sine personopplysninger uten at det foreligger et behandlingsgrunnlag. Som nevnt i kapittel 3.2.3 om behandlingsgrunnlag, er dette en forutsetning for at behandling av personopplysninger skal være lovlig. I tilfellene hvor det samles inn opplysninger uten grunnlag vil dermed ikke risikoreduserende tiltak være tilstrekkelige etter personopplysningsreglene. Når behandlingen i utgangspunktet er ulovlig så krever reglene at personopplysningene skal slettes, jf. art. 17 nr. 1 bokstav d.

I tilfellene hvor det lagres opplysninger om reelle rettighetshavere som har reell innflytelse på selskapet vil dette også kunne ha konsekvenser for personopplysningsvernet. Konsekvensen av å være reell rettighetshaver er at de rapporteringspliktige må gjennomføre kundetiltak ovenfor de registrerte. Dette innebærer at det skal innhentes og registreres en rekke opplysninger om disse personen og fortsette å verifisere disse opplysningene underveis i kundeforholdet, jf. §§ 13 og 24. Hvilke opplysninger som skal innhentes følger av § 13 tredje ledd, andre punktum. Her fremkommer det at opplysningene «skal entydig identifisere den eller de reelle rettighetshaverne» som er identifisert etter § 14. I finanstilsynets rundskriv presiseres det at navn, adresse og fødselsdato normalt vil være tilstrekkelig for å oppfylle kravet, men at det allikevel må gjøres

en konkret risikovurdering.[186] I lovkommentarene fremkommer det at det ofte også bør innhentes informasjon om statsborgerskap og bostedsland, siden det gjør opplysningene mer presise og kan si noe om risikoen.[187] Det avgjørende er imidlertid at man kan skille den registrerte fra andre personer.[188]

Reglene om hvilke opplysninger som skal innhentes for reelle rettighetshavere er mer skjønnsmessig utformet sammenliknet med for eksempel hvilke opplysninger som må innhentes for fysiske personer som er kunder, jf. § 12. Dette fører til at rapporteringspliktige i større grad må avgjøre selv hva som er tilstrekkelig mengde opplysninger, noe som kan bidra til at det innhentes flere opplysninger enn nødvendig for å sikre at lovens krav er oppfylt.[189] En praksis som dette er også med på å skape et spenningsforhold til personopplysningsreglene. Det er krav om at innhentede opplysninger skal begrenses til det som er nødvendig holdt opp imot formålet med behandlingen, jf. formålsbegrensningsprinsippet og dataminimeringsprinsippet. Dersom det innhentes opplysninger for å være «på den sikre siden» av hvitvaskingsloven kan det dermed bidra til at man kommer i uoverensstemmelse med personopplysningsreglene.

Ettersom hvilke kundetiltak som iverksettes beror på hva slags risiko kunden utgjør, så vil risikoen være styrende for hva slags opplysninger som må innhentes om reelle rettighetshavere og intensiteten på den etterfølgende overvåkingen, jf. § 24. Når denne risikoen er høy vil det stilles krav om at rapporteringspliktige må gjennomføre flere tiltak for å bli kjent med kunden, jf. § 17. I denne bestemmelsen om forsterkede kundetiltak fremkommer det at i tillegg til å oppfylle grunnkravene til innhenting av opplysninger, må det iverksettes «ytterligere nødvendige tiltak for å sikre kjennskap om kunden, reelle rettighetshavere og kundeforholdets formål og tilsiktede art». Dette bidrar til at det er enda flere skjønnsmessige vurderinger som må gjennomføres av rapporteringspliktige, som utgjør en enda større risiko for de registrertes rettigheter. Forutsatt at rapporteringspliktige har lovlig grunnlag for å behandle opplysningene i disse tilfellene, vil imidlertid høyere risiko for hvitvasking bidra til at formålet med behandlingen i større grad blir oppfylt. Jo høyere risiko for hvitvasking, desto mer vil opplysningene kunne avdekke hvitvasking. Det som er viktig er at rapporteringspliktige i disse situasjonene iverksetter risikoreduserende tiltak. For selv om man er innenfor formålet, så lagres det flere opplysninger og muligens

[186] Finanstilsynet (2019) s. 31
[187] Stenbeck (2021) § 13 note 4
[188] Finanstilsynet (2019) s. 31
[189] Rui (2021) s. 234

flere kategorier av opplysninger som bidrar til større risiko for den registrertes grunnleggende rettigheter, se kapittel 2.2. Ettersom de registrertes rettigheter etter personopplysningsreglene er begrenset i hvitvaskingsloven, så kan dette tale for at det bør være enda strengere krav til å iverksette tiltak for å sørge for tilstrekkelig vern av deres grunnleggende rettigheter.

Risikoprinsippet gjelder også for myndighetenes tiltak. [190] Når de gir lovregler som § 14, så kan man argumentere for at det ikke iverksettes tiltak som tjener til å kartlegge og avdekke hvitvasking. Når reglene ikke tjener til dette, så kan det tenkes at etterlevelse av § 14 bidrar til brudd på § 6 om risikoprinsippet for rapporteringspliktige. I tillegg vil korrekt etterlevelse av § 14 bidra til at rapporteringspliktige behandler personopplysninger ulovlig. De rapporteringspliktige settes dermed i en vanskelig situasjon hvor de risikerer høye bøter både fra Finanstilsynet og Datatilsynet. Det kan virke som at det er få eller ingen tiltak rapporteringspliktige selv kan gjøre for å ikke havne på kanten med loven på den ene eller andre måten i disse situasjonene.

