Rettslige rammer for å ta i bruk skytjenester

Hvilke konsekvenser har Schrems II-dommen for bruken av skytjenester for kommuner?

Kandidatnummer: 180

Antall ord: 14 355

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

10. mai 2021

Forord

Denne masteroppgaven er et resultat av det avsluttende arbeidet av integrert master i rettsvitenskap på Universitetet i Bergen. Bakgrunnen for valget av oppgaven er aktualiteten rundt skytjenester i offentlig og kommunal sektor. Bruken av skytjenester er økende og Schrems II-dommen, som kom sommeren 2020, har problematisert de rettslige rammene for overføringer av personopplysninger.

Arbeidet med masteroppgaven har vært en langvarig prosess. Prosessen har vært interessant, utfordrende og lærerik. Denne masteroppgaven ville ikke vært levert uten all god bistand underveis. I den forbindelse vil jeg gjerne takke alle dere som har bidratt å ferdigstille denne masteroppgaven. Ingen nevnt, ingen glemt. Trass dette, er det noen jeg vil rette en ekstra takk til.

Først og fremst vil jeg takke Håvard Reknes hos Direktoratet for forvaltning og økonomistyring (DFØ) for et fantastisk samarbeid. Håvard har bidratt med både viktige perspektiver, innspill, informasjon og kontaktpersoner som har gjort det mulig å fullføre masteroppgaven på en god måte.

Jeg vil også takke veilederen min som har tatt seg tid til å lese tekstutkastene mine med grundighet, samt kommet med konstruktiv kritikk og oppmuntrende ord underveis.

Til slutt vil jeg takke informantene til kommunene og skyleverandøren som har vært til stor hjelp for å belyse et tema som fortsatt er uavklart samt gitt meg innsikt i hvordan problemstillingen påvirker kommuner i praksis.

Bergen, 10. mai 2021

Innholdsfortegnelse

1 Innledning

1.1 Tema og hovedproblemstilling

Tema for masteroppgaven er hvilke rammer personvernregelverket setter for kommuners bruk av skytjenester. Med dette menes hvilke muligheter og begrensninger særlig personvernforordningen (heretter GDPR)[1] og Schrems II-dommen (C-311/18)[2] gir for kommuner til å ta i bruk skytjenester. Dette er viktig fordi bruk av skytjenester har en rekke fordeler,[3] men det kan være vanskelig å vite om bruken av skytjenesten er lovlig. Hovedformålet med denne avhandlingen er å gi kommunene en forståelse av hvilke konsekvenser Schrems II-dommen har for bruken av skytjenester som er eller vil bli brukt av kommuner.

Avhandlingen vil særlig fokusere på å besvare følgende spørsmål:

- Hvilke juridiske vurderinger må kommuner foreta ved bruk av databehandlere i et land utenfor EU/EØS (heretter tredjeland)?
- Hvilke konsekvenser har Schrems II-dommen for de ulike skytjenestemodellene?
- Hvordan har produsentene og selgerne av skytjenester (heretter skyleverandørene) og kommuner tilpasset seg standarden satt i Schrems II-dommen?

1.2 Situasjonsbeskrivelse

1.2.1 Aktualitet

Kommuners rettslige rammer for å ta i bruk skytjenester er aktuelt blant annet som en følge av den teknologiske utviklingen i verden. Det kommer stadig ny teknologi og den eksisterende teknologien er konstant i utvikling. Et resultat av den teknologiske utviklingen, er økning i bruken av skytjenester hos kommuner. Denne bruken forventes å fortsette å øke.[4]

[1] 2016/679/EU: GDPR.
[2] Schrems II [GC] C-311/18.
[3] Hvorfor kommuner skal velge å ta i bruk skytjenester, vil bli redegjort for i kapittel 3.1.
[4] Nasjonal sikkerhetsmyndighet (2020) s. 31.

I tillegg har det vært et økende politisk søkelys på bruk av skytjenester, eksempelvis; nasjonal strategi for bruk av skytjenester[5] og digitaliseringsrundskrivet fra 2021[6]. I sistnevnte er det stilt krav om at offentlige virksomheter skal benytte skytjenester når det ikke foreligger spesielle hindringer for å ta i bruk skytjenester, og slike tjenester gir den mest hensiktsmessige og kostnadseffektive løsningen.[7] I den nasjonale strategien for bruk av skytjenester fremmes regjeringens ønske om å etablere en markedsplass for skytjenester.[8] Direktoratet for forvaltning og økonomistyring (DFØ) har en ledende rolle i dette arbeidet. Markedsplassens mål er å gjøre det enklere for virksomhetene å anskaffe sikre, lovlige og kostnadseffektive skytjenester.[9]

I tillegg er det en rekke fordeler med å ta i bruk en skytjeneste. Det kan gi økonomiske gevinster, økt kapasitet, bedre fleksibilitet, økt innovasjon og er mer miljøvennlig. Fordelene vil bli ytterligere utdypet i kapittel 3.1.

Skytjenester muliggjør også i større grad etablering av en global kundekrets. Under dybdeintervjuene med de utvalgte kommunene som ble gjennomført i februar og mars 2021, kom det frem at kommunene ofte bruker flere ulike amerikanske skyleverandører, blant annet Microsoft, AWS og Google. Funnene fra dybdeintervjuene er gjort rede for i kapittel 5. Når personopplysninger krysser landegrensene, kan det oppstå juridiske problemstillinger som kommunene må ta stilling til.

Den 16. juli 2020 avsa EU-domstolen den såkalte Schrems II-dommen som problematiserte de rettslige rammene for overføringer av personopplysninger til tredjelandet USA.[10] Juristen Max Schrems anla sak mot det irske datatilsynet og krevde at datatilsynet skulle stoppe overføringer av personopplysninger mellom Facebook Irland og Facebook Inc. i USA. EU-domstolen kom frem til at Privacy Shield, som tidligere muliggjorde overføring av personopplysninger til USA, er et ugyldig overføringsgrunnlag.[11] De begrunnet dette med at overvåkningspraksisen og regelverket i USA bryter retten til privatliv.[12] Domstolen uttalte

[5] Kommunal- og moderniseringsdepartementet (2016).
[6] Kommunal- og moderniseringsdepartementet (2021).
[7] Kommunal- og moderniseringsdepartementet (2021) punkt 1.11 siste avsnitt.
[8] Kommunal- og moderniseringsdepartementet (2016) s. 31.
[9] Direktoratet for forvaltning og ikt (2018) s. 3.
[10] Schrems II-dommen vil bli redegjort for i kapittel 4.1 og 4.2.
[11] Schrems II [GC] C-311/18, avsnitt 201.
[12] Schrems II [GC] C-311/18, avsnitt 168 flg.

også at Standard Contractual Clauses (SCC) er et gyldig overføringsgrunnlag, men forutsetter at ytterligere beskyttelsestiltak innføres.[13]

Dommen har satt ny standard for overføring av personopplysninger til tredjeland. I lys av dommen er overføringsgrunnlaget SCC blitt mer aktuelt for å kunne ta i bruk tjenester som overfører personopplysninger til tredjeland. Schrems II-dommen er derfor viktig for kommuner som ønsker å ta i bruk slike tjenester.

Det er således en rekke momenter som aktualiserer bruk av skytjenester. I denne avhandlingen skal kun de rettslige utfordringene som gjør seg gjeldende i forbindelse med Schrems II-dommen, analyseres. Avhandlingen presenterer ikke et fullstendig bilde av de juridiske problemstillingene som kan oppstå ved bruk av skytjenester.

1.2.2 Interessenter og behov

Avhandlingens interessenter er personer, grupper og organisasjoner som påvirkes av konsekvensene av Schrems II-dommen eller funnene i denne avhandlingen. Direkte interessenter er blant annet DFØ, kommuner, skyleverandører og innbyggerne i kommunene. I tillegg til direkte interessenter kan det være noen indirekte interessenter som også vil kunne påvirkes av problemstillingen og resultatene i avhandlingen. En indirekte interessenter kan eksempelvis være Datatilsynet og andre brukere av skytjenester.

