UiT Norges arktiske universitet

Det juridiske fakultet

Personvern og samhandling mellom offentlig og privat

Med fokus på sanntidsbasert automatisert utlevering av opplysninger fra bank til offentlige etater

Stian Jensen

Masteroppgave i Rettsvitenskap…JUR-3902…mai 2022

Innholdsfortegnelse

Forord

Informasjon om innholdsfortegnelsen (Slett informasjonen under før du leverer inn oppgaven)

Innholdsfortegnelsen genereres automatisk på bakgrunn av stilvalgene du benytter i hoveddelen. Du må **høyreklikke** i innholdsfortegnelsen og velge «**Oppdater Felt**» og deretter «**Hele Tabellen**» for å oppdatere innholdsfortegnelsen.

Hvis du ønsker et forord til oppgaven plasserer du markøren rett under figurlisten og trykker «ctrl» + «enter» (Sett inn sideskift). Forordet vil da starte på egen side, men ikke bli med i sidenummereringen eller innholdsfortegnelsen. Benytt stilen «Forordsoverskrift» til overskriften for forordet.

1 Innledning

Denne avhandlingen tar sikte på å belyse den juridiske utfordringen som oppstår gjennom teknologisk utvikling og hensynet til personvern. Temaet som skal gjennomgås er hvordan hensynet til personvernet bør ivaretas i forhold til de offentlige etaters ønske om å implementere en helautomatisk løsning for tilgang til bankkunders kontoinformasjon, i forhold til den Europeiske Unions (EUs) implementering av Personvernforordningen[1] (heretter kalt GDPR). Avhandlingen vil utforske hvordan Personvernforordningen og særnorsk lovgivning kan sette begrensninger for offentlige etaters systemadgang til bankkundenes personopplysninger, og om en manuell vurdering av forespørsel vil være nødvendig for å etterleve lovgivningens krav.

1.1 Tema og problemstilling

Gjennom den foreslåtte løsningen vil det behandles personopplysninger og det vil i utgangspunktet finne sted et inngrep i retten til vern av personopplysninger og respekt for privatlivet. Etter GDPR art. 6 nr. 1 er det for finansinstitusjonene et spørsmål om den behandlingen som de utfører av personopplysninger, gjennom å gjøre dem tilgjengelig for fullautomatisert utlevering, er «nødvendig for å oppfylle en rettslig forpliktelse», jf. bokstav c. GDPR bygger på at det er opp til nasjonal rett å fastsette det nærmere lovgrunnlaget for behandlingen – såkalt supplerende rettsgrunnlag. Enkelt sagt; hvilke rettslige forpliktelser som skal etableres og hva som skal være «nødvendig» behandling i den forbindelse, er gjenstand for regulering i nasjonal rett.

1.2 Bakgrunn og aktualitet

Der det er tale om forpliktelser som griper inn i grunnleggende menneskerettigheter, slik som retten til respekt for privatlivet, gjelder visse kvalitative krav til den lovgivningen som innfører slike forpliktelser. Lovhjemlene må være så klare og presise som forholdene tillater og de må inneholde særskilte og egnede garantier og tiltak for å beskytte mot misbruk

[1] Europaparlaments- 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.

(herunder overdreven utøvelse av myndighet) og vilkårlighet. For at behandlingen skal være lovlig etter GDPR, må slike overordnede krav respekteres. Kravene til lovgrunnlag må også ses i lys av inngrepets karakter og alvorlighetsgrad.

Det er enighet mellom partene i DSOP-samarbeidet at de aktuelle hjemmelsgrunnlag gir etatene myndighet til å kreve informasjon utlevert fra finansinstitusjoner. Dette innebærer at de aktuelle lovhjemlene gir myndighet til de respektive etater til å kreve informasjon utlevert etter «krav», «ved forespørsel», ved å «pålegge» eller liknende begreper. At bestemmelsene gir rett til å kreve utlevering ved utferdigelse av pålegg, er imidlertid ikke nødvendigvis det samme som at de offentlige etatene etter loven gis rett og myndighet til en form for direkte tilgang til opplysninger hos bankene som gjør at disse kan samles inn umiddelbart og automatisert. Motsatt er dette heller ikke det samme som at bankene, etter loven, har en plikt til å tilrettelegge for en slik informasjonstilgang og underlegge opplysningene en slik automatisert behandling. I en slik situasjon vil det også kunne være vanskelig for bankene å kontrollere at det ikke hentes mer informasjon enn hva det er rettslig grunnlag for. Dette til tross for at de aktuelle opplysningstyper ligger innenfor rammene av hva som kan kreves utlevert.

Den rettslige uklarheten som gjør at det oppstår betydelig tvil knyttet til lovligheten, er knyttet til at verken ordlyden i de ulike bestemmelsene eller forarbeidene til de aktuelle lovene i særlig grad støtter oppunder en slik direkte tilgang og automatisert innsamling / utlevering som DSOP-samarbeidet tilrettelegger for. Løsningen er også vanskelig å forene med de rettssikkerhetsgarantier som ligger i gjeldende regler knyttet til å kunne motsette seg utleveringspålegg og klage eller kreve rettslig prøving eller anke. Disse forhold gjør at det stilles spørsmål om det verktøy for informasjonstilgang som DSOP-løsningen i realiteten er, har den nødvendige forankring i lov. Et eksempel på lovgivning hvor det eksplisitt åpnes for direkte tilgang til informasjon og/eller systemer, og hvor de nødvendige vurderinger er gjort i forarbeider, er Vegtrafikklovens § 43 b[2]. Det er her viktig å påpeke at vurderingene er gjort opp mot politiets adgang til Statens vegvesens motorvognregister og førerkortregister, hvor den generelle informasjonsbase har et mer snevert omfang av personopplysninger enn hva et bankkundeforhold vil inneholde. Et eksempel på kommende lovgivning hvor tilsvarende

[2] Lov 18. juni 1965 nr. 4 – Vegtrafikkloven, vtrl.

drøftelse er gjort på EU-nivå er Femte hvitvaskingsdirektiv[3], som p.t. ikke er implementert i norsk rett.

Forenklet kan man si at problemet springer ut av at loven ikke gjør det klart at de aktuelle etater skal ha rett til en direkte og umiddelbar tilgang til slik informasjon som DSOP-løsningen åpner for. Det er heller ikke klart at bankene har en forpliktelse til å gi og tilrettelegge for dette. Konsekvensen blir at det vanskelig kan sies at den metoden bankene vil behandle personopplysninger på gjennom DSOP kontroll faktisk er «nødvendig» for å oppfylle en rettslig forpliktelse.

1.3 Avgrensning og videre fremstilling

Denne avhandlingen søker å undersøke om det er hjemmelsgrunnlag i GDPR eller særnorsk lovgivning for å helautomatisere innsyn og deling av bankkunders personopplysninger fra et rettsdogmatisk perspektiv. Hovedfokuset vil være på de lovhjemler i GDPR og særnorsk lovgivning som er direkte anvendelig angående retten til privatliv og privat korrespondanse. Relevant rettspraksis fra Norge og EU-domstol vil også bli trukket inn for nyansering og underbyggelse av forståelse for de aktuelle lovhjemler.

Særlige kategorier av personopplysninger er angitt som en omfattende, men ikke uttømmende liste i GDPR art. 9, og er underlagt et strengere vern enn de «alminnelige» personopplysninger som er regulert i art. 8. Personopplysninger av denne karakter ble tidligere omtalt som «sensitive personopplysninger». I avhandlingen vil det bli drøftet om kontoutskrifter og transaksjonshistorikk er gjenstand for rettslig vern etter GDPR art. 9 grunnet opplysningenes innhold og karakter, som i flere tilfeller kan falle inn under denne kategorien. Vurderingsmomentene vil bli knyttet direkte til tema om kontoutskrifter og beskyttelse av personvernet, og bør ikke ses på som en omfattende analyse eller dyptgående gjennomgang av særlige kategorier av personopplysninger generelt.

Denne avhandling er begrenset til juridiske spørsmål rundt implementering av DSOP-løsningen, for hvordan finansinstitusjoner best kan ivareta hensynet til sine kunders personvern. Det teknologiske aspektet rundt løsningen vil ikke bli gjennomgått i detalj, men

[3] Direktiv (EU) 20018/843.

forklart på et grunnleggende plan for å skape forståelse rundt de rettslige problemstillingene som blir drøftet.

I det følgende vil det tidvis fremkomme forklaringer og beskrivelser av bankinterne rutiner og behandlingsmåter for hvordan håndtering av personsensitive opplysninger gjennomføres i dag, og betraktninger rundt behandlingsmåten. Dette er basert på seks års personlig arbeidserfaring, og noe bankintern dokumentasjon som ikke er anledning å henvise til i denne avhandlingen.