4.2 Politisk eksponerte personer, jf. § 13 fjerde ledd

I § 13 fjerde ledd første punktum er det krav om at rapporteringspliktige skal ha «systemer for å avgjøre om «personer som kan handle på vegne av kunden eller er gitt disposisjonsrett over en konto eller et depot, eller reell rettighetshaver» er «politisk eksponert person eller nært familiemedlem eller kjent medarbeider til en politisk eksponert person». Årsaken til at man skal kartlegge politisk eksponerte personer er at disse kan utgjøre en forhøyet risiko for korrupsjon og at det dermed stilles krav om at disse skal underlegges forsterkede kundetiltak, jf. § 18 fjerde ledd.[191]

Hvem som regnes som politisk eksponert person fremkommer av § 2 bokstav f. Her defineres en politisk eksponert person som en som «innehar eller har innehatt en stilling eller et verv som» som 1. «statsoverhode, regjeringssjef, minister eller assisterende minister», 2. medlem av nasjonalforsamling», 3. «medlem av styrende organ i politisk parti», 4. medlem av høyere rettsinstans som treffer beslutning som ikke eller bare unntaksvis kan ankes», 5. «medlem av styre i riksrevisjon, revisjonsdomstol eller sentralbank», 6. «ambassadør, chargé d'affaires eller militær offiser av høyere rang», 7. «medlem av administrativt, ledende eller kontrollerende organ

[190] Rui (2021) s. 234

[191] Finanstilsynet (2019) s. 46

i statlig foretak» og 8. «medlem av administrativt, ledende eller kontrollerende organ i statlig foretak».

Av formuleringen fremkommer det at både noen som innehar og har hatt en stilling som er definert i bokstav f regnes som en politisk eksponert person. Forsterkede kundetiltak skal gjennomføres «i minst ett år etter at den politiske eksponerte personen avsluttet stillingen eller vervet», jf. § 18 fjerde ledd. Dette innebærer at man må ha en risikobasert tilnærming til fortsettelse av forsterkede kundetiltak når det er gått mer enn ett år siden personen fratrådte sitt verv eller stilling.[192]

Ettersom det i norsk rett er utvidet hvem som er reell rettighetshaver, så medfører dette at kartleggingen av hvem som er «politisk eksponert person eller nært familiemedlem eller kjent medarbeider til en politisk eksponert person» også blir mer omfattende. Hvitvaskingsloven går på dette punktet lengre enn direktivet ved at man må ta stilling til om personer som handler på vegne av kunden og personer som er gitt disposisjonsrett over konto eller depot er PEP. I direktivet skal man kun kartlegge dette for kunden og reelle rettighetshavere.[193] Departementet har ikke begrunnet hvorfor loven går lengre enn direktivet, og forfatterne av lovkommentarene stiller seg skeptiske til denne utvidelsen.[194] De skriver at denne utvidelsen sammenholdt med utvidelsen av hvem er som er reell rettighetshaver er i direkte strid med risikoprinsippet.[195] Som ledd i en risikobasert tilnærming kan man ikke utelukkende se på lovens definisjoner for PEP i kartlegging av hvem som kan utgjøre forhøyet risiko for blant annet korrupsjon. Personer som ligger tett opptil definisjonen kan også utgjøre økt risiko, og dermed må man ta konkret stilling til om det er nødvendig med forsterkede kundetiltak for disse, jf. § 6.

Det tilbys en rekke kommersielle PEP-lister som rapporteringspliktige kan abonnere på. Av både forarbeidene og finanstilsynets rundskriv fremkommer det at det ikke er noen plikt til å abonnere på disse. Først og fremst fordi det ikke er ønskelig å oppstille et slikt krav når ikke det er staten selv som lager listene. [196] [197] Listene har heller ikke så god troverdighet. De gir

[192] Finanstilsynet (2019) s. 46-47
[193] Rui (2021) s. 223
[194] l.c.
[195] Rui (2021) s. 224
[196] NOU 2016:27 s. 83
[197] Finanstilsynet (2019) s. 49

mange falske treff og flere personer som er politisk eksponerte er ikke listet opp. Falske treff utgjør til sammen litt over 50 % av alle treff i rapporteringspliktiges overvåkningssystemer. Dette bidrar til at det må brukes en del ressurser på å finne ut av disse varslene, noe som gjør hvitvaskingsarbeidet mindre effektiv og dermed i strid med risikoprinsippet.[198]

PEP-listene inneholder også mer personopplysninger enn hva både direktivet, hvitvaskingsloven og personvernforordningen gir adgang til å behandle.[199] Dette har å gjøre med varierte definisjoner av hva som er en politisk eksponert person internasjonalt. Variasjonen gjør at det er opplistet flere personer enn hva som er definert som politisk eksponert person i EU og Norge på listene. I Norge har Digital Samhandling Offentlig Privat startet med å lage liste med personer som anses som nasjonale PEP-er.[200] Dette vil forhåpentligvis bidra til at arbeidet med kartleggingen blir mer effektiv og innenfor gjeldende regelverk nasjonalt.