Avhandlingen har kartlagt følgende behov for de direkte interessentene. Kommuner har behov for å forstå hvordan Schrems II-dommen påvirker deres bruk av skytjenester. De har behov for en trygghet om at personopplysningene blir ivaretatt, et tydelig lovverk, klargjøring av roller og ansvar, samt forutsigbarhet. Skyleverandører har behov for å forstå hvilke konsekvenser Schrems II-dommen har for deres kunder. Leverandørene har derfor behov for felles rammebetingelser, tydelig lovverk, klargjøring av roller og ansvar, samt forutsigbarhet siden dommen påvirker kundenes atferd. DFØ og markedsplassen har behov for å bli sett på som en attraktiv, troverdig og oppdatert aktør i det norske markedet med hensyn på skytjenester. Dette innebærer blant annet at de viser forståelse for hvordan Schrems II-dommen påvirker norske virksomheter i deres anskaffelsesprosess av skytjenester og hvilke

[13] Schrems II [GC] C-311/18, avsnitt 122 flg.

skytjenester som påvirkes. Innbyggerne i kommunene har behov for trygghet på at kommunene ivaretar deres personopplysninger ved bruk av skytjenester.

1.3 Rettskildebildet og metode

For å analysere problemstillingen i avhandlingen er det særlig Schrems II-dommen som er relevant. Schrems II-dommen har satt ny standard for overføring av personopplysninger til USA og andre tredjeland. I dommen vurderte EU-domstolen GDPR artikkel 45 og 46.[14] Disse to artiklene hjelmer regler for overføring av personopplysninger til tredjeland.[15] I etterkant av dommen har Personvernrådet kommet med oppklaringer rundt Schrems II-dommen.[16]

Analysen av EU/EØS-retten vil foretas ved hjelp av EU- og EØS-rettslig metode. Det vil også være relevant å se hen til nasjonale rettskilder. Analysen av de nasjonale kildene vil foretas ved hjelp av norsk juridisk metode.

Norge har forpliktet seg til en rekke EU-rettsakter gjennom EØS-avtalen. Utgangspunktet i norsk rett er at EØS-retten må gjennomføres i norsk lov for å danne grunnlag for rettigheter og plikter som kan håndheves av norske domstoler.[17] Det følger av EØS-avtalen artikkel 3 at «[a]vtalepartene skal treffe alle generelle eller særlige tiltak som er egnet til å oppfylle de forpliktelser som følger av denne avtale». EØS-avtalens hoveddel er gjennomført ved § 1 i EØS-loven.[18]

Ved tolkning av EU-rettsakter som er gjennomført i norsk rett, skal analysen foretas ved hjelp av EØS-rettslig metode. Bestemmelsene i den norske loven skal analyseres, men skal tolkes i en EØS-rettslig kontekst. En tolkning i EØS-rettslig kontekst innebærer å identifisere den EU-rettslige regelen, identifisere den EØS-rettslige regelen ved å vurdere eventuelle avvik fra den EU-rettslige regelen grunnet særegenheter i EØS-avtalen samt analysere den EØS-rettslige regelens gjennomslagskraft i norsk rett.[19] Analysen av bestemmelsene i den norske loven skal analyseres i tråd med norsk juridisk metode, samt se hen til EU-rettsaktene.

[14] Overføring av personopplysninger etter GDPR artikkel 49, ble ikke vurdert av EU-domstolen.
[15] Bestemmelsene for overføring av personopplysninger til et tredjeland, vil redegjøres for i kapittel 2.4.
[16] Analysen av Schrems II-dommen og veilederne fra Personvernrådet, vil bli redegjort for i kapittel 4. GDPR redegjøres for i kapittel 2.
[17] Fredriksen og Mathisen (2014) s. 273.
[18] Lov 27. november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven).
[19] Stemsrud (2015) s. 104.

I EU-retten utgjør de grunnleggende traktatene og de uskrevne rettsprinsippene, primærretten i EU.[20] Primærretten anses som den viktigste rettskilden i EU. Så langt det er mulig må sekundærretten tolkes i samsvar med primærretten.[21] Sekundærretten består av avledet regelverk, eksempelvis forordninger, direktiver og vedtak.[22]

Det er særlig tre kilder som EU-domstolen benytter seg av; bindende, skrevne rettskilder (eksempelvis GDPR), rettspraksis fra EU-domstolen og formålsorientert fortolkning av reglene («effet utile»).[23]

GDPR er en EU-forordning som skal «fastsette regler om vern av fysiske personer i forbindelse med behandling av personopplysninger samt regler om fri utveksling av personopplysninger», jf. artikkel 1. GDPR vil videre redegjøres for i kapittel 2.1. Forordningen ble i 2018 gjennomført i norsk rett gjennom en henvisningsbestemmelse i personopplysningsloven i tråd med forpliktelsene til Norge.[24] Kommunene må derfor forholde seg til personopplysningsloven som gjennomfører GDPR ved bruk av skytjenester som overfører personopplysninger til tredjeland.

Som nevnt er kontekst og formålsorient tolkning av EU-rettslige bestemmelser viktig. Kontekstuell tolkning innebærer at sammenhengen som den EU-rettslige teksten inngår i, er av betydning ved tolkningen av den.[25] Formålsrettet tolkning, «effet etile», innebærer at bestemmelsen skal tolkes slik at formålet fremmes i størst mulig utstrekning.[26]

Schrems II-dommen ble avsagt sommeren 2020 av EU-domstolen. Den handler om gyldighet av Privacy Shield og SCC samt betingelsene for overføring av personopplysninger til tredjeland. Domstolens vurderinger og konklusjoner vil redegjøres for i kapittel 4.

Det følger av Traktaten om Den europeiske union (heretter TEU) artikkel 19 nr. 1 at EU-domstolen er den øverste vokter av «lov og ret».[27] EU-domstolens oppgaver er å avgjøre tvister som bringes inn, samt avklare og utvikle EU-rettens innhold.[28] EU-domstolens

[20] Fredriksen og Mathisen (2014) s. 32.
[21] Ibid.
[22] Fredriksen og Mathisen (2014) s. 22.
[23] Stemsrud (2015) s. 105.
[24] Lov 16. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven).
[25] Fredriksen og Mathisen (2014) s. 222.
[26] Fredriksen og Mathisen (2014) s. 236.
[27] Traktaten om Den europeiske union (TEU).
[28] Fredriksen og Mathisen (2014) s. 124.

avgjørelser anses ikke som bindende for verken nasjonale domstoler, Underretten eller EU-domstolen selv, men det kreves gode grunner for å fravike slike tungtveiende rettskilder.[29]

Schrems II-dommen er en prejudisiell avgjørelse (også kalt forhåndsavgjørelse) fra EU-domstolen. Den irske domstolen ba EU-domstolen om en slik forhåndsavgjørelse. I tvilsspørsmål er det obligatorisk at nasjonale domstoler ber EU-domstolen om en uttalelse av hvordan EU-retten skal tolkes. Uttalelsen fra EU-domstolen vil da fungere som en prejudisiell avgjørelse og er i utgangspunktet bindende for den nasjonale domstolen og eventuelle ankeinstanser.[30] EØS-avtalen sin overordnede målsetting om å integrere statene i Det europeiske frihetsforbund (EFTA)[31] i EUs indre marked.[32] Dette forutsetter at EØS-regelverket som er hentet fra EU-retten, tolkes og anvendes likt som innenfor EU.[33] Dette prinsippet om ensartethet eller homogenitet, omtales som homogenitetsprinsippet.[34] På grunn av homogenitetsprinsippet og det faktum at Schrems II-dommen er en prejudisiell avgjørelse om hvordan EU-retten skal forstås, må kommuner forholde seg til dommen ved bruk av skytjenester som overfører personopplysninger til tredjeland.