2 Digital samhandling mellom offentlig og privat – DSOP

2.1 Hva løsningen er

I april 2016 kom en tilråding fra kommunal- og moderniseringsdepartementet som la grunnlaget for den digitale agenda og videreutviklingen i Norge innenfor IKT-løsninger og elektronisk kommunikasjon. Meldingen inneholder en beskrivelse av hvordan IKT kan benyttes for å fornye, forenkle og forbedre offentlig sektor. Den omhandler videre en nasjonal plan for elektronisk kommunikasjon, kalt ekomplanen.[4]

I tråd med denne digitaliseringsplanen startet finansnæringen i 2016 et samarbeid med Skatteetaten, Brønnøysundregisteret, Digitaliseringsdirektoratet, NAV, Politiet og Kartverket et omfattende samarbeid om digitalisering av viktige prosesser i samfunnet kalt «Digital Samhandling Offentlig Privat (heretter referert til som DSOP). Samarbeidet er basert på en porteføljetankegang der DSOP-programmet setter sammen ulike prosjektinitiativer som balanserer innsats og nytte for de involverte parter. Noen prosjekter er allerede fullført og implementert som en standardløsning i dag, som for eksempel «samtykkebasert lånesøknad - SBL». I denne prosessen kan en bankkunde ved registrering av lånesøknad samtykke til at bankinstitusjonen får tilgang til å innhente lønns- og skatteopplysninger automatisk fra Alltinn / Skatteetaten. Det er viktig å presisere at i denne prosessen samtykker bankkunden aktivt til at spesifisert informasjon er mulig å innhente automatisk av finansinstitusjonen. Alternativet har tidligere vært at finansinstitusjoner har etterspurt papirdokumentasjon direkte

[4] Meld. St. 27 (2015-2016)

fra kunde, som måtte fremskaffes. Den nye løsningen tillater imidlertid at det opplyses om hvilken informasjon som vil bli uthentet, også samtykker kunde til dette ved å legitimere seg med BankID. Eventuelt avslag på denne forespørselen vil føre til at søknadsprosessen avsluttes.

Det neste initiativet som ble lansert i DSOP-samarbeidet var DSOP Kontrollinformasjon (heretter omtalt som Kontrollinformasjon). Dette er en sanntidsbasert maskinell og automatisert tjeneste for utlevering av nærmere fastsatte kategorier av informasjon fra bankene til den aktuelle etat i forbindelse med hjemmelsbasert kontrollvirksomhet. Gevinstene ved å etablere en maskin til maskin utveksling av kontoinformasjon, med standardisert og analyserbart innhold fra alle bankene til etatene, er at etatene settes i stand til å utføre betydelig flere kontroller og innhente kvalitativt bedre kontoinformasjon raskere uten menneskelig involvering fra bankens side. Basert på analyse av innhentet informasjon kan etatene også foreta en bedre utvelgelse av kontrollobjekter.

Forespørslene fra etatene vil for bankene se like ut, men formålet (med referanse til hjemmel) og behandlingen av mottatt kontoinformasjon i etatene vil være forskjellig. Forespørslene fra etatene med informasjon om «objektet» (org.nr./fødselsnr./d-nummer) går først til et register i finansnæringen som lister hvilke banker som har – eller har hatt – en relasjon til objektet. Basert på denne banklisten sendes det fra etaten en automatisk forespørsel til disse bankene for å få en kontoliste – og deretter spør etaten om saldo og eventuelt transaksjonshistorikk for hver av disse kontoene.

Det er ingen uenighet mellom partene i DSOP-samarbeidet om etatenes hjemler for å be om informasjon som er nødvendig for å oppfylle den rettslige forpliktelse, og som behandles manuelt. DSOP Kontrollinformasjon er imidlertid en løsning som vil hente ut informasjonsdata uten en manuell behandling eller kontroll.

2.2 Kontrollinformasjon

Formålet med utlevering av kontrollinformasjon til det offentlige er at finansinstitusjonene skal overholde sine rettslige forpliktelser. Finansinstitusjonene må i dag manuelt samle denne type informasjon og sende til de som etterspør. Forespørslene kan komme per telefon, e-post eller digitale brev via Altinn. Ved automatisering av disse oppgavene vil finansinstitusjonene spare tid og ressurser, samtidig som det offentlige raskere vil få tilgang til informasjon. Ved

raskere tilgang til informasjon vil man tidligere kunne etterforske, behandle, stoppe eller forhindre kriminelle handlinger.

De som berøres av denne løsningen vil være privatkunder, bedriftskunder og kontaktpersoner i virksomheter, samt mindreårige. Det vil kunne bli behandlet personopplysninger om samtlige kunder i finansinstitusjonene. Det er foreløpig ikke lagt opp til at bankene skal utlevere kontrollinformasjon om personer med skjermet identitet gjennom løsningen, selv om etatene også ønsker dette. Med skjermet identitet menes privatpersoner som av ulike årsaker har sin kundeinformasjon skjult selv fra finansinstitusjonens ansatte, hvor kun et fåtall nøkkelpersoner har tilgang til å se denne. Formålet med å skjerme identiteten er at kundes adresse eller oppholdssted, transaksjonsinformasjon, disponenter mv. ikke skal kunne gjøres kjent av hensyn til kundens sikkerhet.

Dataene som benyttes hentes fra finansinstitusjonenes systemer, som kan ha vært oppdatert mot offentlige registre. Videre stammer personopplysningene fra kunden selv, og/eller er innhentet ved legitimasjon, kjøp av produkter, mv.

Kontrollinformasjon-løsningen er ment å gi etater tilgang til følgende informasjon som de har mulighet til å etterspørre automatisk, basert på behov og lovhjemmel i deres kontrollvirksomhet:

- Kontoliste – Oversikt over konti som kunde eier. Disse kan det videre bes om utfyllende informasjon om.
- Kontodetaljer – Saldo på konto som kunde eier
- Transaksjoner – Oversikt over historiske transaksjoner på en kundes konto
- Disponenter – Oversikt over hvem som er disponent på en kundes konto
- Debetkort – Oversikt over hvilke debetkort som er tilknyttet en kundes konto

Underveis i prosessen har det blitt gjennomført en vurdering av personvernkonsekvenser (data protection impact assessment – DPIA) som kan gjøre seg gjeldende. Hovedhensikten er å sørge for at det gjøres grundige vurderinger hvis behandlingen av personopplysninger medfører spesielt høy risiko for rettighetene og friheten til den registrerte.[5]

[5] Jarbrekk og Sommerfeldt, *Personvern og GDPR i praksis*, side 138.

De følgende tre risikoer blir ansett som særs alvorlige:

Risiko	**Kontrollinformasjon**
Overskuddsinformasjon	Etatene kan hente informasjon fra flere API-er enn det de har behov for i en pågående kontrollsak
Ulovlig behandlingsgrunnlag hos etatene	Hjemmelsgrunnlaget for kontrolletat for utlevering av kontrollinformasjon fra bank er ikke tilpasset en digital kontrollinformasjonsløsning, men skrevet for en manuell behandling. Det er en risiko for at behandlingsgrunnlaget ikke er lovlig
Snoking	Ansatte i etatene kan gjøre oppslag på kunder uten at det foreligger tjenstlig behov

3 Grunnleggende menneskerettigheter

Ved utarbeidelse av Kontrollinformasjon-løsningen har det blitt stilt spørsmål om det innebærer en omfattende inngripen i menneskets personvern, og dermed et brudd på de grunnleggende menneskerettigheter som respekt for retten til privatliv og sin kommunikasjon.

3.1 Menneskerettigheter – EMK

Mange av de vilkårene som stilles er også vilkår som utledes av EMK[6]. Det vil derfor være naturlig å innledningsvis skrive noe om kravene til hjemmel i lov, nødvendighet, forholdsmessighet og uavhengig domstol, som er en del av menneskerettighetsgarantiene.

EMK artikkel 8 hjemler retten til respekt for privatliv og familieliv. Uttrykket «respekt» er ifølge EMD[7] ikke entydig, jf. B. v. France § 44, men omfatter både negative og positive forpliktelser. Den negative forpliktelsen innebærer at staten må avstå fra å gripe inn i

[6] Inkorporert i norsk rett ved Lov 21. mai 1999 nr. 30 - Menneskerettsloven, mrl.

[7] Den europeiske menneskerettsdomstolen.

beskyttede interesser etter art. 8 nr. 1 såfremt ikke vilkårene for inngrep er oppfylt etter art. 8 nr. 2. Den positive plikten innebærer at staten må beskytte individer fra krenkelser begått av andre, jf. art. 8 nr. 1 og Södeman v. Sweden § 78.

Dette analytiske skillet mellom negative og positive forpliktelser er likevel ikke renskåret. EMD finner det heller ikke alltid nødvendig å avgjøre om man står overfor et brudd på en negativ eller positiv plikt. Ifølge EMD er de anvendelige rettsreglene uansett beslektede eller tilsvarende, jf. Nunez v. Norway § 69. Det sentrale vurderingstemaet er i begge tilfeller om staten har lykkes i å treffe «the fair balance between the competing interests of the individual and the community as a whole», jf. Aksu v. Turkey § 59.

Skillet mellom negative og positive forpliktelser kan imidlertid ha betydning for skjønnsmarginen som EMD tilkjenner stater etter art. 8. Statens skjønnsmargin vil for eksempel være vid der det er tale om å balansere konkurrerende rettigheter, jf. Fernandez Martines v. Spain § 78, og snever der «a particular important facet of an individual´s existence or identity is at stake", jf. E.S. v. Sweden § 58.

Uttrykket "privatliv" er ikke gitt en uttømmende definisjon. Privatlivsbegrepet omfatter lagring og publisering av personlig informasjon, samt vilkårlig ransaking og beslag, jf. Robathin v. Austria § 39.

Kopieringen av bankdata og myndighetens påfølgende lagring av slike data, er handlinger som faller inn under begrepene «privatlig» og «korrespondanse», og utgjør en påvirkning i henhold til EMK artikkel 8, jf. M.N. and Others v. San Marino, 2015, § 55.