Et spørsmål som blir reist om PEP-regelverket i lovkommentarene er om det er proporsjonalt utformet. [201] Det bli fremhevet at reglene er ganske firkantede, i likhet med reglen om reelle rettighetshavere, og at dette bidrar til å undergrave risikoprinsippet og forhindre formålstjenlig ressursbruk.[202] Det kreves mye ressurser for rapporteringspliktige å etterleve kravene, i tillegg til at problematikken rundt PEP-listene som nevnt ovenfor løftes frem. Det er også usikkert om reglene i det hele tatt bidrar til å forebygge og avdekke hvitvasking.[203] Det er ikke avdekket diktatorer eller depoter som har plassert korrupte midler i Europa de siste årene, og ifølge tyske undersøkelser er det veldig få mistenkelige forhold som kan tilbakeføres til politisk eksponerte personer.[204] Det stilles dermed spørsmål ved om dette bidrar til at regelverket virker mot sin hensikt, fordi det nedlegges masse ressurser på å avdekke hvitvasking på et område hvor det muligens ikke er størst risiko for at det skjer.[205]

4.2.1 Hvordan utfordrer PEP-reglene personvernreglene?

[198] Rui (2021) s. 225
[199] l.c.
[200] Rui (2021) s. 82
[201] Rui (2021) s. 84
[202] l.c.
[203] l.c.
[204] l.c.
[205] l.c.

Følgen av å bli definert som PEP er som nevnt at rapporteringspliktige er forpliktet til å gjennomføre forsterkede kundetiltak for disse personene, jf. § 18 første ledd. Dette innebærer at det må «iverksettes ytterligere nødvendige tiltak for å sikre kjennskap om kunden, reelle rettighetshavere og kundeforholdets formål og tilsiktede art», i tillegg til de alminnelige opplysningene, jf. § 17 andre ledd. Følgen er dermed at disse personene blir satt under strengere overvåking. Dette bidrar mest sannsynlig til økt risiko for den registrertes rettigheter ettersom det lagres mer opplysninger og graden av overvåkning blir høyere.

Definisjonen av reelle rettighetshavere har også betydning for reglene om PEPer. Utvidelsen bidrar til at personer som er PEPer og har en eierandel i et selskap uten å utøve kontroll over denne, blir definert som en reell rettighetshaver. Ettersom de er PEPer blir de dermed satt under forsterkede kundetiltak. Dette fremstår, som nevnt i kapittel 4.1.3, som vilkårlig og ulovlig behandling av personopplysninger.

Usikkerheten om reglene om politisk eksponerte personer er effektive, har betydning for diskusjonen om hvitvaskingsloven gir tilstrekkelig behandlingsgrunnlag. Som nevnt er årsaken til at det foreligger en spesialregel for politisk eksponerte personer at de utgjør en forhøyet risiko for korrupsjon og dermed hvitvasking. Når man er usikker på om dette faktisk stemmer eller om det kun er en hypotese, er det ikke sikkert at reglene tjener til å oppfylle hvitvaskingslovens formål. Dersom de ikke gjør det, gir heller ikke loven nødvendig behandlingsgrunnlag for disse opplysningene.

Ettersom PEPlistene som tilbys også inneholder personopplysninger i større grad enn hva EU og norsk rett tillater, er det problematisk for personvernet at disse benyttes. Her vil både kravet til riktighet, formålsbegrensningsprinsippet, lagringsbegrensningsprinsippet og dataminimeringsprinsippet kunne spille inne. Dette bidrar mest sannsynlig til merarbeid og ekstra anstrengelser for den rapporteringspliktige, ettersom disse prinsippene stiller krav til at man både må undersøke om opplysningene er korrekte, om de tjener til å oppfylle hvitvaskingslovens formål og eventuelt må slettes, og om enkelte av opplysningene må slettes fordi man har for mange opplysninger. I tillegg vil som nevnt en del av disse listene inneholde opplysninger som behandlingsansvarlige ikke har lov til å behandle. Bruk av disse utgjør dermed tilsynelatende en høy risiko for de registrertes rettigheter, som setter krav til at den rapporteringspliktige må iverksette tiltak for å minimere denne.

4.3 Hvitvaskingslovens regler mot terrorfinansiering og sanksjonsregelverket

En annen side av hvitvaskingsregelverket handler om terrorfinansiering. Det er de samme kravene til risikoklassifisering, undersøkelser, oppfølging og rapportering for å avdekke terrorfinansiering som for hvitvasking.[206] Dette innebærer at det her også innhentes stores mengder personopplysninger. I relasjon til oppgavens tema så er det behandlingsgrunnlaget for særlige kategorier av personopplysninger og straffedommer som skaper et spenningsforhold til personopplysningsreglene.

I forbindelse med terrorfinansiering så må de rapporteringspliktige også forholde seg til sanksjonsregelverket.[207] Sanksjonsregelverket består av tre komponenter: FN-loven, sanksjonslova og politiloven §§ 17 g til 17 i. [208] Det er Utenriksdepartementet som håndhever de to første og PST og domstolene som håndhever det siste.[209]

Tiltakene som kreves etter sanksjonsregelverket går ut på å fryse transaksjoner eller å båndlegge formuesgoder som tilhører en bestemt person eller foretak.[210] For å finne ut om man har kunder dette skal gjøres ovenfor, så må man screene egen kundedatabase mot sanksjonslistene. Det er først og fremst FNs konsoliderte sanksjonsliste som gjelder direkte som norsk rett,[211] men det screenes imidlertid også mot EU sine sanksjonslister.[212] Det fremkommer av veilederen for screening mot sanksjonslister at rapporteringspliktige som minimum skal screene kundens eller rolleinnehaverens navn mot listene. Dersom man får treff på listen, så kan det være aktuelt å screene annen informasjon som fødselsdato, statsborgerskap, adresse mv. [213]

[206] Rui (2021) s. 67
[207] l.c.
[208] l.c.
[209] Rui (2021) s. 69-71
[210] Clausen (2020)
[211] Lovkommentarer hvitvasking (s. 68)
[212] Clausen (2020)
[213] Clausen (2020)

Dersom rapporteringspliktige ikke iverksetter tiltakene som sanksjonsregelverket krever ovenfor listeførte personer, så kan den rapporteringspliktige bli straffet og møtes med inndragning.[214] Rapporteringspliktige har dermed ikke noe valg om å følge disse reglene eller ikke.