Den 10. november 2020 publiserte Personvernrådet utfyllende veiledere om Schrems II-dommen. I dokumentet Recommendations 01/2020 presenterer Personvernrådet veiledning som skal foretas i seks steg ved overføring av personopplysninger til et tredjeland.[35] I dokumentet Recommandations 02/2020 har Personvernrådet gjort rede for hvordan steg tre, vurderingen av lovverket og praksisen i tredjelandet, skal gjennomføres.[36] Veilederne fra Personvernrådet rundt Schrems II-dommen vil redegjøres for i kapittel 4.

Personvernrådet (European Data Protection Board) er et uavhengig europeisk organ som er opprettet etter GDPR kapittel VII avsnitt 3. Personvernrådet er satt sammen av nasjonale datatilsyn fra EU-medlemslandene og European Data Protection Supervisor (heretter EDPS).[37] I tillegg deltar datatilsynet til EØS/EFTA-landene.[38], [39] Personvernrådet sin

[29] Fredriksen og Mathisen (2014) s. 238.
[30] Fredriksen og Mathisen (2014) s. 193.
[31] EFTA-landene er Norge, Island, Liechtenstein og Sveits.
[32] Fredriksen og Mathisen (2014) s. 40.
[33] Ibid.
[34] Ibid.
[35] European Data Protection Board 2020a.
[36] European Data Protection Board 2020b.
[37] European Data Protection Board (u.å.).
[38] Ibid.
[39] Siden Norge ikke er et EU-land, har ikke Datatilsynet stemmerett i Personvernrådet. Se European Data Protection Board (u.å.).

oppgave er å sikre at GDPR tolkes og anvendes likt i EU- og EØS-landene.[40] For å sikre dette har rådet en rekke oppgaver, blant annet å «utstede retningslinjer, anbefalinger og beste praksis», jf. GDPR artikkel 70 nr. 1 bokstav g.

Retningslinjer og veiledninger fra Personvernrådet er ikke bindende. Den rettskildemessige vekten til retningslinjene fra Personvernrådet er likevel stor. Grunnen til dette er fordi de er direkte hjemlet i GDPR og oppgaven deres er å tolke GDPR.[41] Siden det er Personvernrådets oppgave å tolke GDPR, bør kommuner forholde seg til veilederne for å forstå standarden satt i Schrems II-dommen.

EDPS har som formål å sikre at EUs institusjoner respekterer retten til personvern.[42] EDPS har hatt en sentral rolle ved utviklingen av GDPR og har i denne forbindelse utgitt proposisjonsnotater, blant annet om forståelse av begrepet «overføring». Proposisjonsnotatene er kun rådgivende. Redegjørelse for forståelsen av begrepet overføring, vil avhandlingen komme tilbake i kapittel 2.3.

Datatilsynet har publisert oppdateringer om problematikken rundt Schrems II-dommen. De har som oppgave å føre tilsyn med virksomheter og kommuner om de etterlever personvernreglene og være et ombud.[43] Oppdateringene i forbindelse med dommen er for eksempel kortfattede sammendrag av vurderingene til EU-domstolene og veilederne fra Personvernrådet. Datatilsynet kan ilegge overtredelsesgebyr eller andre sanksjoner til databehandler eller behandlingsansvarlige ved brudd på GDPR.[44]

For kommuner kan i tillegg arkivlova[45], bokføringsloven[46] og sikkerhetsloven[47] være gjeldende ved bruk av skytjenester. Disse vil imidlertid ikke bli videre analysert i avhandlingen.

I forbindelse med arbeidet av masteroppgaven er det intervjuet elleve informanter, det vil si de som svarte på spørsmålene på vegne av kommunene og skyleverandøren. Siden avhandlingen handler om kommuners erfaringer, bekymringer og betraktninger rundt bruken

[40] Datatilsynet (u.å.a.).
[41] Ibid.
[42] European Data Protection Supervisor (u.å.).
[43] Datatilsynet (u.å.c.).
[44] Reglene om sanksjoner er regulert i GDPR kapittel VIII.
[45] Lov 4. desember 1992 nr. 126 om arkiv (arkivlova).
[46] Lov 19. november 2004 nr. 73 om bokføring (bokføringsloven).
[47] Lov 1. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven).

av skytjenester etter Schrems II, er forskningen basert på en kvalitativ fremgangsmåte. Dybdeintervjuene har som hensikt å belyse kommunenes egen forståelse, erfaringer og bekymringer rundt Schrems II-problematikken. Vurderingen er dermed at den kvalitative metoden er best egnet for å belyse problemstillingen i avhandlingen.

Funnene av dybdeintervjuene presenteres i kapittel 5. Spørsmålene som ble stilt til informantene, er vedlagt avhandlingen i vedlegg 1 og 2. Funnene av dybdeintervjuene er særlig brukt i kapittel 6 om hvilken betydning Schrems II-dommen og veilederne fra Personvernrådet har for kommuner. For å ivareta vernet av personopplysninger til innbyggerne og informantene, samt få verdifull innsikt fra informantene som møter problemstillingene Schrems II medfører i det daglige, er personopplysninger til informanter anonymisert og navnene på kommunene og skyleverandøren utelatt. For å bevare hensynet til transparens og etterprøvbarhet, er en utfyllende fremstilling av valget av kommuner og skyleverandører, samt gjennomføringen av dybdeintervjuene redegjort for i kapittel 5. Valget om å utelate navnene på kommunene og skyleverandøren er drøftet med veileder og emneansvarlig for masteroppgaver. Det er enighet om at denne løsningen ivaretar både prinsippene om transparens og etterprøvbarhet samt vernet av personopplysninger. Emneansvarlig har i epost av 9. mars 2021 uttalt at denne «løsningen skal legges til grunn ved sensuren».

1.4 Avgrensning og presisering

Som nevnt i punkt 1.2 er det mange juridiske problemstillinger som oppstår i forbindelse med bruk av skytjenester. I denne avhandlingen vil konsekvensene av Schrems II-dommen analyseres. Oppgaven vil fokusere på skytjenester som er eller vil bli brukt av kommuner.

Det blir henvist til internasjonale og nasjonale regler og rettspraksis der det er hensiktsmessig, men kun regler og rettspraksis av særlig betydning for avhandlingen drøftes nærmere. Personvernregler i annen norsk lovgivning vil ikke bli behandlet da dette vil gå utover avhandlingens omfang å ta det med. Dette inkluderer eksempelvis sikkerhetsloven, arkivlova og bokføringsloven.

Avhandlingen avgrenses også mot å kartlegge for behandling av personopplysninger av særlige kategorier i skyen. Grunnen til dette er at disse personopplysninger krever et høyere beskyttelsesnivå enn andre opplysninger, jf. GDPR art. 9.

Respondentene til denne masteroppgaven er begrenset til ti kommuner og en skyleverandør. Det presiseres derfor at resultatene av dybdeintervjuene illustrerer meningene til de utvalgte informantene, og det derfor ikke nødvendigvis kan trekkes slutninger om dette er representativt for alle de andre kommunene og skyleverandørene.

Rettstilstanden rundt overføring av personopplysninger til tredjeland var under skrivingen av masteroppgaven uavklart. Det presiseres derfor at avhandlingen kun har tatt hensyn til nye uttalelser, anbefalinger og dommer fra relevante kilder frem til den 15. april 2021.

Avhandlingen avgrenses også mot å behandle problemstillinger knyttet til overføring av personopplysninger til tredjeland med Binding Corporate Rules (BCR) som overføringsgrunnlag. Grunnen til dette er at EU-domstolen ikke har vurdert gyldigheten av BCR i Schrems II-dommen. Innvirkningen Schrems II dommen har for BCR, er ikke avklart per 15. april 2021. Personvernrådet har uttalt følgende; «[t]he precise impact of the Schrems II judgment on BCRs is still under discussion. The EDPB will provide more details as soon as possible as to whether any additional commitments may need to be included in the BCRs in the WP256/257 referentials».[48]

1.5 Metodiske utfordringer

Rettstilstanden rundt overføring av personopplysninger til tredjeland med SCC som overføringsgrunnlag, er ved innlevering av denne masteroppgaven fortsatt uavklart. Underveis i skrivingen har det blitt publisert nye uttalelser og anbefalinger samt kommet avgjørelser fra blant annet Frankrike og Tyskland. Disse avgjørelsene illustrerer hvordan ulike EU-medlemsland forholder seg til standarden satt i Schrems II-dommen. Avgjørelsene har ikke betydning for hvordan andre land forholder seg til Schrems II-dommen. Det har vært en metodisk utfordring å skrive om et tema hvor det stadig kommer nye kilder man må forholde seg til.