3.2 Legalitetsprinsippet – hjemmel i lov

Legalitetsprinsippet er et prinsipp om at inngrep overfor borgerne fra myndigheter krever hjemmel i lov. Det er særlig kravet om rettssikkerhet og forutberegnelighet for borgerne som er begrunnelsen for legalitetsprinsippet. Man skal vite hva man kan straffes for, slik at man ikke straffes vilkårlig. I Rt. 1933 s. 212 ble det uttalt at «særlig hvor det gjelder den alminnelige straffelov må landets borgere ha krav på å få klar beskjed om, hva de kan straffes for».

Legalitetsprinsippet er å anse som konstitusjonell sedvanerett, dvs. at det er en sedvane av samme konstitusjonelle rang som en grunnlovsbestemmelse. Sedvane oppstår når det utvikler seg en praksis i den tro at det er en rettsregel som må følges, og den faktisk følges.

I statsforfatningsretten er legalitetsprinsippet en betegnelse på to forskjellige prinsipper:

For det første betegner prinsippet i Grunnlovens § 113* om at forvaltningsorganene må ha hjemmel i lov for å treffe vedtak som griper inn i det enkelte individs rettsstilling. For det andre betegner det prinsippet i Grunnlovens § 96 om at ingen kan straffedømmes uten etter lov (også kalt lovprinsippet).

Tilsvarende legalitetsprinsipp finnes også i flere menneskerettighetskonvensjoner som Norge er tilsluttet og som er gjort til norsk lov gjennom menneskerettsloven.

En nyansert betraktning av legalitetsprinsippet ble uttalt i Rt. 1995 s. 539 – Fjordlaksdommen:

«Jeg antar, med bakgrunn i teori og praksis, at kravet til lovhjemmel må nyanseres blant annet ut fra hvilket område en befinner seg på, arten av inngrepet, hvordan det rammer og hvor tyngende det er overfor den som rammes. Også andre rettskildefaktorer enn loven selv må etter omstendighetene trekkes inn. En slik mer sammensatt vurdering må etter min mening legges til grunn ved avgjørelsen av de hjemmelsspørsmål som oppstår i denne saken.»

En tilsvarende metode vil bli benyttet i det følgende for å vurdere hjemmelsgrunnlaget til Kontrollinformasjon-løsningen.[8]

3.3 Nødvendighet

Det vil senere bli sett nærmere på politiets lovhjemmel til å innhente informasjon i forbindelse med etterforskning. I den anledning er det derfor aktuelt å henvise til NOU 2009:15 punkt 6.7 hvor nødvendighetskravet er særskilt drøftet opp mot denne lovhjemmel.

Både politiets informasjonsinnhenting og videre informasjonsbehandling bør skje ut fra et minimalitetsprinsipp eller et nødvendighetsprinsipp. Dette kan utledes fra Personverndirektivet art. 6 første ledd bokstav c, art. 7 og art. 8, samt EUs rammebeslutning art. 3 nr. 1. Dette innebærer for det første at man ikke skal åpne for større tilgang til bruk av skjulte tvangsmidler i etterforskning enn det som er nødvendig ut fra de legitime forhold.

[8] https://snl.no/legalitetsprinsippet

For det andre innebærer prinsippet at reglene må utformes på en slik måte at politiets informasjonshenting blir mest mulig målrettet og i minst mulig grad omfatter informasjon som ikke er relevant for etterforskningen.

Nødvendighetsprinsippet tilsier at metodene bør brukes på en måte som rammer færrest mulig personer som ikke er mistenkte for straffbare handlinger. Jo flere som rammes av informasjonsinnhentingstiltaket, jo strengere mener utvalget at inngrepsvilkårene bør være. Dette prinsippet gjenspeiles for eksempel i straffeprosessloven § 216 c tredje ledd*, hvor det stilles krav om at det foreligger «særlige grunner» for å eksempelvis avlytte telefoner som er tilgjengelige for et større antall personer. På samme måte bår det for eksempel stilles strengere krav for å innhente informasjon om alle telefonsamtaler foretatt i et område i en periode, enn for å innhente informasjon om samtaler ført av en navngitt person på bakgrunn av mistanke om at vedkommende har begått en kriminell handling.

Nødvendighetsprinsippet tilsier også at innsamlet informasjon ikke bør videreformidles til flere personer eller virksomheter enn det som er nødvendig. Dette innebærer etter utvalgets mening at det bør stilles krav til at politiets datasystemer utformes på en måte som begrenser ansattes tilgang til etterforskningsmateriale. Prinsippet medfører i utgangspunktet også at informasjon som ikke er nødvendig i et straffeforfølgings- eller kriminalitetsbekjempelsesperspektiv ikke bør lagres og at relevante opplysninger ikke bør lagres lengre enn nødvendig.

Under etterforskningen er det imidlertid ikke alltid mulig å praktisere et strengt nødvendighetsprinsipp. Innledningsvis fordi det er vanskelig for politiet å vite hva som er relevant. Informasjon som på et tidspunkt ikke anses relevant, kan vise seg å være relevant på et senere tidspunkt. Videre forutsetter innsynsreglene at den innsamlede informasjonen skal videreformidles den mistenkte og hans forsvarer for derved å underkastes en selvstendig relevansvurdering. For at innsynsretten skal være reell, kan materialet ikke slettes. Muligheten for gjenåpning av straffesaker tilsier også at informasjonen lagres.[9]

[9] NOU 2009:15

3.4 Forholdsmessighet

Forholdsmessighetsprinsippet går ut på at det skal oppstilles et krav om forholdsmessighet mellom mål og middel. Det finnes ikke klare eksempler på at Høyesterett har lagt et slikt generelt prinsipp til grunn, men det antas likevel at det gjelder en ulovfestet sedvanerett om at forholdsmessigheten av et vedtak som ilegger sanksjoner kan prøves, for eksempel med grunnlag i EMK art. 6.

Det er et ulovfestet prinsipp om forholdsmessighet som kommer til uttrykk i forvaltningsretten på flere ulike forhold:

1. En forholdsmessig vurdering i forvaltningen dreier seg om ekstra tyngende eller inngripende tiltak kan være uforholdsmessige.
2. En annen forholdsmessighetsvurdering i forvaltningen knytter seg til om vilkårene som knytter seg til et begunstigende forvaltningsvedtak er forholdsmessige.
3. En tredje forholdsmessighetsvurdering i forvaltningen gjelder avveiningene som er gjort under forvaltningens skjønnsutøvelse. Hvis forvaltningen overser eller ignorerer et relevant hensyn, eller legger overdreven vekt på et perifert hensyn, kan avgjørelsen bli uforholdsmessig.
4. En fjerde forholdsmessighetsvurdering i forvaltningen angår resultatet av forvaltningsvedtaket og vedtakets konsekvenser. Forvaltningsvedtak kan bli uforholdsmessig inngripende dersom forvaltningen griper til hardere lut enn nødvendig slik at det ikke blir samsvar mellom mål og midler. Det er ikke omstridt at domstolene kan kontrollere de tre første betydningene av forholdsmessighetsprinsippet. Mens forholdsmessighetsprinsippet i denne betydningen er en intern pliktregel for forvaltningen, er det delte meninger om hvor langt en domstol kan gå i å sette et slikt vedtak til side som ugyldig.[10]

3.5 Uavhengig domstol

Domstolenes og dommernes uavhengighet er et grunnleggende prinsipp som sikres gjennom at ingen kan gi domstolene eller dommerne instrukser om hvordan de skal behandle en sak.

[10] https://jusleksikon.no/wiki/Proporsjonalitetsprinsippet

Høyesteretts avgjørelser kan ikke overprøves av andre myndigheter. Stortinget, regjeringen, Domstoladministrasjonen eller de ulike departementene kan ikke forlange at domstolene skal komme fram til et bestemt resultat i en sak.[11]

Grunnloven § 95 annet ledd pålegger staten en plikt til å sikre uavhengige og upartiske domstoler og dommere. Denne sikringsplikten er drøftet i lys av EMK art. 6 nr. 1 og må ses i lys av nasjonale utfordringer når det gjelder å styrke og bevare tilliten til at domstolene og dommere kan opptre uavhengig og upartisk.

Retten til å få en sak avgjort av uavhengige og upartiske domstoler er vernet av flere internasjonale menneskerettighetskonvensjoner. Sentralt for norsk rett står EMK art. 6 nr. 1 og SP art. 14 nr. 1. Begge disse konvensjonene er inkorporert slik at de gjelder som norsk lov og skal ved motstrid gis forrang fremfor annen lovgivning, jf. menneskerettsloven § 3.* Størst praktisk betydning har EMK fordi EMD er en aktiv og dynamisk fortolker av rettighetens innhold gjennom individklageretten.