Selv om norske rapporteringspliktige kun er forpliktet av de delene av sanksjonsregelverket som er nevnt ovenfor, så er det praksis at det også screenes mot lister som ikke er en del av norsk rett. Dette gjelder spesielt amerikanske lister. Disse sanksjonslistene har ekstraterritoriell virkning og brudd på disse kan medføre sanksjoner. Sanksjonene kan innebære at rapporteringspliktige ikke får gjennomført transaksjoner i dollar eller blir stengt ute fra markeder i andre tredjeland.[215] [216] Å ikke screene mot disse listene og iverksette tiltak kan dermed innebære store konsekvenser for de rapporteringspliktige.

4.3.1 Hvordan utfordrer sanksjonsreglene personvernreglene?

Sanksjonsregelverket er et selvstendig regelverk fra hvitvaskingsreglene. Rapporteringspliktige må imidlertid etterleve begge to. Dersom det oppstår treff i sanksjonslistene, så må rapporteringspliktige foreta nærmere undersøkelser etter hvitvaskingsloven § 25.[217] Dette i seg selv er ikke nødvendigvis problematisk for personopplysningsvernet. En forutsetning er imidlertid at man har tilstrekkelig behandlingsgrunnlag- og formål for å behandle opplysningene disse listene innebærer. Når det gjelder lister som for eksempel de amerikanske, så skaper dette imidlertid større utfordringer. Disse listene kan innebære personopplysninger i større omfang enn hva norsk rett og EU/EØS-retten tillater.[218]

I artikkelen «Personvern og tiltak mot hvitvasking: – Særlig om screening mot sanksjonslister»[219] problematiseres det om det bør gis klarere hjemler for nettopp å screene individer mot tredjestaters sanksjonslister.[220] Dette behovet henger sammen med at for rapporteringspliktige som for eksempel banker, så kan det innebære store konsekvenser å ikke screene mot for

[214] Rui (2021) s. 68
[215] Ibid. s.73
[216] Clausen (2020)
[217] Rui (2021) s. 75
[218] Ibid. s. 73
[219] Clausen (2020)
[220] Clausen (2020)

eksempel amerikanske lister. På grunn av dette er det vanlig praksis at det screenes til tross for usikkert hjemmelsgrunnlag, fordi gevinsten trolig er større å gjøre det enn å ikke gjøre det.[221]

Årsaken til at det er usikkerhet rundt hjemmelsgrunnlaget er at listene kan inneholde både særlige kategorier av personopplysninger, jf. GDPR art. 9 og informasjon om «straffedommer, lovovertredelser eller tilknyttede sikkerhetstiltak», jf. GDPR art. 10. Dette innebærer opplysninger om straffedommer, i tillegg kan det diskuteres om de også inneholder opplysninger om religiøs og politisk overbevisning.

Her er noe av diskusjonen tatt opp i kapittel 3.2.4 om behandlingsgrunnlag for behandling av særlige kategorier personopplysninger i hvitvaskingsloven relevant. Det er generelt kritisert at behandlingsgrunnlaget for disse ikke i stor nok grad ivaretar de registrertes rettigheter og dermed er i strid med GDPR. Når dette er utgangspunktet så gir trolig ikke hvitvaskingsloven adgang til å behandle opplysninger fra disse sanksjonslistene. Dette er problematisk fordi det anses som praktisk viktig for rapporteringspliktige å få screenet i disse tilfellene. Artikkelen ovenfor sier at det antakeligvis ikke er meningen at personopplysningsreglene skal begrense norske selskapers mulighet til å handle i utenlandske markeder. I tillegg så har Datatilsynet ved flere anledninger gitt midlertidige tillatelser til selskaper for å behandle opplysninger i disse tilfellene. Dette tyder på at det er stort behov for screening, og kompetente myndigheter har tidvis ment at dette bør tillatelse. Siden behandling av særlige kategorier i disse tilfellene er nødvendig, samtidig som at behandlingen utgjør en større risiko for de registrertes rettigheter, kan det tenkes at et veloverveid behandlingsgrunnlag er nødvendig. Dette vil bidra til at behandlingen skjer innenfor satte rammer, som vil gi større forutsigbarhet for de registrerte.

5 Hvordan kan hvitvaskingsregelverket harmoniseres bedre med GDPR?

Som drøftelsene ovenfor viser, skaper hvitvaskingsreglene et spenningsforhold til personvernreglene. Det at loven har et tilsynelatende utilstrekkelig behandlingsgrunnlag for særlige kategorier av personopplysninger, innskrenker de registrertes rettigheter og har definisjonsbestemmelser som pålegger rapporteringspliktige å behandle personopplysninger uten tilstrekkelig

[221] Rui (2021) s. 73

grunnlag skaper dette. Loven gir heller ikke inntrykk av å ha fokus på eller sette krav til at rapporteringspliktige skal iverksette kompenserende tiltak for å jevne ut dette. Gjennomgående bærer hvitvaskingsregelverket dermed preg av å ikke være samkjørt med eller ta i betraktning kravene som GDPR og personopplysningsloven stiller. Det er der norsk rett fraviker direktivet, hvor det kan sies at risikoprinsippet ikke er gjennomført i sin helhet og hvor det ligger mye skjønn til de rapporteringspliktige, som gjennomgående bidrar til dette helt grunnlegge spenningsforholdet.