Forskningsmetoden som har blitt benyttet i denne avhandlingen, har vist seg å være en god metode for å få innsikt i hvordan kommunene og skyleverandørene forholder seg til standarden satt i Schrems II-dommen. Resultatene av dybdeintervjuene er basert på samtaler med informanter fra ti kommuner og en skyleverandør. Ideelt sett skulle flere kommuner og

[48] European Data Protection Board 2020a, avsnitt 59.

skyleverandører vært intervjuet. Det har tatt tid å komme i kontakt med skyleverandører som har sagt seg villig til å delta. Mer om gjennomføringen av dybdeintervjuene redegjøres for i kapittel 5.

1.6 Avhandlingens oppbygning

Avhandlingen følger en trinnvis struktur. I kapittel 2 vil det redegjøres for kravene ved overføring av personopplysninger til tredjeland. Kapittelet vil blant annet inneholde en redegjørelse for hva GDPR er, de ulike overføringsgrunnlagene, hva som regnes som en personopplysning og prinsippet om ansvarlighet.

I kapittel 3 vil det redegjøres for hva en skytjeneste er, hvilke fordeler bruk av skytjeneste medfører, de ulike tjenestemodellene og ansvarsfordelingen i en skytjeneste.

I kapittel 4 vil Schrems II-dommens faktum, konklusjoner og premisser redegjøres for. I tillegg vil de to veilederne fra Personvernrådet om Schrems II-dommen belyses.

Kapittel 5 vil oppsummere funnene av dybdeintervjuene. Her vil det også redegjøres for utvelgelsen av kommunene og skyleverandøren samt gjennomføringen av dybdeintervjuene.

Kapittel 6 vil ta for seg en analyse av hvilke hovedutfordringer bruk av skytjenester medfører i lys av Schrems II. I hvilken grad påvirkes tjenestemodellene av Schrems II-dommen? Hvilke utfordringer har oppstått knyttet til veilederne fra Personvernrådet for bruk av skytjenester for en kommune? Denne delen vil ta utgangspunkt i dybdeintervjuene med informantene fra ulike kommuner som skal ta i bruk skytjenester og dybdeintervjuet med skyleverandøren.

Avslutningsvis vil det i kapittel 7 gis en oppsummering av avhandlingens funn, hindringer og muligheter for at markedsplassen blir en suksess samt knyttes noen bemerkninger de lege ferenda til dette.

2 Overføring av personopplysninger ved bruk av skytjenester

2.1 Innledende ord

GDPR er en EU-forordning som «fastsetter regler om vern av fysiske personer i forbindelse med behandling av personopplysninger samt regler om fri utveksling av personopplysninger», jf. GDPR artikkel 1.

Forgjengeren til GDPR var EUs Personverndirektiv som blant annet regulerte virksomheters adgang til å behandle personopplysninger.[49] EUs Personverndirektiv var et direktiv, mens GDPR er en forordning. Forskjellen mellom gjennomslagskraften i nasjonal rett til et direktiv og en forordning, er markant. Det følger av Traktaten om Den europeiske unions virkeområde (heretter TEUV) art. 288 at et direktiv «shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods».[50] En forordning «shall have general application. It shall be binding in its entirety and directly applicable in all Member States», jf. TEUV art. 288. En forordning gjelder dermed direkte til forskjell fra et direktiv som gir landene mer handlingsrom.[51] I EFTA-landene skal forordninger «være eller gjøres» til en del av avtalepartenes interne rettsorden, jf. EØS-avtalen art. 7.[52] Bakgrunnen for dette er hensynet til at flere av EFTA-landene har en dualistisk tradisjon.[53] I Norge gjøres dette ofte i praksis ved at det vedtas en lov- eller forskriftsbestemmelse som slår fast at forordningen gjelder som norsk rett.[54]

[49] Direktiv 95/46/EF: EUs personverndirektiv.
[50] Traktaten om Den europeiske unions virkeområde (TEUV).
[51] Det bemerkes imidlertid at medlemslandene har et visst handlingsrom også ved en forordning, se blant annet GDPR art. 8 nr.1.
[52] Fredriksen og Mathisen (2014) s. 277.
[53] Dualisme betegner forholdet mellom nasjonal rett og folkerett. Land med dualistisk tradisjon inkorporerer forpliktelsene istedenfor at forpliktelsene direkte gjelder i landet.
[54] Fredriksen og Mathisen (2014) s. 278.

2.2 Hva er en «overføring» av «personopplysning»?

2.2.1 Innledende ord

Problemstillingen i avhandlingen er hvilke konsekvenser Schrems II-dommen har for overføring av personopplysninger ved bruk av skytjenester. I denne forbindelse er det sentralt å se på hva begrepene «personopplysning» og «overføring» omfatter.

2.2.2 Hva er en «personopplysning»?

Det følger av GDPR art. 4 (1) hva som menes med en personopplysning. Personopplysninger er et vidt begrep som tilsier «enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte)». Med en identifiserbar fysisk person menes «en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator […] eller ett eller flere elementer».

Ordlyden «enhver» opplysning tilsier at personopplysninger skal tolkes vidt.[55] Enhver opplysning tilsier alle uttalelser og informasjon om personen, uavhengig av arten, innholdet eller formen på uttalelsene. Dette dekker både objektive og subjektive opplysninger.[56]

En vid tolkning av ordlyden er også støttet opp av EU-domstolen, jf. blant annet C-434/16 Nowak.[57] Domstolen fastslo i Nowak-dommen at så lenge opplysningen kan «relates to the data subject», er det en personopplysning.[58] Videre uttaler EU-domstolen at det er en personopplysning dersom opplysningen «by reason of its content, purpose or effect, is linked to a particular person».[59]

[55] European Commission (2007) s. 6.
[56] Ibid.
[57] Nowak, [Second Chamber], C-434/16.
[58] Nowak, [Second Chamber], C-434/16, avsnitt 34.
[59] Nowak, [Second Chamber], C-434/16, avsnitt 35.

2.2.3 Hva er en «overføring»?

Som nevnt følger det av GDPR art. 44 at enhver «overføring» av personopplysninger som behandles etter overføring til en tredjestat, skal kun finne sted dersom den behandlingsansvarlige og databehandleren oppfyller vilkårene i kapittel V.