EU-domstolen er en tilsvarende dynamisk rettsutvikler som EMD. Domstolens avgjørelser er ikke bindende for Norge, men kan likevel stå sentralt i rettskildebildet ved avgjørelse av rettsspørsmål for norske domstoler. Dette er en konsekvens av EØS-avtalen som er gjennomført ved lov. I traktaten om Den europeiske union (TEU) art. 2 er rettsstaten angitt som en del av det felles verdigrunnlaget for medlemsstatene. I EUs Charter om grunnleggende rettigheter (Charteret) art. 47 er også enhver gitt rett til en rettferdig rettergang for en uavhengig og upartisk domstol. Når TEU art. 19 nr. 1 pålegger medlemsstatene en plikt til å gi dadgang til domstolsprøvelse for å sikre effektiv rettsbeskyttelse på områder som er beskyttet av EU-retten, er det tale om en uavhengig og upartisk domstol i Charterets forstand. EU-retten fortolkes både av EU-kommisjonen og EU-domstolen som har tatt standpunkt til flere saker som gjelder mulige brudd på kravene til uavhengige og upartiske domstoler. EMD betrakter EU-retten som relevant ved tolkningen av om et EFTA-medlem har oppfylt kravene til uavhengige og upartiske domstoler i EMK art. 6. Norske rettsanvendere kan med andre ord ikke lukke øynene for hva som er unionens forståelse av hva en uavhengig og upartisk domstol er.[12]

---

[11] https://lovdata.no/artikkel/domstoler_maktfordeling_og_uavhengighet/1468

[12] https://www.idunn.no/doi/10.18261/issn.1504-3126-2021-04-01

4 Personvernforordningen – GDPR

4.1 Lovens virkeområde

Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven) inkorporerte forordning (EU) 2016/679 (personvernforordningen eller forordningen) som norsk lov gjennom personopplysningsloven § 1. Både personopplysningsloven og forordningen har omfattende bestemmelser om behandling av personopplysninger som har stor innvirkning på både individer, privat næringsliv og offentlig sektor.

Personvernforordningen består av 99 artikler og 174 fortalepunkt i innledningen. Fortalepunktene har ikke rettslig eller operativ virkning, men bidrar med avklaring og belyser formålet med artiklene. Metoden som EU-domstolen benytter ved tolkning av den operative loven viser at fortalene er av stor betydning for å belyse den videre forståelsen av artiklene. Anvendelse av fortalene er imidlertid begrenset til de tilfeller hvor den ikke er i strid med artikkelen. Normene som artiklene setter er juridisk bindende og primærkilde. Klare og entydige artikler kan derfor ikke overstyres eller modifiseres ved bruk av fortalepunkt. Likevel er forordningen preget av noen vage og generelle bestemmelser som er ment å være fleksible, der bruk av fortalepunkt vil være nødvendig i utstrakt grad, noe som gir tilleggsinformasjon og vilkår til lovnormen. Den europeiske domstolen, sammen med retningslinjene og uttalelsene til Det Europeiske Databeskyttelsesråd og Artikkel 29-gruppen, refererer ofte til fortalepunktene og de ser ut til å ha viktig betydning for å gi artiklene ytterligere eller mer spesifikk mening.

Forarbeidene til loven er Prop. 56 LS 2017-2018.

4.2 Begrepsavklaringer

Personopplysninger – Enhver opplysning om en identifisert eller identifiserbar fysisk person, også referert til som «den registrerte».[13] Kontoutskrifter og transaksjonsdetaljer faller under denne kategorien.

[13] GDPR art. 4 nr. 1

Behandling – Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller manuelt. Dette omfatter innsamling, registrering, lagring, bruk og utlevering, for å nevne noe.[14]

Artikkel 29-gruppen, WP29 – «Arbeidsgruppen for beskyttelse av enkeltpersoner med hensyn til behandling av personopplysninger», bestående av databeskyttelsesmyndigheter i hvert EU-medlemsland, European Data Protection Supervision og EU-kommisjonen.

Rapporteringspliktig – Person eller selskap som i henhold til norsk lovgivning er pliktig å gi opplysninger etter konkret lovhjemmel.

Behandlingsansvarlig – Person eller selskap som har det juridiske ansvaret for behandling av personopplysninger, og som bestemmer hvordan og hvorfor personopplysningene blir behandlet.

API – Application Programming Interface – Et digital grensesnitt mellom to dataprogrammer.

4.3 Personvernkonsekvenser - DPIA

GDPR art. 35 pålegger banker å foreta en vurdering av personvernkonsekvenser. På engelsk kalles en slik vurdering en Data Protection Impact Assessment, forkortet til DPIA. Betegnelsen er også blitt vanlig i norsk språk, og benyttes derfor videre. Hovedhensikten er å sørge for at det gjøres grundige vurderinger hvis behandlingen av personopplysninger medfører spesielt høy risiko for rettighetene eller friheten til den registrerte. WP29 har utgitt en egen veileder om når og hvordan en DPIA skal gjennomføres.

En DPIA er en forhåndskontroll som virksomheten selv er ansvarlig for. Det er en av de viktigste mulighetene virksomheten har for å sikre at den etterlever personopplysningsloven, og man plikter å ha en oversikt over hvilke vurderinger som eksisterer i virksomheten. Dersom man må fremlegge dokumentasjon på sin internkontroll for Datatilsynet, vil gjennomførte DPIAer være en sentral del av dette.

Dersom en DPIA viser at det etter foreslåtte tiltak fremdeles er en høy risiko for den registrertes rettigheter og friheter, må den behandlingsansvarlige kontakte Datatilsynet. Tilsynet vil da vurdere om de kan godkjenne virksomhetens behandling av

[14] GDPR art. 4 nr. 2

personopplysninger, til tross for den påviste risiko. Hovedfokuset på den utførte analyse skal ligge på risikoen for den registrerte og overholdelsen av den registrertes rettigheter gjennom hele behandlingens livsløp, uavhengig av om dette er for en kort eller lengre tid.

De følgende kriterier er direkte oversatt fra WP-29 gruppens veileder for DPIA og har blitt spesielt vektlagt ved vurderingen av Kontrollinformasjon-løsningen[15]:

- Automatiske beslutninger med rettslig eller tilsvarende betydning eller virkning. Behandlingen har som formål å ta beslutninger om den registrerte som har «rettsvirkning for den fysiske personen» eller «på lignende måte i betydelig grad påvirker den fysiske personen», jf. art. 35 nr. 3 a.
- Systematisk monitorering. Behandlingsaktiviteter brukes for å observere, overvåke eller kontrollere den registrerte, inkludert opplysninger som har blitt samlet inn gjennom nettverk eller «en systematisk overvåkning i stor skala av et offentlig tilgjengelig område», jf. art. 35 nr. 3 c.
- Særlige kategorier av personopplysninger eller opplysninger av svært personlig karakter, som definert i art. 9.
- Personopplysninger behandles i stor skala. Forordningen definerer ikke hva som menes med stor skala, selv om det gis en viss veiledning i fortalepunkt 91. WP29-gruppen anbefaler at følgende faktorer vurderes spesielt:
  a. Antallet registrerte som berøres, enten som et spesifikt antall eller som en andel av den relevante populasjonen.
  b. Mengden og/eller spennvidden i personopplysningene som behandles.
  c. Databehandlingens varighet eller regelmessighet.
  d. Behandlingens geografiske omfang.
- Personopplysninger om sårbare registrerte. Behandling av denne typen av personopplysninger er et kriterium på grunn av den skjeve maktbalansen mellom de registrerte og den behandlingsansvarlige. Sårbare registrerte kan omfatte mindreårige, sårbare befolkningsgrupper som behøver sosial beskyttelse, mv.

[15] Datatilsynet, Veiledning for Vurdering av personvernkonsekvenser, https://www.datatilsynet.no/regelverk-og-skjema/veiledere/vurdering-av-personvernkonsekvenser/.

- Innovativ bruk eller anvendelse av ny teknologisk eller organisatorisk løsning. Anvendelse av ny teknologi kan medføre nye former for innsamling og bruk av personopplysninger, eventuelt med høy risiko for den enkeltes rettigheter og friheter.[16]

På dette grunnlag har de offentlige etaters mulighet for å innhente mer informasjon enn nødvendig, manglende mulighet til å manuelt kontrollere de offentlige etaters behandlingsgrunnlag og muligheten for snoking blitt vurdert som særs risikofylte momenter dersom Kontrollinformasjon-løsningen implementeres.

4.4 Behandling av personopplysning

4.4.1 Lovlig og rettferdig

Personvernforordningens fortalepunkt 39 angir at enhver behandling av personopplysninger bør være lovlig og rettferdig. De særlige formålene med behandlingen av personopplysningene bør især være berettigede, uttrykkelig angitt og fastsatt når personopplysningene samles inn. Personopplysningene bør være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for. Dette krever særlig at det sikres at personopplysningene ikke lagres lenger enn det som er strengt nødvendig. Personopplysningene bør behandles bare dersom formålet med behandlingen ikke med rimelighet kan oppfylles på annen måte. Personopplysninger bør behandles på en måte som gir tilstrekkelig sikkerhet og konfidensialitet, herunder for å hindre ulovlig tilgang til eller bruk av personopplysninger og utstyret som brukes i forbindelse med behandlingen.

4.4.2 Generelt

Artikkel 5 angir de grunnleggende prinsippene for personvern. De angis her overordnet, og er beskrevet nærmere i mange av forordningens øvrige artikler. Slik som formålsbestemmelser generelt, vil prinsippene i artikkel 5 være sentrale som tolkningselementer når øvrige artikler skal tolkes. Det er den behandlingsansvarlige som er ansvarlig for at prinsippene overholdes, selv om databehandlere benyttes. Det er sentralt å se at den behandlingsansvarlige skal «påvise» at prinsippene er overholdt, noe som gir en omfattende plikt til dokumentasjon.

En behandling skal være lovlig, hvilket innebærer at den må ha en hjemmel. Se artikkel 6, 9 og 10 om dette. Andre bestemmelser om hjemmel kan finnes i særlovgivning, slik som

[16] Jarbekk, Eva og Simon Sommerfeldt, *Personvern og GDPR i praksis*, s. 138 flg.

skatteforvaltningsloven. Tilsvarende gjelder Grunnloven § 102 om retten til personvern. Her vises også til den europeiske menneskerettighetskonvensjonen (EMK) art. 8 som angir retten til vern om privatlivet. I norsk rettskildelære har legalitetsprinsippet en sentral plass.