Dersom man ser tilbake innledningsvis om de grunnleggende formålene og rettskildene for hvitvaskingsregelverket og personopplysningsreglene, så angir disse avveininger som lovverkene skal gjenspeile. Siden hvitvaskingsregelverket i stor grad er basert på at rapporteringspliktige må innhente store mengder personopplysninger, så forutsetter dette at det er harmonisert med personopplysningsloven og GDPR. Grunnleggende innebærer dette regelverket må gjenspeile en forholdsmessig avveining av retten til privatliv og samfunnet interesse i å bekjempe økonomisk kriminalitet.

I dette kapittelet vil det drøftes hvordan hvitvaskingsregelverket bør balanseres på ulike nivåer for at det skal bli mer velbalansert med personopplysningsreglene. Drøftelsen tar utgangspunkt i uttalelser og kritikk fra EDPB og Datatilsynet, ettersom disse bør anses som de best kvalifiserte til å vurdere kvalitet på personopplysningsvern.

European Data Protection Board

Som nevnt har EDPB satt som et mål for 2021-2023 at tiltak etter hvitvaskingsdirektivene skal være i tråd med retten til privatliv og personvernbeskyttelse etter charteret.[222] Man ser gjennomgående at de europeiske personvernmyndighetene er kritiske til regelverket når det skal gjøres endringer.

Allerede ved fremleggelsen av forslaget til det fjerde hvitvaskingsdirektivet kritiserte det europeiske personverntilsynet (The European Data Protection Supervisor) definisjonen av reelle rettighetshavere for å utfordre personvernreglene.[223]

[222] European Data Protection Board (2020)

[223] European Data Protection Supervisor (2017)

Den 15. desember 2020 kom det en uttalelse fra EDPB om at oppdateringer av hvitvaskingsregelverket ikke bør gjennomføres uten en gjennomgang av forholdet mellom hvitvaskingstiltak og retten til privatliv og personopplysningsvern.[224] De påpeker misforholdet og ber om å bli involvert tidlig i prosessen når oppdateringer skal foretas.

Den 7. mai 2021 kom det enda uttalelse fra EDPB i et såkalt «letter», hvor de igjen påpeker ubalansen mellom hvitvaskingsregelverket og GDPR. Det uttales spesielt at prinsipper om nødvendighet og proporsjonalitet, dataminimering, kravet til riktighet og lagringsbegrensning bør tas i betraktning for ethvert steg i gjennomførelsen av reglene for å sikre at antihvitvaskingstiltakene er i tråd med kravene etter artikkel 7 og 8 i EU charteret.

Det poengteres at det har vist seg vanskelig for rapporteringspliktige å selv foreta vurderingene av hvitvaskingstiltak i tråd med risikoprinsippet, fordi dette ikke er klart nok definert i lovgivningen eller at det er manglende oppfølging av tilsynsmyndighetene.[225] Et resultat av dette er at det innhentes for mye informasjon som ikke tjener til å avdekke hvitvasking og terrorfinansiering. Som vist tidligere i oppgaven, har risikovurderingene i hvitvaskingsloven direkte sammenheng med formålet for behandlingen av personopplysninger. En følge av dette, ifølge rådet, er dermed at praktiseringen av den risikobaserte tilnærmingen etter dagens hvitvaskingsregelverket fører til et ubalansert forhold med personopplysningsregelverket.[226] Til slutt i brevet så kommer de også med en uttalelse om at dersom ikke hvitvaskingsregelverket blir bedre harmonisert med GDPR, så vil de respektive myndighetene som håndhever personopplysningsreglene bli tvunget til å bruke deres makt for å få rapporteringspliktiges tiltak i overensstemmelse med forordningen. [227]

Dette viser at det foreligger en ubalanse mellom de to regelverkene på et helt grunnleggende nivå. Siden både hvitvaskingsreglene og personopplysningsreglene er basert på EU-regelverk, og Norge via EØS-avtalen er forpliktet til å følge forordninger og direktivet, så er det en forutsetning av disse reguleringene er velbalanserte før de skal gjennomføres. Dette vil trolig få betydning for hvordan de norske reglene blir utformet.

[224] European Data Protection Board (2020)
[225] European Data Protection Board (2021) s. 3
[226] European Data Protection Board (2021) s. 3
[227] European Data Protection Board (2021) s. 7

Datatilsynet

For å gjennomføre det femte hvitvaskingsdirektivet i norsk rett, så foregår det en høringsrunde.[228] Datatilsynet har som nevnt avgitt et høringssvar hvor de er kritiske til noe av reguleringene i hvitvaskingsloven, men ikke i like stor grad som EDPB.

Datatilsynet er først og fremst kritiske til hjemmelen for å lagre særlige kategorier av personopplysninger.[229] Behandlingsgrunnlaget for særlige kategorier er fastsatt i forskrift. Datatilsynet sier at det ikke er noe i veien for å gi en unntakshjemmel til å lagre særlige kategorier av personopplysninger i forskrift, men dette forutsetter at «hjemmelen må stå i rimelig forhold til det mål som søkes oppnådd og være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger».[230] Denne forutsetningen mener de ikke er oppfylt og kommer deretter konkrete tiltak som vil bringe loven i bedre overensstemmelse med personopplysningsreglene.[231]

For å overholde kravene som nevnt, så mener Datatilsynet at det bør presiseres hvilke opplysninger man kan behandle til hvilke formål, og gi eksempler på situasjoner hvor man ikke kan behandle enkelte opplysninger. Dette kommer av at det innhentes store mengder personopplysninger ved overholdelse av hvitvaskingsreglene, og prinsippene om proporsjonalitet og dataminimering derfor står svært sentralt. [232]

Det er i høringsnotatet foreslått en plikt til å ha en rutine for lagring av særlige kategorier. Denne fremkommer allerede av hvitvaskingsforskriften § 6-1 (2). Datatilsynet mener at det bør vurderes «om den foreslåtte plikten til å ha en rutine for en slik behandling er tilstrekkelig tiltak for å sikre de registrertes rettigheter».[233] De peker videre på §§ 6-8 i hvitvaskingsloven som og sier at disse bestemmelsene angir konkret hvordan risiko skal håndteres og hvilke krav som stilles til dette for hvitvaskingstiltak. De mener lignende krav kan stilles til behandling av personopplysninger og peker spesielt på § 8 som gjelder utforming av rutiner.