Hva som regnes som en «overføring» av personopplysninger, er ikke definert i GDPR eller i rettspraksis. EDPS har derimot i et proposisjonsnotat uttalt at overføringsbegrepet brukes om data som er «move[d] or allowed to move between different user».[60]

Begrepet favner vidt. Datatilsynet har definert overføring av personopplysninger som at «personopplysningene sendes eller overføres til et annet land, eller at noen i et annet land får fjerntilgang til opplysningene».[61]

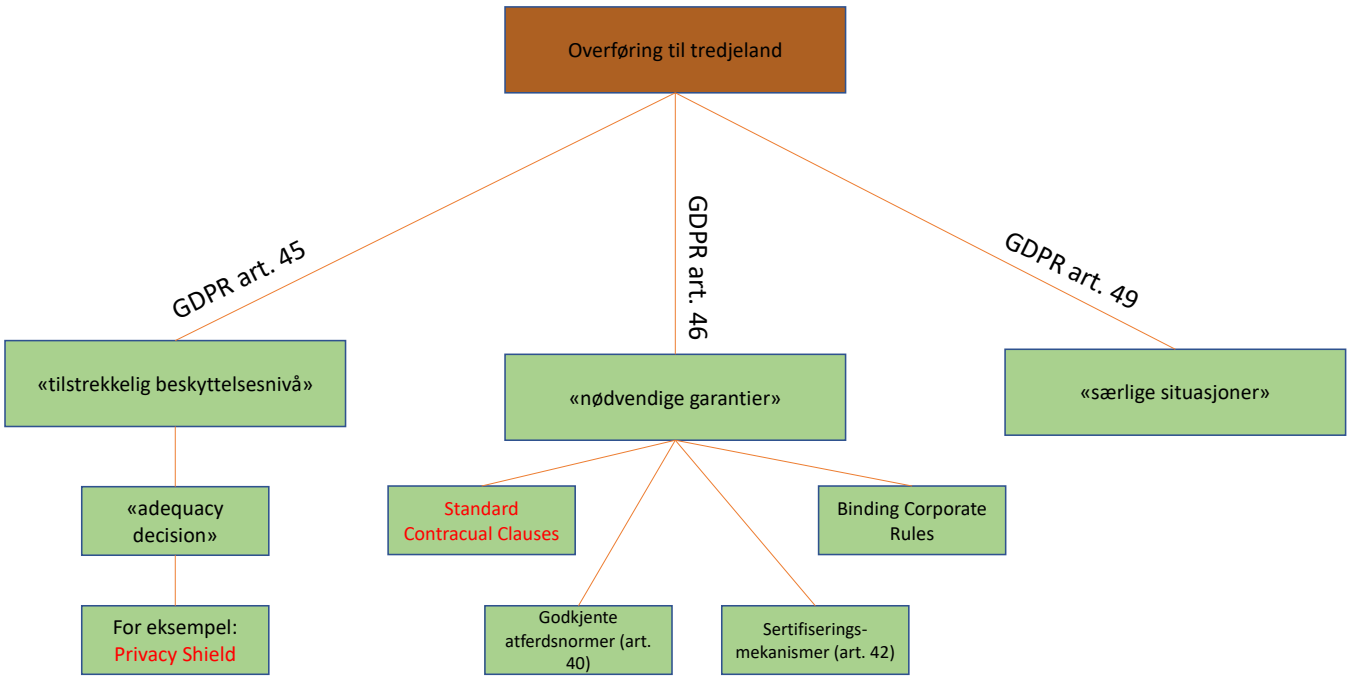
2.3 Bestemmelsene for overføring av personopplysninger til et tredjeland

Bestemmelsene om overføringer av personopplysninger til et tredjeland reguleres av GDPR kapittel V.

Utgangspunktet for overføring av personopplysninger følger av GDPR art. 44 der det fremkommer at «[e]nhver overføring av personopplysninger som behandles […] etter overføring til en tredjestat […], skal finne sted bare dersom den behandlingsansvarlige og databehandleren […] oppfyller vilkårene i dette kapittelet». Dette vil si at det i utgangspunktet er ulovlig å overføre personopplysninger til et tredjeland, med mindre det foreligger et overføringsgrunnlag. Som nevnt under kapittel 1.2.1 bruker kommuner i mange tilfeller skytjenester som overfører personopplysninger til tredjeland. Kommunene må derfor bruke et overføringsgrunnlag for at overføringen skal være lovlig.

Hva som anses som et overføringsgrunnlag er også regulert i GDPR kapittel V. Overføringsgrunnlagene kan deles inn i tre typer: 1) beslutning om «tilstrekkelig beskyttelsesnivå», jf. art. 45, 2) «nødvendige garantier», jf. art. 46 og 3) «særlige situasjoner», jf. art. 49. Denne avhandlingen vil redegjøre for Privacy Shield (art. 45) og SCC (art. 46).

[60] Skullerud, Rønnevik, Skorstad og Pellerud (2018) s. 254.
[61] Datatilsynet (2020).



Figur 1: Oversikt over de ulike overføringsgrunnlagene for overføring av personopplysninger til tredjeland. Modellen er laget av forfatteren av avhandlingen.

Det følger av GDPR art. 45 at personopplysninger «kan overføres til en tredjestat […] når Kommisjonen har fastslått at tredjestaten […] sikrer et tilstrekkelig beskyttelsesnivå». Europakommisjonen kan altså forhåndsgodkjenne og anerkjenne at beskyttelsesnivået for vern av personopplysninger er tilstrekkelig i et konkret land. Oversikt over de forhåndsgodkjente landene er publisert på EU-kommisjonens nettside.[62] Eksempler på forhåndsgodkjente land er Argentina, Japan og Storbritannia.[63] Privacy Shield-avtalen mellom USA og EU var før Schrems II-avgjørelsen ble avsagt, forhåndsgodkjent etter denne hjemmelen.[64]

[62] Lenke: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (lest 05.03.21).
[63] EDPB støtter EU-kommisjonens beslutning om at Storbritannia er et «godkjent land» for overføring av personopplysninger fra EU/EØS. Per 15.04.21 gjenstår kun en formell beslutning av medlemslandene før Storbritannia kan regnes som et forhåndsgodkjent land.
[64] Schrems II [GC] C-311/18, avsnitt 181.

Den andre typen overføringsgrunnlag er der den behandlingsansvarlige og databehandleren har «gitt nødvendige garantier», jf. GDPR artikkel 46. Hvem som er behandlingsansvarlig og hvem som er databehandler ved bruk av en skytjeneste, vil bli redegjort for i kapittel 2.3.

En nærmere forklaring på hva «nødvendige garantier innebærer» er beskrevet i forordningens fortale punkt 108. Det følger av dette punktet at nødvendige garantier «kan omfatte bruk av bindende virksomhetsregler, standard personvernbestemmelser vedtatt av Kommisjonen, standard personvernbestemmelser vedtatt av en tilsynsmyndighet eller avtalevilkår godkjent av en tilsynsmyndighet». Formålet med garantiene er at garantiene skal kompensere for manglende vern av personopplysningene. Eksempler på overføringsgrunnlag som gir nødvendige garantier etter art. 46 er SCC og BCR.

Den siste typen er unntaket som følger av GDPR art. 49 om «særlig situasjoner». Denne artikkelen åpner for at overføring av personopplysninger kan forekomme selv om det ikke foreligger en «beslutning om tilstrekkelig beskyttelsesnivå i henhold til artikkel 45 […] eller nødvendige garantier i henhold til artikkel 46», jf. art. 49 nr. 1. Det oppstilles nærmere vilkår som må være oppfylt for at artikkelen kan brukes. Denne artikkelen er ikke aktuell for avhandlingen og vil derfor ikke behandles nærmere.

I kapittel 4 vil det redegjøres for hvordan Schrems II har påvirket lovligheten til overføringsgrunnlagene Privacy Shield og SCC.

2.4 Behandlingsansvarlig og databehandlers rolle ved overføring av personopplysninger til tredjeland

Den behandlingsansvarlige er den som har det overordnede ansvaret for å overholde personvernprinsippene, jf. GDPR art. 5 nr. 2. GDPR skiller mellom rollene behandlingsansvarlig og databehandler. Før en kommune ønsker å ta i bruk en skytjeneste må det avklares hvilken rolle kommunen har samt hvilken rolle skyleverandøren og eventuelle underleverandører som behandler personopplysninger på vegne av kommunen, har. Hvilken rolle partene har, vil blant annet ha betydning for kravene som stilles til parten og ansvaret parten har. Ansvarsfordelingen ved bruk av en skytjeneste vil avhandlingen behandle i kapittel 3.4.

Det følger av GDPR art. 4 nr. 7 at med behandlingsansvarlig menes «en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes».

Med databehandler menes «en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlig», jf. GDPR art. 4 nr. 8. Databehandler behandler altså personopplysningene på vegne av den behandlingsansvarlige.

Når en kommune inngår en avtale med en skyleverandør om å ta i bruk deres skytjeneste, vil kommunen være den behandlingsansvarlige og leverandøren være databehandleren etter definisjonene i GDPR. En eventuell underleverandør som skyleverandøren tar i bruk, vil bli ansett som en underdatabehandler.