Informasjon uthentet fra et individs bankdokumenter utgjør personlig data, enten det er sensitiv privat informasjon eller informasjon om den registrertes profesjonelle forretninger, jf. «M.N. and Others v. San Marino», 2015, § 51; G.S.B. v. Switzerland, 2015, § 51.

4.4.3 Rettferdighetskravet

Art. 5 nr. 1 bokstav a angir at behandlingen skal være rettferdig. Det vil ofte være en subjektiv vurdering, noe som gir åpning for skjønn. Den registrertes synspunkt bør vektlegges, det samme gjelder den behandlingsansvarliges oppfatning.

4.4.4 Dataminimering

Art. 5 nr. 1 bokstav c omtaler det som ofte kalles dataminimering. Dette er et grunnleggende element i forordningen. Ofte benyttes begrepet minimumsprinsippet også. Konsekvensen av prinsippet er at man ikke skal behandle flere personopplysninger enn hva som er nødvendig for et bestemt formål. Prinsippet har også en såkalt innebygget personvern, eller «privacy by design». Begge prinsippene innebærer at man ikke skal behandle flere personopplysninger enn nødvendig. Det er også relevant for en behandlingsansvarlig å spørre seg om det overhodet er nødvendig å behandle personopplysninger for å nå et bestemt formål. I tillegg til å vurdere hvilke opplysninger som er absolutt nødvendig, skal man vurdere hvor lenge opplysninger oppbevares. Ingen opplysninger skal oppbevares lengre enn nødvendig. Den behandlingsansvarlige bør dokumentere og begrunne sine vurderinger av hva som er nødvendig. For offentlig sektor har prinsippet vært sentralt i flere rettsaker om nødvendigheten av kontrolltiltak. Her har bestemmelsene i EMK spilt inn. Dommen om datalagringsdirektivet, ECJ sak C-293/12, hadde en omfattende vurdering av om kontrolltiltakene var forholdsmessige og i tråd med dataminimeringsprinsippet. I premiss 308 i saken som ofte benevnes Case of Big Brother Watch and others vs. the United Kingdom (Applications nos. 58170/13, 62322/14 and 24960/15) skrev ECJ at en stat har en viss frihet til å vedta kontrollerende tiltak, men at dette er betinget av at det er adekvate og effektive garantier mot misbruk av kontrollsystemet. De konkrete tiltakene som var foreslått i England ble ansett for å være ulovlige. Vurderingstemaene som dommen angir, er relevante også for andre saker. Det er at det skal tas hensyn til de konkrete omstendighetene, herunder arten, omfanget og varigheten av behandlingen samt bakgrunnen for å iverksette tiltakene, hvilke

myndigheter som gis kompetanse til å tillate, gjennomføre og overvåke tiltakene og hvordan nasjonal rett åpner for rettsmidler for å støtte den registrerte.

I saken «Centrum for Rättvisa v. Sweden» om bulk-overvåkning, anså EMD allerede stadiet for innsamling av kryptert og anonymisert metadata som et svakt inngrep i korrespondanse- og privatliv, og uttalte at inngrepet blir sterkere dess mer filtrert og rettet analyseringen av materialet blir, jf. § 239 flg.

4.4.5 Ivareta prinsippene

Art. 5 andre ledd angir dels at den behandlingsansvarlige er den som skal sørge for at de grunnleggende prinsippene blir ivaretatt. Videre angis at den behandlingsansvarlige må kunne påvise at så er tilfelle. Ordet «påvise» medfører en dokumentasjonsplikt.

4.5 Behandlingsgrunnlag

4.5.1 Generelt

Bestemmelsen GDPR art. 6 er en av forordningens mest sentrale artikler. Den angir behandlingsgrunnlagene for vanlige personopplysninger. Artikkel 9 angir behandlingsgrunnlagene for særlige kategorier av personopplysninger. Det er ikke de samme grunnlagene som er behandlingsgrunnlag for de to typene personopplysninger. Behandlingsgrunnlagene i art. 6 er likestilte. Der noen tidligere mente at samtykke er et bedre grunnlag enn for eksempel berettiget interesse, er dette ikke slik med forordningen. Allerede etter den gamle personopplysningsloven hadde man gått bort fra en slik forståelse.

4.5.2 Rettslig forpliktelse

GDPR art. 6 bokstav c angir at personopplysninger kan behandles når det er nødvendig for å oppfylle en «rettslig forpliktelse» som den behandlingsansvarlige er underlagt. Her er art. 6 nr. 3 meget relevant, der det står at det også må finnes hjemmel i unionsretten eller nasjonal rett for at det er hjemmel for behandlingen. Der er ikke tilstrekkelig at vilkårene i art. 6 nr. 1 foreligger. Se PVN-2020-13 om Arendal kommunes behandling av personopplysninger i kartleggingsverktøyet Spekter som omhandlet klage fra Arendal kommune på Datatilsynets vedtak der tilsynet nedla forbud mot behandling av personopplysninger innhentet ved bruk av dataprogrammet, og påla kommunen å slette de innhentede personopplysningene. Datatilsynet konkluderte blant annet med at særlovgivning i lov 17. juli 1998 nr. 61 om grunnskolen og

den videregående opplæringa kap. 9A ikke ga tilstrekkelig supplerende rettsgrunnlag, jf. personvernforordningen art. 6 nr. 3. Nemda poengterte at Arendal kommune har behandlingsgrunnlag for personopplysningene i dataprogrammet i personvernforordningen art. 6 nr. 1 bokstav c, jf. opplæringsloven kap 9A. Ettersom dataprogrammet ikke kartlegger særlige kategorier av personopplysninger, kommer ikke forordningens artikkel 9 til anvendelse. Det ble videre konkludert med at kommunen ikke oppfylte de øvrige reglene i personvernforordningen, herunder prinsippene for behandling av personopplysninger i art. 5 nr. 1, og reglene om de registrertes rettigheter i forordningen kap. III. For å benytte dataprogrammet i fremtiden må kommunen etablere internkontrolldokumentasjon og rutiner som sikrer etterlevelse av personvernforordningen, blant annet også når det gjelder informasjon til elevene og retten til innsyn.

4.5.3 Offentlig sektor

Bestemmelsens bokstav e er spesielt praktisk viktig for offentlig sektor som har hjemmel i egen lov. Den hjemler oppgaver som er nødvendig for allmenhetens interesser eller utøving av offentlig myndighet som den behandlingsansvarlige er pålagt. Art. 6 nr. 3 kommer i tillegg, slik at behandlingen også krever hjemmel i nasjonal lovgivning. Der det offentlige ikke utøver offentlig myndighet vil andre bestemmelser være mer relevante. Dette kan f.eks. skje der det offentlige er arbeidsgiver. Bestemmelsen kan også brukes av private dersom vilkårene foreligger.

4.5.4 Nasjonal lovgivning

Art. 6 nr. 2 angir at den enkelte stat kan opprettholde eller innføre mer spesifikke og detaljerte bestemmelser for behandlinger som er hjemlet i art. 6 nr. 1 bokstav c eller e. Det finnes flere lover og reguleringer på disse områdene. Forordningens prinsipper må ivaretas også på disse områder.

Hjemmel i art. 6 nr. 1 bokstav c eller e ikke er nok i seg selv, og at det i tillegg kreves hjemmel i nasjonal rett eller unionsretten. Det mest praktiske er at det foreligger hjemmel i nasjonal rett. I henhold til fortalepunkt 41 er det ikke alltid nødvendig med en «regelverksakt». I Prop. 56 LS (2017-2018) står det at lov- og forskriftsbestemmelser kan være supplerende rettsgrunnlag. Det står også at vedtak fattet i medhold av lov eller forskrift er tilstrekkelig.

4.6 Særlige kategorier av personopplysninger

4.6.1 Generelt

GDPR art. 9 nr. 1 angir at behandling av særlige kategorier av personopplysninger. Tidligere kalte man dette sensitive opplysninger, og begrepet er fremdeles mye i bruk. Behandlinger som ikke kan hjemles i en av artikkelens alternativer, er ikke lovlige. Særlige kategorier av personopplysninger er underlagt spesielle krav fordi de er spesielt sensitive. Fortalepunkt 51 angir at selv om begrepene «rasemessig eller etnisk opprinnelse» brukes i ordlyden, innebærer ikke dette at EU godtar teorier om at det finnes ulike menneskeraser. I hovedsak har ordlyden samme innhold som det tidligere personopplysningsregelverket, selv om det er noen ulikheter. Genetiske opplysninger og biometriske opplysninger omfattes nå av regelverket. Fortalepunkt 51 slår fast at fotografier ikke automatisk er å anse som behandling av særlige kategorier av personopplysninger. Slik informasjon, bilder, kan være biometriske opplysninger når det er mulig å entydig identifisere eler å autentisere en person.