[228] Finansdepartementet (2019)
[229] Datatilsynet (2020) s. 2
[230] l.c.
[231] Datatilsynet (2020) s. 3
[232] Datatilsynet (2020) s. 3
[233] Datatilsynet (2020) s. 4

Finanstilsynet har på sine side uttalt at det er behov for en klar hjemmel for behandling av særlige kategorier, men anser det ikke hensiktsmessig å gi en avgrenset og uttømmende liste for hvilke kategorier og når i kundeforholdet man kan behandle disse. [234]

Hva skal til for bedre harmonisering?

Som nevnt innledningsvis om risikobaserte regelverk, så flyttes risikoen for vurderingene fra myndighetene over på de forpliktede. Som EDPB påpeker, kan dette vise seg å være vanskelig å håndtere. Når det utarbeides slike regelverk, kan man dermed stille spørsmål om hvor mye risiko statene kan flytte over på de forpliktede. Dette bør trolig avhenge av hva slags risiko det er snakk om. Risikovurderingen i hvitvaskingsregelverket kan trolig være godt egnet isolert sett. Når regelverket forutsetter et annet risikobasert regelverk som personopplysningsreglene, blir det mer komplisert. Som vist i kapittel 2 er det sammenheng mellom de to risikoene. Å legge ansvar ukritisk over på rapporteringspliktige kan dermed fremstå som uforsvarlig av staten. Det må derfor vurderes konkret når dette bør gjøres.

I lovkommentarene nevnes definisjonsbestemmelsen av reelle rettighetshavere som en av bestemmelsene i loven hvor risikoprinsippet ikke er fullstendig gjennomført.[235] I denne bestemmelsen vil gjennomføring kunne bidra til bedre harmonisering. Formålet med hvitvaskingsloven, som også er behandlingsformålet vil være styrende for hvem det er aktuelt å innhente opplysninger om. Her vil det å ikke gjennomføre prinsippet gi store personvernskonsekvenser, siden det bidrar til ulovlig behandling i enkelte tilfeller. I slike definisjonsbestemmelser vil trolig det mest effektive og lovlige være å gjennomføre risikoprinsippet. Dette vil trolig bidra til mer effektiv ressursbruk for de rapporteringspliktiges anti-hvitvaskarbeid, fordi de slipper å bruke ressurser på mennesker som i prinsippet ikke kan benytte tjenesten deres til å hvitvaske penger. Samtidig gjør det det mulig å harmonisere hvitvaskingsreglene og personopplysningsreglene bedre ved at det er behandlingsformålet som er styrende. En forutsetning for at dette skal være en bedre løsning er imidlertid god risikoforståelse hos den rapporteringspliktige[236], både når det gjelder hvitvaskingsloven og personopplysningsreglene.

[234] Finanstilsynet (2020) s. 42

[235] Rui (2021) s. 133

[236] Rui (2021) s. 143

I kapittel 3 er det overordnet gjort rede for kravene som stilles til lagring av personopplysninger både generelt og spesielt hvitvaskingsloven. Dette viser at kravene som stilles skal garantere et godt vern for de registrerte, men også at det er mulig å harmonisere reglene med andre regelverk. Redegjørelsen i kapittel 3.2.3 viser at det er strengere krav til behandlingsgrunnlag for særlige kategorier, enn alminnelige. Når behandlingsgrunnlagene hvitvaskingsloven er utformet relativt likt, så kan man undre seg over hva som gjør at Finanstilsynet mener det er tilstrekkelig. Muligens er det en frykt for at oppstramming av personopplysningsvernet i hvitvaskingsloven vil vanskeliggjøre hvitvaskingsarbeidet. Kanskje er dette en alminnelig frykt hos finansmyndighetene, ettersom det ikke er gjort så mye med personopplysningsvernet i hvitvaskingsloven siden den trådte i kraft.

Ettersom det pålegges rapporteringspliktige å innhente opplysninger uten behandlingsgrunnlag og det trolig ikke er tilstrekkelig behandlingsgrunnlag for særlige kategorier, vitner dette om at hensynet til personopplysningsvern ikke har vært i fokus ved utarbeidelsen av hvitvaskingsloven. Behandlingsgrunnlag er som nevnt en forutsetning for lovlig behandling. Selve funksjonen til behandlingsgrunnlaget er å skape forutsigbarhet for de registrerte. Det skal gi mening når man får behandlet personopplysningene sine. Når det behandles særlige kategorier stilles det ekstra strenge krav. At rapporteringspliktige selv må vurdere hva som anses som å være en særlig kategori i relasjon til hvitvasking, kan resultere i at det er rapporteringspliktige som til syvende og sist vurderer hvor stort inngrep de kan gjøre i retten til privatliv ved etterlevelse av hvitvaskingsreglene. Det bør derfor oppstilles tydelige krav til hvilke typer opplysninger som kan behandles og når dette kan gjøres av lovgiver. Dette vil fremstå som mer forutsigbart for de registrerte og vil harmonisere regelverkene bedre.