2.5 Prinsippet om ansvarlighet

I GDPR art. 5 er det hjelmet generelle prinsipper for behandling av personopplysninger. Personopplysningene skal behandles på en «lovlig, rettferdig og åpen måte med hensyn til den registrerte», skal samles inn for «spesifikke, uttrykkelige antatte og berettigede formål», skal «begrenset til det som er nødvendig for formålene de behandles for», «være korrekte og om nødvendig oppdaterte», ha «lagringsbegrensning» slik at det ikke er mulig å identifisere den registrerte i lengre perioder enn det som er nødvendig og behandles på en måte som sikrer «integritet og konfidensialitet», jf. GDPR art. 5 nr. 1 bokstav a-f.

Som nevnt i punkt 2.3 vil behandlingsansvarlig og databehandleren ha ulike ansvar ved behandling av personopplysninger. Det følger av GDPR art. 5 nr. 2 at «[d]en behandlingsansvarlige er ansvarlig for og skal kunne påvise at nr. 1 overholdes («ansvar»)». Dette prinsippet er et sentralt prinsipp i forbindelse med problemstillingen til avhandlingen. Grunnen til dette er at prinsippet hjelmer den behandlingsansvarlige sitt ansvar om å etterleve og påvise at prinsippene i nr. 1 følges. Dette vil si at det er den behandlingsansvarlige som har hovedansvaret for behandling av personopplysninger, også dersom denne gjennomføres av en

databehandler.[65] Betydningen av dette prinsippet i forbindelse med kommuners bruk av skytjenester, vil bli redegjort for i kapittel 3.4

Etterlevelse kan påvises gjennom å ha et godt internkontrollsystem som blant annet beskriver hvilke opplysninger som behandles for hvilke formål og hvordan opplysningene behandles.[66]

[65] Skullerud, Rønnevik, Skorstad og Pellerud (2018) s. 79.
[66] Ibid.

3 Skytjenester

3.1 Hvorfor skal kommuner velge å bruke skytjenester?

I digitaliseringsrundskrivet fra 2021 er det stilt krav om at kommuner skal benytte skytjenester når det ikke foreligger spesielle hindringer for å ta i bruk skytjenester.[67] Dette vil si at kommuner skal vurdere skytjenester når de anskaffer eksempelvis nye applikasjoner.

Kommunene er egne rettssubjekter som selv har ansvar og utøver sitt selvstyre innenfor nasjonale rammer, jf. Grunnloven[68] § 49 andre avsnitt og kommuneloven[69]. Kommunene er regulert gjennom lover og forskrifter samt budsjettrammer som er vedtatt av Stortinget. Det kommunale selvstyre kan være en grunn til at bruken av skytjenester varierer i de ulike kommunene.

Det er flere fordeler med å ta i bruk en skytjeneste. I en undersøkelse utført av kommunesektorens organisasjon (heretter KS) oppga kommunene at hovedgrunnen til at de valgte å ta i bruk skytjeneste er økonomiske faktorer, ønske om å fokusere på tjenesteutvikling, skalering og fleksibilitet, samt økt tilgjengelighet til kommunen sine løsninger for innbyggerne.[70]

Det er flere grunner til at skytjenester kan medføre reduserte kostnader. Siden en skytjeneste ikke krever lokal infrastruktur, vil kostnadene og investeringen tilknyttet selve IT-driften hos kommunen reduseres. I tillegg kan kostandene knyttet til oppdateringer, administrasjon og programvarelisenser reduseres. Ressursbruken til kommunen blir også målt, kontrollert og rapportert. Dette medfører at kommunen kun betaler for kapasiteten den bruker.[71]

Skytjenester tilbyr nærmest ubegrenset kapasitet for behandling, prosessering og lagring av data.[72] Ved bruk av skytjenester trenger ikke kommunen å bekymre seg for å gå tom for kapasitet.

[67] Kommunal- og moderniseringsdepartementet (2021).
[68] Lov 17. mai 1814 Kongeriket Norges Grunnlov (Grunnloven).
[69] Lov 22. juni 2018 nr. 83 om kommuner og fylkeskommuner (kommuneloven).
[70] Advokatfirma Føyen Torkildsen AS (2015) s. 66.
[71] Kommunal- og moderniseringsdepartementet (2016) s. 9.
[72] Kommunal- og moderniseringsdepartementet (2016) s. 10.

En annen fordel med skytjenester er at det gir bedre fleksibilitet. Kommunen har tilgang til dataen uavhengig av hvor brukerne i kommunen befinner seg og på ulike type klienter (eksempelvis PC, nettbrett, mobil).[73]

Økt innovasjon er også en fordel med skytjenester. Bruk av skytjenester kan redusere investeringene som er nødvendige for å starte ny virksomhet, tilby nye produkter eller tjenester og sette opp nye plattformer for utvikling og innovasjon. Bruk av skytjenester kan gjøre det lettere for kommuner å teste ut, utvikle og tilby nye innbyggertjenester.[74]

I dagens samfunn er det mange kommuner som har fokus på miljøvennlig drift. Skyleverandørene kan dele maskinvareressursene mellom flere kunder. Bruk av skytjenester er bedre for miljøet da dette gir mer effektiv energibruk enn om alle kommuner skulle hatt sitt eget maskinsenter med maskinvare, kjøling og mer.[75] I tillegg er kapasiteten tilpasset kommunens behov. Siden serverkapasiteten skaleres etter kommunens behov, vil dens energibruk kun være den energien som trengs for å utføre operasjonene.

3.2 Definisjonen av skytjeneste

Det finnes ingen allmenn anerkjent definisjon på skytjeneste.

En av de mest brukte internasjonale definisjonene av skytjeneste er definisjonen til National Institute of Standards and Technology (heretter NIST): «a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction».[76] Regjeringen viser også til denne definisjonen i den nasjonale strategien for bruk av skytjenester.[77]

Videre i avhandlingen vil begrepet skytjeneste basere seg på definisjonen fra NIST.

[73] Kommunal- og moderniseringsdepartementet (2016) s. 12.
[74] Ibid.
[75] Kommunal- og moderniseringsdepartementet (2016) s. 11.
[76] Mell og Grance (2011) s. 2.
[77] Kommunal- og moderniseringsdepartementet (2016) s. 7.

3.3 Tjenestemodeller og leveransemodeller

Som beskrevet i kapittel 2.3.1 vil kommunen anses som behandlingsansvarlig, og skyleverandøren og den eventuelle underleverandører anses som databehandler etter GDPR artikkel 4 nr. 7 og 8. I dette kapittelet vil de ulike tjenestemodellene redegjøres for. Dette vil være et viktig utgangspunkt for drøftelsen i kapittel 6.2 om hvilken grad tjenestemodellene påvirkes av Schrems II-dommen.

Skytjenester kan deles inn i både tjeneste- og leveransemodeller. Tjenestemodell er et begrep som beskriver hvor mye av applikasjonen og/eller infrastrukturen som er med i tjenesten.[78] Ordlyden leveransemodell viser til om skytjenesten kun er ment for virksomheten selv eller om skytjenesten er i ulik grad delt med andre virksomheter.[79] Leveransemodellene vil ikke bli videre redegjort for i avhandlingen.

NIST deler inn skytjenester inn i tre ulike tjenestemodeller; programvare som tjeneste (software as a service, forkortet SaaS), plattform som tjeneste (platform as a service, forkortet PaaS) og infrastruktur som tjeneste (infrastructure as a service, forkortet IaaS).[80]

Tjenestemodellen SaaS er en modell for leveranse over et nettverk hvor kunden benytter leverandørens applikasjon(er) på en nettsky-infrastruktur.[81] Dette er altså ikke programvare som kan lastes ned lokalt for å tas i bruk, men en tjeneste som ytes over internettet. Kunden leier eller bruker programvaren som en tjeneste, og det kan derfor ikke stilles hvilke krav som helst til tjenesten. Eksempel på en Saas-applikasjon er Microsoft Office 365.