4.6.2 Behandlingsgrunnlag

Behandlingsgrunnlaget for særlige kategorier av personopplysninger fremgår av GDPR art. 9 nr. 2, som oppgir flere alternative grunnlag. For noen kreves i tillegg i art. 9 nr. 2, at det finnes hjemmel i nasjonal rett eller unionsrett. Prop. 56 LS (2017-2018) angir på s. 40 at det kreves enten lov eller forskrift eller vedtak med hjemmel i slike. Forarbeidene diskuterer også om det kreves en sterkere nasjonal hjemmel etter art. 9 nr. 2 enn etter art. 6 nr. 3, ettersom denne angår særlige kategorier av personopplysninger. Det ville følge naturlig av legalitetsprinsippet, men forarbeidene konkluderer ikke på dette. Dog pekes det på at personopplysningenes sensitivitet teller inn i vurderingen av et inngreps art og omfang, og at det har betydning for hvilke krav man kan stille, og må stille, til en inngrepshjemmel.

4.6.3 Arbeids-, trygde- og sosial rett

Dersom den behandlingsansvarlige eller den registrerte har forpliktelser innenfor områdene arbeidsrett, trygderett eller sosial rett, kan dette hjemle behandling av særlige personopplysninger. Det kreves at dette er stadfestet i nasjonal rett, tariffavtale eller unionsretten. Videre må den registrerte gis nødvendige garantier for vedkommendes rettigheter og interesser, jf. art. 88. Norsk rett har flere regelverk og særlover som dekker

disse områdene. Eksempelvis bestemmelsene om arbeidsgivers adgang til å lese anattes e-post som tidligere sto i den gamle personopplysningsloven, og nå står i aml. § 9-5.[17]

4.6.4 Forhold til rettskrav

Der behandlingen av særlige kategorier av personopplysninger er nødvendig for å fastsette, gjøre gjeldende eller forsvare et rettskrav, kan bestemmelsen brukes. Det samme gjelder når domstolene handler innenfor rammen av sin domsmyndighet. Bestemmelsen er relevant der rettskravet det gjelder, angår den behandlingsansvarlige, den registrerte eller eventuelt en tredjepart. Bestemmelsen er åpen i ordlyden om hvem som kan benytte den og den vil derfor antakelig også kunne brukes av advokater og rettshjelpere i rettslige prosesser og ved juridisk rådgivning. For domstolene kan den hjemle behandling av personopplysninger om parter i en sak, samt om tredjepersoner.

4.7 Beskyttelse mot automatisert databehandling

Bestemmelsen angir i utgangspunktet en rett for individet til å ikke bli utsatt for avgjørelser som utelukkende baseres på automatiserte behandlinger, herunder profilering med rettsvirkning av en bestemt grad på den enkelte. Hovedregelen i nr. 1 modifiseres av artikkelens nr. 2-4, der det angis at det på bestemte betingelser likevel kan utføres slik automatisk behandling. Artikkel 29-gruppen har utgitt en retningslinje for automatiske avgjørelser og profileringer, se «Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251 (rev. 01)». Merk at det er en rekke kriterier som må være oppfylt for at bestemmelsen skal få anvendelse, ikke enhver profilering faller inn under bestemmelsens virkeområde.

Artikkel 29-gruppen angir i sin retningslinje for automatiske avgjørelser og profilering at nr. 1 skal forstås som et forbud mot å fatte avgjørelser som utelukkende baserer seg på automatisert behandling. Merk at hvorvidt dette faktisk er et forbud, er debattert. Gitt at det er et forbud, vil det avgjørende for å avgjøre om forbudet gjelder eller ikke, være hvorvidt behandlingen har rettsvirkning eller på tilsvarende måte i betydelig grad påvirker vedkommende. Det er også vesentlig at det foreligger en «avgjørelse», noe som for eksempel medfører at enkel markedsføring på bakgrunn av profilering som regel ikke vil omfattes bestemmelsen ettersom ingen avgjørelse treffes. På den annen side angir fortalepunkt 71 at dersom et individ får

[17] Lov 17. juni 2005 nr. 62 – arbeidsmiljøloven, aml.

automatisk avslag på søknad om kreditt, eller avvises fra en mulig stilling, så vil dette være en avgjørelse omfattet av art. 22. Dersom en behandling har «rettsvirkning» på den registrertes rettigheter, vil behandlingen være omfattet. Andre avgjørelser som «på tilsvarende måte i betydelig grad påvirker vedkommende», kan være økonomiske konsekvenser for den enkelte. Det må gjøres en konkret vurdering der individets situasjon og egenskaper kan spille inn. Dersom bestemmelsen får anvendelse, er den registrerte gitt en rekke rettigheter, se nærmere art. 12, 13 nr. 2 bokstav f og 14 nr. 2 bokstav g.

I art. 22 nr. 2 bokstav b blir det poengtert at dersom behandlingen baseres på avtale, lovhjemmel eller samtykke, angir bestemmelsen at en automatisk individuell avgjørelse ofte kan benyttes, samt profilering. Bestemmelsen har stor betydning for offentlige myndigheter, som normalt baserer mange av sine behandlinger på lovhjemmel.

I art. 22 nr. 4 fremkommer det at avgjørelsene fattet med hjemmel i nr. 2 ikke skal bygge på særlige kategorier av personopplysninger nevnt i art. 9 nr. 1, med mindre art. 9 nr. 2 bokstav a eller g får anvendelse og det er innført egnede tiltak for å verne den registrertes rettigheter, friheter og berettigede interesser. Handlingsrommet for behandling som er nødvendig av hensyn til viktige samfunnsinteresser er således snevert.

Det kan av dette utledes at hovedregelen for automatisert behandling av personopplysninger er at dette ikke skal forekomme, med mindre hjemmelens krav er møtt. Et betydelig skille mellom hjemmelens formål og behandlingsprosessen er at denne i hovedsak baserer seg på at den registrerte informasjonen innsamles og prosesseres i en automatisk prosess ut fra angitte vilkår. Slik løsningen fungerer i dag er det manuell innsamling og manuell behandling og gjennomgang av mottatt informasjon hos de offentlige etatene. Ved å implementere Kontrollinformasjon-løsningen vil derimot bankene ikke lengre ha kontroll over hvordan de offentlige etater innsamler, bearbeider og behandler denne informasjonen, og en tilpasset automatisk prosessering kan derfor utvikles av etatene. Som rapporteringspliktig vil bankene miste kontrollen over hvordan informasjon registreres og utleveres.

Eksistensen av en offentlig interesse i å gi tilgang til og tillate innsamling av store mengder skattedata betyr ikke nødvendigvis eller automatisk at det også er en offentlig interesse i å formidle en mengde slik rådata i uendret form uten noe analytisk innspill, jf. Satakunnan Markkinapössi Oy and Satamadia Oy v. Finland [GC], 2017 §§ 172-178, 198.

5 Nasjonal lovgivning

5.1 Generelle plikter

Finansforetak utleverer i dag opplysninger om kundenes gjeld og formue direkte til Skatteetaten én gang per år. Eventuelle formuesforhold (investering i kryptovaluta, utenlandsk beholdning, mv.) som ikke fremkommer av finansforetakenes opplysninger er det hver enkelt person sitt ansvar å melde inn selv. Systemet er i stor grat tillitsbasert.

Eventuelle muligheter til å gi offentlige myndigheter tilgang til å gå rett inn i kunders transaksjonshistorikk for å hente ut spesifikke opplysninger vil kunne regnes som et brudd på denne tilliten.

5.2 Skatteforvaltningsloven

Skattemyndighetene har etter skatteforvaltningsloven § 10-2 hjemmel til å innhente opplysninger som kan ha betydning for noens skatteplikt.

I lovens forarbeid, Prop. 38 L (2015-2016) er det konkretisert noen begrensninger om opplysningsplikten som er hjemlet i lov.

I begrepet tredjepart ligger det også en begrensning ved at det må være en tilknytning mellom den det ønskes opplysninger om og den det bes om opplysninger fra. Dette vil for eksempel være tilfelle der tredjeparten har kjøpt varer eller tjenester fra, eler har inngått andre avtaler med, den som myndighetene krever opplysninger om. Det kan derimot ikke kreves kontrollopplysninger fra en aktør som bare er i en sammenlignbar situasjon som, men ikke har noen øvrig forbindelse med, den som opplysningene gjelder. Når skattemyndighetene krever opplysninger etter § 10-2 første ledd må de videre kjenne til et bestemt navn på et kontrollobjekt eller en bestemt transaksjon, mv.

Den generelle hovedregelen om plikt til å gi kontrollopplysninger gjelder imidlertid bare for tredjeparter som er næringsdrivende. Begrensningene fra ligningsloven og merverdiavgiftsloven i privatpersoners plikt til å gi kontrollopplysninger som tredjeparter ble foreslått videreført og gjort generelle. Privatpersoner skal bare ha plikt til å gi opplysninger i nærmere bestemte tilfeller. Dette gjelder opplysninger om arbeid på bygg og anlegg, om tilgodehavende og gjeld som navngitt person mv. har, om utleie mv. av fast eiendom, om mellommenn som vedkommende har gitt oppdrag, samt om utbetalt lønn eller annen godtgjøring for arbeid.

I utgangspunktet må myndighetene kjenne til et bestemt navn eller en bestemt transaksjon mv. for å kunne kreve opplysninger. Kontroll hvor verken bestemte navn eller transaksjoner er angitt kan kun utføres overfor næringsdrivende. I Prop. 141 L (2011-2012) punkt 2.5.1.6 er det nevnt som eksempel at myndighetene innhenter informasjon om all kortbruk med tilknytning til utenlandske betalingskort brukt i Norge over en viss periode. Denne typen kontroller skiller seg fra kontroller hvor det bes om opplysninger om bestemte skattepliktige eller bestemte transaksjoner. I enkelte tilfeller vil det kunne bes om en betydelig mengde informasjon fra tredjepartene, og kontrollene vil da kunne kreve betydelige ressurser hos de opplysningspliktige. Dette er bakgrunnen for at det er oppstilt vilkår om særlig grunn. Departementet har understreket at det ved målretting av kontroller er særlig viktig at myndighetene foretar en forholdsmessighetsvurdering av hvilken nytte de innhentede opplysningene antas å ha for etaten, holdt opp mot den byrde som pålegges de opplysningspliktige.