Ettersom retten til privatliv har grunnlovsvern i norsk rett, og skal tillegges betydelig vekt og fungere som en skranke i alminnelige lovbestemmelser, så kan det tenkes at denne burde bli tillagt mer vekt i hvitvaskingsloven. En viktig del av jobben med å harmonisere de to regelverkene er trolig dermed større bevissthet rundt personopplysningsvern også ved gjennomførelse av regler. Når ikke myndighetene har fokus på dette, er det vanskelig å klandre de rapporteringspliktige for manglende etterlevelse av personopplysningsreglene. Det er ikke utenkelig at dette blir veien man går om regelverkene ikke harmoniseres, ettersom både EDPB og Datatilsynet virker misfornøyde med personvernet i hvitvaskingsregelverket.

Det må også nevnes at det trolig ikke er kun hvitvaskingsregelverket som ikke ivaretar hensynet til personvern. I lovkommentarene til GDPR art. 24 så fremkommer det at mange virksomheter ikke har gjennomført risikovurderinger, men at dette trolig vil endres fremover.[237] Kanskje kan man trekke en generell slutning ut av denne uttalelsen, om at det ikke har vært stort fokus på personopplysningsvern siden GDPR trådte i kraft. Og at det er først nå etter noen år man har skjønt både hvordan det skal gjøre og at det er viktig.

Oppsummering

Hvordan man bedre kan harmonisere de to regelverkene kan dermed i første omgang innebære at man iverksetter de lovmessige tiltakene som både EDPB og Datatilsynet foreslår. Dette er konkrete tiltak som tydeliggjør hvordan man skal behandle personopplysninger ved etterlevelse av hvitvaskingsreglene. Dette vil trolig bidra til et sterkere personvern, siden det setter tydeligere rammer for hvordan de rapporteringspliktige bør tolke regelverket.

For at risikobaserte regelverk skal fungere best mulig, så forutsetter dette at de forpliktede har god forståelse av det relevante regelverket. Siden det er stor variasjon av rapporteringspliktige og deres ressurser, så varierer trolig både forståelse for reglene og graden av etterlevelse også. Flere og mer kompliserte vurderinger vil derfor samlet sett kreve økt ressursbruk, som ikke alle nødvendigvis greier å innfri av ulike grunner. For at dette ikke skal resultere i for stor risiko for de registrere, så vil tydeligere krav til personverntiltak i reglene trolig bidra til et generelt sterkere personopplysningsvern. Da blir en del av ansvaret for risikoavveiningen flyttet over på lovgiver. Rapporteringspliktige vil dermed mest sannsynlig være tjent med tydeligere krav til håndtering av personopplysninger i lovgivningen. Dette kan også muligens bidra til at begge regelverkene på generell basis får oppfylt sine formål i større grad. Som vist tidlige, så vil formålet med hvitvaskingsreglene, som også er behandlingsformål, være styrende for hvilke opplysninger som trengs.

Som nevnt innledningsvis er det nødvendig i lys av samfunnsutviklingen å sette begrensninger for behandling av personopplysninger for å sikre at retten til privatliv og personopplysningsvern ivaretas. Samtidig er det viktig at personopplysningsreglene ikke begrenser muligheten til å for eksempel bekjempe kriminalitet. Det er nettopp derfor personvernreglene forutsetter at de som

[237] Jarbekk (2021) art. 24 note 2

skal etterleve dem har god forståelse for hvordan man helt grunnleggende kan gjøre inngrep i retten til privatliv. Så lenge inngrep er forholdsmessige, så er behandling lovlig. Og man kan dermed behandle personopplysninger for bestemte formål, samtidig som at de registrerte får et tilstrekkelig godt vern for sine grunnleggende rettigheter.

Litteraturliste

Juridisk teori

- Bergseng Skullerud, Åste Marie mfl. *Personopplysningsloven og personvernforordningen (GDPR), kommentarutgave*. Oslo: Universitetsforlaget, 2019.

- Clausen, Christopher Sparre-Enger og Munte-Kaas, Hugo-A. B. «Personvern og tiltak mot hvitvasking: – Særlig om screening mot sanksjonslister» *Lov&Data* årg. 141, nr. 1 (2020) s. 20-22. [Lest i Lovdata Pro]

- Datatilsynet. «Etablere internkontroll- Hvordan gjennomføre internkontroll i praksis». (2018) https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/hvordan-gjennomfore-internkontroll-i-praksis/#beskrive-rammer hentet 24.11.2021

- European Data Protection Board. «European Data Protection Board - 43rd Plenary session.” (2020) https://edpb.europa.eu/news/news/2020/european-data-protection-board-43rd-plenary-session_en hentet 23.11.2021

- Høgberg, Alf Petter og Høgberg, Benedikte Moltumyr. ” Tolkning av grunnloven” *Jussens venner* (2013) s. 193- 226. [Lest i Lovdata Pro]

- Jarbekk, Eva. «Karnov lovkommentar til personvernforordningen.» I *Lovdata Pro* (2021) hentet 23.11.2021

- Justis- og beredskapsdepartementet. «Ny personopplysningslov og EUs personvernforordning.» (2018) https://www.regjeringen.no/no/tema/lov-og-rett/innsikt/ny-personopplysningslov/id2592984/ hentet 23.11.2021

- Lovdata. “Om EU-rettsaktene.” (u.å.) https://www.europalov.no/laer-mer/eu-rettsaktene#direktiv hentet 23.11.2021

- Rui, Jon Petter, Holm Ringen, Gunnar og Frivold Rørholt, Kristine. *Hvitvaskingsloven, lovkommentar*. Oslo: Universitetsforlaget, 2021.