PaaS er en plattform der kunden innfører applikasjoner utviklet eller kjøpt av kunden i leverandørens nettsky-infrastruktur gjennom å benytte programmeringsspråk og verktøy støttet av leverandøren.[82] Kunden vil da ha kontroll over egne applikasjoner, men kan i liten grad kontrollere og stille krav til nettverk, servere, operativsystem og lagring.

Tjenestemodellen IaaS er en modell som gjelder levering av datainfrastruktur som en tjeneste over et nettverk.[83] Kunden har kontroll over egne applikasjoner, servere, operativsystem og

[78] Normen (2020) s. 11.
[79] Normen (2020) s. 12.
[80] Mell og Grance (2011) s. 2–3.
[81] Datatilsynet (2018).
[82] Ibid.
[83] Ibid.

lagring, men kontrollerer ikke den underliggende infrastrukturen. I enkelte tilfeller har kunden også kontroll over nettverket, eksempelvis på brannmursiden.[84]

De ulike tjenestemodellene kan medføre ulike utfordringer for en kommune. Dette vil avhandlingen komme tilbake til i kapittel 6.3.

3.4 Plassering av roller og ansvar

3.4.1 Innledende ord

I 2019 skrev digi.no at tre av ti virksomheter mener at skyleverandøren har alt ansvar for sikkerheten i skyen.[85] Det er bekymringsverdig at en så stor andel av virksomhetene ikke er klar over ansvarsfordeling ved bruk av skytjenester. Når en kommune tar i bruk en skytjeneste, har kommunen deler av ansvaret. Hvilket ansvar kommunen har og hvilket ansvar skyleverandøren har, varierer med tjenestemodellen til skytjenesten. I det følgende skal rollene og ansvaret til kommunene og skyleverandørene presenteres.

3.4.2 Ansvarsfordelingen i en skytjeneste

Et av hovedprinsippene i GDPR er prinsippet om ansvarlighet som hjelmer at det er den behandlingsansvarlige som har hovedansvaret for behandling av personopplysninger, også dersom denne gjennomføres av en databehandler.[86] Dette gjelder til tross for at en rekke bestemmelser retter seg direkte mot en databehandler.[87] Behandlingsansvarlig har ansvar for å velge en databehandler som kan levere tjenester i tråd med GDPR sine krav.

Når en kommune vurderer å ta i bruk en skytjeneste, er det viktig at kommunen forstår modellen for «the shared responsibility» og dermed hvilke oppgaver kommunen selv må håndtere.[88] Hvilket ansvar kommunen har, varierer med hvilken tjenestemodell kommunen

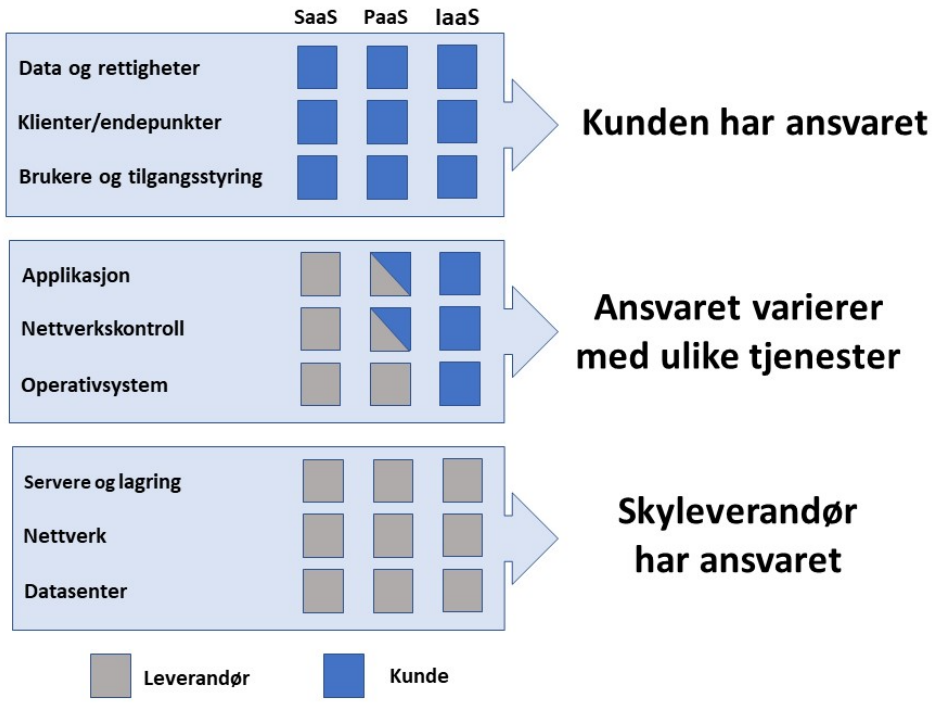
[84] Ibid.
[85] Sævold (2019).
[86] Skullerud, Rønnevik, Skorstad og Pellerud (2018) s. 79.
[87] Ibid.
[88] Microsoft (2021).

har valgt. Dersom kommunen bruker et lokalt datasenter, har kommunen selv alt ansvar.[89] Dersom kommunen bruker en skytjeneste, har skyleverandøren deler av ansvaret.[90]

Nasjonal sikkerhetsmyndighet skiller mellom «security of the cloud» som omfatter leverandørens plattform/tjenesteleveranse og «security in the cloud» som omfatter kundens bruk.[91] Førstnevnte er det skyleverandøren som har ansvar for. «Security in the cloud» er det som regel kommunen som har ansvar for alene.[92] Det er viktig at fordelingen av ansvaret mellom kommunen og leverandøren er avklart på forhånd og at grensen for hvilke oppgaver kommunen har, er tydelig.

Felles for alle tjenestemodellene er at kommunen selv eier dataen og identiteter, samt er ansvarlig for å beskytte sikkerheten til sin data, hvem som skal ha tilgang til dataen, on-prem ressurser og skykomponentene som kommune styrer.[93] Sistnevnte beror på hvilken tjenestemodell kommunen har valgt. Ansvaret til skyleverandøren vil strekke seg lengre ved en SaaS-tjenestene enn ved en PaaS-tjeneste på samme måte som ansvaret vil strekke seg lengre ved en PaaS-tjeneste enn en IaaS-tjeneste.[94]

[89] Ibid.
[90] Ibid.
[91] Nasjonal Sikkerhetsmyndighet (u.å.) spørsmål 2.
[92] Ibid.
[93] Microsoft (2021).
[94] Normen (2020) s. 20.



Figur 2: Modell over ansvarsfordelingen mellom leverandør og kunde etter leverandøren sin oppfatning. Kilde: Figuren er utarbeidet av Håvard Reknes hos DFØ. Håvard delte modellen med forfatteren av avhandlingen den 9. april 2021.

Det kan være utfordrende for kommuner å få oversikt over hvem som har hvilket ansvar. Grunnen til dette er at det kan være uklart for kommunen hvem som er leverandøren og underleverandøren(e) med tilhørende ansvarslinjer. Det er viktig at kommunen kontakter leverandøren på forhånd for å få oversikt over fordelingen av ansvaret mellom dem og at grensen for hvilke oppgaver kommunen har, er tydelig.

4 Schrems II-dommen

4.1 Innledende ord

I dette kapittelet vil Schrems II-dommen og de to veilederne fra Personvernrådet datert 10. november 2020, redegjøres for. Hvilken betydning dommen og veilederne har for kommuner drøftes i kapittel 6. Betydningen for kommunene vil behandles i lys av dybdeintervjuene som presenteres i kapittel 5.