Selv om statens skjønnsmargin i skattespørsmål er bredere når det gjelder beskyttelse av rent økonomiske data som ikke inkluderer data som er personlig eller nært knyttet til identiteten til den registrerte, jf. G.S.B. v. Switzerland, 2015, § 93, så kommer privathensyn inn i situasjoner der skatteopplysninger er utarbeidet om en spesifikk person, eller hvor de er offentliggjort på en måte eller i en grad som går utover det den registrerte med rimelighet kunne ha forutsett, jf. M.N. and Others v. San Marino, §§ 52-53, Satakunnan and Satamedia Oy v. Finland, § 136.

5.3 Hvitvaskingsloven

Etter hvitvaskingsloven § 26 har Økokrim krav på opplysninger i forbindelse med mistanke om hvitvasking og terrorfinansiering. Det er kun Enheten for Finansiell Etterretning (EFE) som har adgang til å benytte denne lovhjemmelen for å etterspørre opplysninger. Politiet kan ikke be om kunde- eller transaksjonsinformasjon med hjemmel i denne lov.

Bestemmelsen gjennomfører deler av fjerde hvitvaskingsdirektiv (EU) 2015/849 artikkel 32, 33 og 34 og FATF-anbefaling 20 og deler av anbefaling 29.[18]

[18] Prop. 40 L (2017-2018) pkt 6.7.2

I høringen har Økokrim etterspurt en klar lovforankring av adgangen til å utlevere opplysninger til Økokrim som ledd i innhenting av ytterligere opplysninger fra rapporteringspliktige. Det ble da påpekt at det vil fremgå indirekte av hvitvaskingsloven § 26 at Økokrim etter omstendighetene må gi opplysninger som kan være underlagt taushetsplikt i forbindelse med begjæring om ytterligere opplysninger. Behovet for en ytterligere presisering vil kunne vurderes på et senere tidspunkt.

Departementet foreslo en bestemmelse om ansvarsfrihet for oversendelse av opplysninger i god tro til Økokrim, og plasserte denne i samme paragraf som reglene om rapporterings- og opplysningsplikt, § 26 fjerde ledd. Ansvarsfriheten skal forstås slik at det dekker uaktsom, men ikke grovt uaktsom, villfarelse om plikten til å oversende opplysninger. For å avskjære eventuell tvil om hva som ligger i kravet til «god tro», ble det foreslått å presisere at ansvarsfriheten ikke gjelder ved grov uaktsomhet.

Det ble i lovforslaget understreket at FATF-anbefaling 21 bokstav a uttrykkelig omtaler at ansvarsfriheten skal gjelde der rapporteringspliktig «did not know precisely what the underlying criminality was», og uavhengig av om det overhodet har skjedd noen illegal aktivitet. Dette skal legges til grunn ved forståelsen av regelen om ansvarsfrihet i § 26.[19]

I høringen av lovforslaget har Datatilsynet anført at utvalgets utkast til bestemmelse som uttrykkelig gir grunnlag for behandling av personopplysninger, ikke er klar nok eller gir nødvendige garantier for å sikre at kun personopplysninger som er nødvendige og proporsjonale å behandle, blir behandlet. Dette gjelder blant annet sensitive opplysninger.[20]

Departementet presiserte at adgangen til å behandle personopplysninger må sees i sammenheng med lovens forpliktelser. Hva forpliktelsene går ut på, eksempelvis indentifisering av kunde og reell rettighetshaver, vurdering av kundeforholdets formål og tilsiktede art mv., vil dermed være styrende for hvilke opplysninger som kan registreres. I denne sammenheng ble forskriftsregulering ansett for å være mer hensiktsmessig enn lovregulering på dette punktet, dels fordi vurderingene av hva som er nødvendige og proporsjonale opplysninger kan endre seg, og dels på grunn av detaljnivået.

---

[19] Prop. 40 L (2017-2018) pkt. 6.7.4

[20] Prop. 40 L (2017-2018) pkt. 7.2.6.4

En del av opplysningene som det er adgang til å innhente etter hvitvaskingsregelverket kan også lovlig innhentes med grunnlag i annen lovgivning. Ett eksempel er foretak underlagt opplysningsplikten i skatteforvaltningsloven § 7-3 med tilhørende forskrift. Disse foretakene skal blant annet innhente opplysninger om kontohaver og reell rettighetshaver, og vil i en del tilfeller kunne legge til grunn opplysninger som allerede er innhentet etter hvitvaskingsloven. Det skal ikke være nødvendig å innhente opplysninger om kunde to ganger, bare fordi opplysningene skal innhentes med grunnlag i ulike regelsett. Et annet eksempel er krav om lagring av opplysninger om kunden, eksempelvis transaksjonsinformasjon som ledd i løpende oppfølging. Bokføringsregelverket kan medføre krav om at transaksjonshistorikk oppbevares lengre enn det hvitvaskingsregelverket krever. Tilsvarende vil kunne gjelde for en del andre opplysninger i andre sammenhenger.[21]

Ved utarbeidelse av lovforslaget ble det foreslått at behandling av sensitive personopplysninger forutsetter hjemmel i forskrift. Det bør vurderes nærmere hvilke typer sensitive opplysninger som kan behandles i hvilke tilfeller. Forskrift for å regulere dette ble bestemt å forberede etter at lovforslaget ble vedtatt, og foreligger foreløpig ikke.

I visse tilfeller skal det også gjøres unntak fra retten til innsyn i registrerte opplysninger, jf. § 32. Selv om det foreligger gode grunner til å unnta opplysninger fra retten til innsyn, er det nødvendig at disse konkretiseres. Personvernforordningen stiller også strengere krav til unntak fra retten til innsyn, enn det som gjelder etter personverndirektivet.

Unntaksadgangen er presisert til å gjelde opplysninger omfattet av avsløringsforbudet i § 28 første ledd. I tillegg skal opplysninger innhentet gjennom undersøkelsene unntas fra innsyn. Dette dekker blant annet situasjoner der Økokrim gir rapporteringspliktig tilbakemelding om bruken av rapporterte opplysninger.

En lignende angivelse av unntaket fra retten til innsyn er også vedtatt i svensk rett.

Rapporteringspliktige bør ikke gi innsyn i andre opplysninger som kan vanskeliggjøre etterlevelse av denne loven, etterforskning eller lignende undersøkelser, jf. fjerde

[21] Prop. 40 L (2017-2018) pkt. 7.2.6

hvitvaskingsdirektiv artikkel 41. Tilstrekkelig spesifisering av hvilke opplysninger som kan og ikke kan unntas fra retten til innsyn, vil bli regulert nærmere i forskrift.

Den rapporteringspliktige skal gi Økokrim andre nødvendige opplysninger på forespørsel, uavhengig av om vedkommende har rapportert det aktuelle forholdet på forhånd, jf. § 26 første ledd andre punktum. Opplysningene Økokrim ber om må være «nødvendige». Dette innebærer at de må ha tilknytning til konkret informasjon om hvitvasking eller terrorfinansiering som Økokrim sitter på. Det er Økokrim som vurderer nødvendigheten, og det skal dermed ikke foretas en selvstendig vurdering hos rapporteringspliktige ved slike forespørsler.[22]

Oversendelse av opplysninger til Økokrim i god tro medfører ikke brudd på taushetsplikt og gir ikke grunnlag for erstatningsansvar eller straffansvar, med mindre det foreligger grov uaktsomhet, jf. § 26 fjerde ledd. Dette gjelder både taushetsplikt som medfølger av kontrakt, lov og administrative bestemmelser. Bestemmelsen skal forhindre at den rapporteringspliktige avstår fra å rapportere når det er tvil om en rapportering vil krenke taushetsplikten. Den innebærer at det blant annet er ansvarsfrihet når følgende uriktige vurderinger ligger til grunn for en rapportering:

- Uriktige vurderinger av grunnlaget for mistanke eller uriktig tolkning av hva som ligger i kravet til mistanke
- Uriktig vurdering av om det foreligger straffbar hvitvasking eller terrorfinansiering, eller en feiltolkning av disse straffebudene
- Man har feilaktig vurdert at hvitvaskingsloven kommer til anvendelse

Kravet til «god tro» innebærer at man kan stilles til ansvar dersom man vet at rapporteringen til Økokrim er uriktig. Det samme gjelder dersom man opptrer grovt uaktsomt. Det er en høy terskel, og ansvarsfriheten rekker langt. Ansvarsfriheten gjelder alle opplysninger oversendt Økokrim i medhold av både rapporteringsplikten og plikten til å gi tilleggsopplysninger og nødvendige opplysninger.[23]

[22] RFT-2019-8 pkt. 621

[23] RFT-2019-8 pkt. 6.2.2

Hvitvaskingsloven § 31 (3) gir mulighet til, men ikke en plikt til, å få angitt opplysninger vedrørende KYC-besvarelser hos finansinstitusjoner. Det er opp til hver institusjon om, og hvor mye, av denne informasjonen de ønsker å dele.[24]

5.4 Straffeprosessloven

Straffeprosessloven § 210 gir domstolene og påtalemyndigheten adgang til å be om utlevering av opplysninger som kan antas å ha betydning som bevis i en sak. I paragrafens tredje ledd er det også påpekt at dersom sterke allmenne hensyn tilsier at utlevering skjer, kan pålegg om utlevering gis uten hensyn til om det er åpnet etterforskning i en straffesak.