- Stenbeck, Henriette. «Karnov lovkommentar til hvitvaskingsloven.» I *Lovdata Pro* (2021) hentet 23.11.2021

- Stortinget. «EU-domstolen: generell og vilkårlig datalagring er ulovlig.» (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/ hentet 24.11.2021

- Wiese Schartum, Dag. *Personvernforordningen- en lærebok*. Bergen: Fagbokforlaget, 2020.

Lover og internasjonale rettsakter

1814	Lov 17. mai 1814 Kongeriket Norges Grunnlov (Grunnloven).
EMK	*Konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter*, Roma 4. november 1950. [Offisiell norsk oversettelse].
2018	Lov 15. juni 2018 nr. 38 Lov om behandling av personopplysninger (Personopplysningsloven)
2018	Lov 01. juni 2018 nr. 23 Lov om tiltak mot hvitvasking og terrorfinansiering (Hvitvaskingsloven)
2018	Forskrift 14. september nr. 1324 Forskrift om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsforskriften)
2019	Lov 01. mars 2019 nr. 2 Lov om register over reelle rettighetshavere
EMK	*Konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter*, Roma 4. november 1950. [Offisiell norsk oversettelse].
Forordning 2016/679	Europaparlamentets- og rådsforordning (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 (GDPR)

Direktiv 2015/849 — Europaparlamentets- og rådsdirektiv (EU) 2015/849 av 20. mai 2015 om tiltak for å hindre at finanssystemet brukes til hvitvasking av penger eller finansiering av terrorisme (det fjerde hvitvaskingsdirektivet)

Forarbeider, høringsdokumenter og veiledere

Datatilsynet. — *Høring - Endringer i hvitvaskingsregelverket (lov og forskrift) - EUs femte hvitvaskingsdirektiv mv – Finansdepartementet.* 2020. https://www.regjeringen.no/no/dokumenter/horing--endringer-i-hvitvaskingsregelverket-lov-og-forskrift--eus-femte-hvitvaskingsdirektiv-mv/id2683265/Download/?vedleggId=dc003daf-cdb2-4bfe-beaf-2bf6ea27c3e9

Den europeiske menneskerettighetsdomstolen. — *Guide to the Case-Law of the of the European Court of Human Rights- Data Protection,* 31. desember 2020. https://rm.coe.int/guide-data-protection-eng-1-2789-7576-0899-v-1/1680a20af0

Dokument 16 (2011–2012) — *Rapport fra Menneskerettighetsutvalget om menneskerettigheter i Grunnloven.*

European Data Protection Board — *EDPB letter to the European Commission on the protection of personal data in the AML-CFT legislative proposals*, [Letter], 2021. https://edpb.europa.eu/system/files/2021-05/letter_to_ec_on_proposals_on_aml-cft_en.pdf

European Data Protection Supervisor — *EDPS Opinion on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC- Access to beneficial ownership information and data protection implications*,[Opinion],2017. https://edps.europa.eu/sites/default/files/publication/17-02-02_opinion_aml_en.pdf

Finansdepartementet — *Høring – endringer i hvitvaskingsregelverket (lov og forskrift) – EUs femte hvitvaskingsdirektiv mv.* 2019.

https://www.regjeringen.no/no/dokumenter/horing--en-dringer-i-hvitvaskingsregelverket-lov-og-forskrift--eus-femte-hvitvaskingsdirektiv-mv/id2683265/

Finans Norge. *Minimumsstandard for screening av egen kundedatabase mot sanksjonlistene,*17.04.2018. https://www.finansnorge.no/conten-tassets/5e2aa5ea2c4a4610a20bedf416c87b7e/minimums-standard-for-screening-av-egen-kundedatabase-mot-sank-sjonslistene.pdf

Finanstilsynet. *Høringsnotat- forslag til endringer i hvitvaskingsloven og hvitvaskingsforskriften.*2019. https://www.regje-ringen.no/conten-tassets/56fe59758a8f41979c0b2979e2835410/horingsno-tat-hvitvaskingsforskrift-2019-master-v11-endelig-2194816.pdf

Finanstilsynet. *Rundskriv: Veileder til hvitvaskingsloven,* 31.05.2019. https://www.finanstilsynet.no/conten-tassets/c3262e6c85fc47c7ad77c7ee10282b72/veileder-til-hvitvaskingsloven.pdf

NOU 2009: 1 Individ og integritet – Personvern i det digitale samfunnet

NOU 2016: 27 Ny lovgivning om tiltak mot hvitvasking og terrorfinansie-ring II — Andre delutredning

Ot.prp. nr. 72 (2002-2003) Lov om tiltak mot hvitvasking av utbytte fra straffbare hand-linger mv. (hvitvaskingsloven)

Ot.prp. nr. 3 (2008-2009) Om lov om tiltak mot hvitvasking og terrorfinansiering mv. (hvitvaskingsloven)

Prop. 40 L (2017-2018) Lov om tiltak mot hvitvasking og terrorfinansiering (hvit-vaskingsloven)

Tax Justice Network *Direkte og indirekte eierskap*. Oslo: 2018.

https://taxjustice.no/artikkel/ny-rapport-direkte-og-indirekte-eierskap

Økokrim. *Høringssvar fra ØKOKRIM*. 2020. Høring – endringer i hvitvaskingsregelverket (lov og forskrift) – EUs femte hvitvaskingsdirektiv mv. - regjeringen.no

Rettsavgjørelser

HR-2015- 206-A

Case C-362/14 Maximillian Schrems v. Data Protection Commissioner	ECLI:EU:C:2015:650
Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland	*Case of Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, no. 931/13, 27 June 2017