Etter gjeldende rett kan besitteren av ting som antas å ha betydning som bevis, pålegges å utlevere denne, jf. § 210 første ledd. Utleveringspålegg kan utferdiges i alle sakstyper, men kan ikke rettes mot personer som er fritatt for vitneplikt eller mot mistenkte selg.

Utleveringspålegg kan besluttes av retten. Politiet har imidlertid hastekompetanse etter § 210 annet ledd. Politiets beslutning skal snarest mulig forelegges for retten for godkjennelse.

Mistenkte skal underrettes om at det er fattet beslutning om utleveringspålegg, jf. § 53 første ledd, jf. § 52 annet ledd. Dersom det er strengt nødvendig for etterforskningen i saken at underretning ikke gis, kan retten på nærmere vilkår treffe kjennelse om utsatt underretning, jf. § 210 a.[25]

5.5 Folketrygdloven

Etter folketrygdloven § 21-4 har NAV adgang til å innhente opplysninger om transaksjoner og saldo, og eventuelt etterspørre ytterligere opplysninger.

Bestemmelsen gjelder rett til å innhente opplysninger uten hinder av taushetsplikten som ledd i sin behandling av om vilkårene for en ytelse er til stede, eller ved etterfølgende kontroll av innvilget ytelse.

[24] DSOP Aktivitetsrapport 2021, s. 13

[25] Prop. 68 L (2015-2016) kap. 10-2

Forutsetningen for retten til å innhente opplysninger er at den særskilt angitte personen / instansen besitter opplysningene. I kontrolløyemed vil det også være relevant å få utlevert kontoutskrifter fra banken.

Hjemmelen etter ftr. § 21-4 a er med vidtgående med hensyn til hvem opplysningene kan hentes fra. I motsetning til § 21-4 gjelder § 21-4 a «enhver».

Vilkårene for å innhente opplysninger etter §§ 21-4 og 21-4 a er formulert forskjellig. Det skal mer til for å benytte § 21-4 a, selv om det også er en viss overlapp.

Det fremkommer ikke i lovtekst eller forarbeider noen spesifisering av hvilken informasjon som det er adgang til å opplyse. Hovedgrunnlaget er at de har rett til å innhente de opplysninger som er nødvendige for å kontrollere om vilkårene for en ytelse er oppfylt, vil kunne være oppfylt eller har vært oppfylt i tilbakelagte perioder, eller for å kontrollere utbetalinger etter en direkte oppgjørsordning.[26]

6 Avsluttende bemerkninger

Som det fremkommer av Personvernforordningen er det stilt strenge krav til innsamling, oppbevaring og deling av personsensitive opplysninger.
Gjeldende bestemmelser i nasjonal rett levner ikke tvil om at banker har en rapporteringsplikt dersom formålet kan begrunnes i konkret lovhjemmel, men åpner ikke for noen direkte tilgang til bankenes systemer. Finansinstitusjonene har også en forpliktelse overfor sine kunder for behandling av deres kundeopplysninger.
For å sikre bankkunders personvern vil det derfor være fordelaktig om DSOP Kontrollinformasjon-løsningen ble implementert etter hjemmel i lov, og det er derfor nødvendig å utrede dette nærmere.

[26] Lovkommentar fra Karnov, Imran Haider – Advokat LO, 11. oktober 2021.

Referanseliste

Norske lover

Kongeriket Norges Grunnlov, Lov 17. mai 1814

Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven)

Lov 5. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven)

Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven)

Lov 27. mai 2016 nr. 14 om skatteforvaltning (skatteforvaltningsloven)

Lov 01. juni 2018 nr. 23 om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsloven)

Lov 28. februar 1997 nr. 19 om folketrygd (folketrygdloven)

Lov 18. juni 1965 nr. 4 om vegtrafikk (vegtrafikkloven)

Lov 17. juli 1998 nr. 61 om grunnskolen og den vidaregåande opplæringa (opplæringslova)

Lovforarbeider og offentlige utredninger

NOU 2009:15 Skjult informasjon – åpen kontroll. Metodekontrollutvalgets evaluering av lovgivningen om politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker.

Prop. 56 L S (2017-2018) Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen.

Prop. 38 L (2015-2016) Lov om skatteforvaltning (skatteforvaltningsloven)

Prop. 141 L (2011-2012) Endringer i ligningsloven og merverdiavgiftsloven mv. (kontrollbestemmelser og personalliste)

Prop. 68 L (2015-2016) Endringer i straffeprosessloven mv. (skjulte tvangsmidler)

Stortingsdokumenter

Meld. St. 27 (2015-2016) Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet. Tilråding fra Kommunal- og moderniseringsdepartementet 15. april 2016, godkjent i statsråd samme dag.

Høyesterettsavgjørelser

Rt. 1933 s. 212

Rt. 1995 s. 539 - Fjordlaksdommen

Internasjonale konvensjoner

Europarådets konvensjon av 14. november 1950 om beskyttelse av menneskerettighetene og de grunnleggende friheter (Den europeiske menneskerettighetskonvensjonen eller EMK)

De forente nasjoners internasjonale konvensjon 16. desember 1966 om sivile og politiske rettigheter.

Avgjørelser fra EMD

B. v. France, 1992	Case of B. v. France [plenary session] no. 57/1990/248/319
Söderman v. Sweden, 2013	Söderman v. Sweden [GC] no. 5786/08
Nunez v. Norway, 2011	Case of Nunez v. Norway [fourth section] no. 55597/09
Aksu v. Turkey, 2012	Case of Aksu v. Turkey [GC] no. 4149/04 and 41029/04
Fernandez Martines v. Spain, 2014	Case of Fernández Martínez v. Spain [GC] no. 56030/07
S.J.P and E.S. v. Sweden, 2018	Case of S.J.P. and E.S v. Sweden [fourth section] no. 8610/11

Robathin v. Austria, 2012	Case of Robathin v. Austria [first section] no. 30457/06
Big Brother Watch and Others v. The United Kingdom, 2021	Case of Big Brother Watch and Others v. The United Kingdom [GC] no. 58170/13, 62322/14 and 24960/15
Frérot v. France, 2007	Affaire Frérot v. France [second section] no. 70204/01
Centrum for Rättvisa v. Sweden, 2018	Case of Centrum for Rättvisa v. Sweden [third section] no. 35252/08
M.N. and Others v. San Marino, 2015	Case of M.N. and Others v. San Marino [third section] no. 28005/12
G.S.B. v. Switzerland, 2015	Case of G.S.B. v. Switzerland [third section] no. 28601/11
Satakunnan and Others v. Finland, 2017	Case of Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [GC] no. 931/13

Avgjørelser fra EU-domstolen

ECJ sak C-293/12	Digital rights Ireland Ltd. v. Ministerfor Communications, Marine and natural Resources and Others and Kärntner Landesregierung and Others, ECLI:EU:C:2014:238

EU- og EØS rettsakter

Traktat om Den Europeiske Union

EU Charter of Fundamental Rights

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 samt om oppheving av direktiv 95/46/EF (generell personvernforordning)

Fjerde hvitvaskingsdirektiv (EU) 2015/849 – Europaparlaments- 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, om endring av europaparlaments- og rådsforordning (EU) nr. 648/2012 og om oppheving av europaparlaments- og rådsdirektiv 2005/60/EF og kommisjonsdirektiv 2006/70/EF (fjerde hvitvaskingsdirektiv)

Juridisk litteratur

Jarbekk, Eva og Simen Sommerfeldt, *Personvern og GDPR i praksis*, 1. utgave, 5. opplag, Cappelen Damm AS, 2019

Jarbekk, Eva, *Personopplysningsloven og personvernforordningen (GDPR) med kommentarer*, 1. utgave, 1. opplag, Gyldendal Norsk Forlag AS, 2019

Andre kilder

RFT-2019-8, rundskriv fra Finanstilsynet. Veileder til hvitvaskingsloven.

DSOP aktivitetsrapport 2021 - https://www.bits.no/document/dsop-aktivitetsrapport-for-2021/ (02.05.2022)

Personvernnemdas vedtak PVN-2020-13, dato 09.11.2020

WP 251 rev.01 – Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 6. February 2018, Artikkel 29-gruppen

FATF-anbefaling 21 – Financial Action Task Force (FATF), *Internal standards on combating money laundering and the financing of terrorism and proliferation,* The FATF Recommendations, 2012

Datatilsynet – Veiledning for Vurdering av personvernkonsekvenser, https://www.datatilsynet.no/regelverk-og-skjema/veiledere/vurdering-av-personvernkonsekvenser/

https://snl.no/den_europeiske_menneskerettskonvensjon (sist sjekket 02.05.2022)

https://snl.no/legalitetsprinsippet (sist sjekket 02.05.2022)

https://jusleksikon.no/wiki/Proporsjonalitetsprinsippet (sist sjekket 02.05.2022)

https://lovdata.no/artikkel/domstoler_maktfordeling_og_uavhengighet/1468 (sist sjekket 02.05.2022)

https://www.idunn.no/doi/10.18261/issn.1504-3126-2021-04-01 (sist sjekket 02.05.2022)