4.2 Om faktum og dommen

Den 16. juli 2020 avsa EU-domstolen en prejudisiell avgjørelse etter klage fra juristen Maximillian Schrems om overføringer av personopplysninger fra Facebook Irland til Facebook Inc. i USA.[95] Domstolen ugyldiggjorde bruk av Privacy Shield som overføringsgrunnlag til USA med umiddelbar virking.[96] SCC kan fortsatt brukes som overføringsgrunnlag, men EU-domstolen presiserte at både databehandleren og behandlingsansvarlig må vurdere om beskyttelsesnivået i mottakerlandet er tilstrekkelig.[97]

Bakgrunnen for Schrems II-dommen er EU-domstolens avgjørelse om Safe Harbor, den såkalte Schrems I-dommen.[98] Maximillian Schrems sendte inn klage på Safe Harbor-avtalen. Han begrunnet klagen med at hans rett til personvern ikke ble ivaretatt når Facebook Irland overførte personopplysninger til Facebook Inc. i USA med Safe Harbor som overføringsgrunnlag. EU-domstolen ugyldiggjorde Safe Harbor som overføringsgrunnlag med den begrunnelse at det ikke ga tilstrekkelig beskyttelse av personopplysningene i henhold til EUs grunnleggende prinsipper.[99]

Etter Schrems I-dommen kom EU og Obama-administrasjonen til enighet om et nytt overføringsgrunnlag mellom EU og USA. Dette overføringsgrunnlaget ble kalt Privacy Shield.[100] Facebook tok deretter i bruk SCC og Privacy Shield som overføringsgrunnlag for overføringer av personopplysninger til USA. Maximillian Schrems omformulerte klagen til at

[95] Schrems II [GC] C-311/18, avsnitt 2.
[96] Schrems II [GC] C-311/18, avsnitt 201.
[97] Schrems II [GC] C-311/18, avsnitt 142.
[98] Schrems I [GC] C-362/14.
[99] Schrems I [GC] C-362/14, avsnitt 106.
[100] Decision (EU) 2016/1250 (EU–US Privacy Shield).

SCC og Privacy Shield er i strid med EUs grunnleggende rettigheter. Klagen endte opp hos Irish High Court[101], som ba EU-domstolen om å vurdere om SCC og Privacy Shield er gyldige overføringsgrunnlag for overføringer til USA.

4.3 EU-domstolens vurderinger og konklusjoner

4.3.1 Gyldigheten av Privacy Shield

EU-domstolen har uttrykkelig uttalt at Privacy Shield ikke er et gyldig overføringsgrunnlag for overføring av personopplysninger.[102] Dommen har umiddelbar virkning. Domstolen begrunner ugyldiggjøringen med at den amerikanske lovgivningen ikke sikrer tilstrekkelig beskyttelsesnivå som kreves i henhold til GDPR artikkel 45.[103] I avsnitt 171 uttaler EU-domstolen at formidling av personopplysninger til en tredjepart, eksempelvis offentlige myndigheter, utgjør brudd på beskyttelsesnivået som kreves.

Domstolen viste til at The Foreign Intelligence Surveillance Act (FISA) 702 og Executive Order 12333 (EO 12.333) åpnet for at amerikanske myndigheter kunne masseovervåke europeiske borgere uten samtykke og uten begrensning knyttet til hva som er strengt tatt nødvendig.[104] Lovene begrenset også europeiske borgeres adgang til å etterprøve og adgangen til å rettslig forfølge beslutningene om overvåkning.

4.3.2 Gyldigheten av SCC

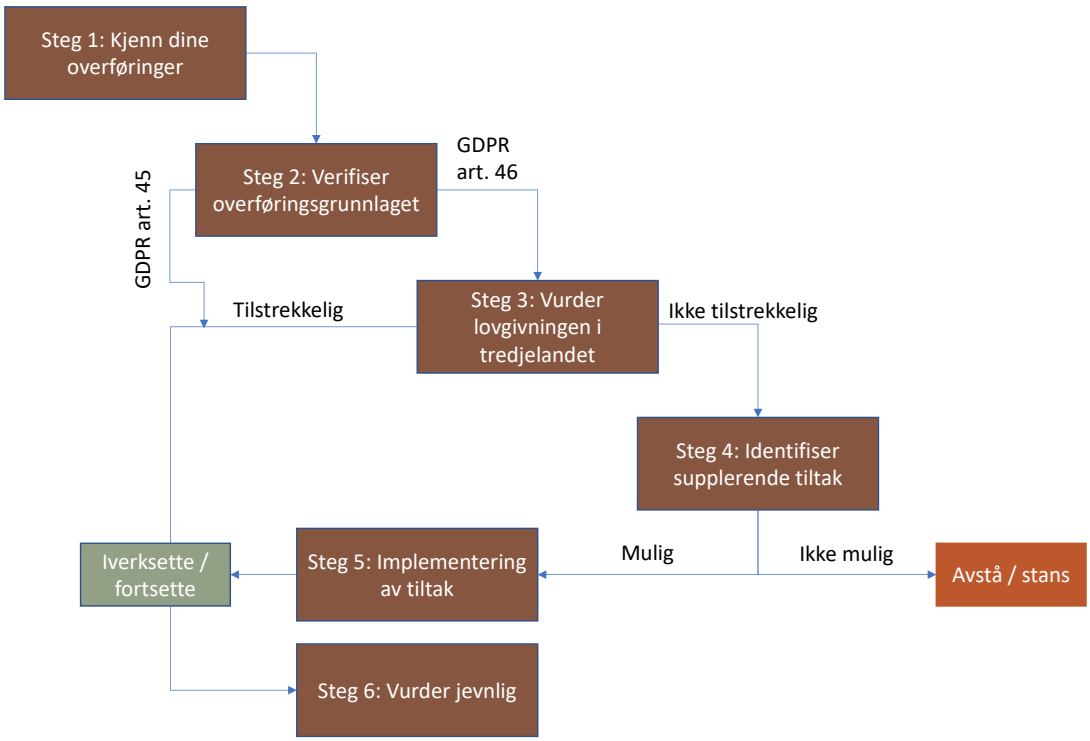
EU-domstolen konstaterte at overføringsgrunnlaget SCC fremdeles er gyldig, men i seg selv ikke er tilstrekkelig for at overføring av personopplysninger til tredjeland er lovlig.[105] I tillegg til å bruke SCC som overføringsgrunnlag må personopplysningene i praksis være underlagt samme vern som ved utveksling av personopplysninger innenfor EU/EØS. Gjennomføringen av denne vurderingen innebærer at lovgivningen i mottakerlandet undersøkes og at den registrertes rettigheter i praksis ivaretas. Dersom lovgivningen medfører at beskyttelsesnivået

[101] The High Court Commercial, The Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, 3. oktober 2017, 2016 No. 4809 P.
[102] Schrems II [GC] C-311/18, avsnitt 201.
[103] Schrems II [GC] C-311/18, avsnitt 168 flg.
[104] Schrems II [GC] C-311/18, avsnitt 179 flg.
[105] Schrems II [GC] C-311/18, avsnitt 122 flg.

ikke er tilsvarende innenfor EU/EØS, må det iverksettes ytterligere tiltak som medfører at kravene likevel oppfylles.

4.4 Veilederne fra Personvernrådet med oppklaringer rundt Schrems II-dommen

Personvernrådet i EU kom den 10. november 2020 med to veiledere som skulle bidra med å oppklare noen av punktene i Schrems II-dommen. Veilederne har vært på høring, men de endelige veilederne er per 15. april ikke publisert. I dokumentet Recommendations 01/2020 presenterer Personvernrådet veiledning som skal foretas i seks steg.[106] Disse stegene skal gjennomføres ved hver enkelt behandling og må dokumenteres. I dokumentet Recommandations 02/2020 har Personvernrådet gjort rede for hvordan behandlingsansvarlig skal gjennomføre vurderingen av lovverket og praksisen i tredjelandet.[107]



Figur 3: Oversikt over de seks stegene Personvernrådet har anbefalt ved overføring av personopplysninger til tredjeland. Modellen er laget av forfatteren av avhandlingen.

[106] European Data Protection Board 2020a.
[107] European Data Protection Board 2020b.

Det første steget i denne veiledningen går ut på å skaffe seg oversikt over alle overføringer av personopplysninger til tredjeland.[108] Dette inkluderer også overføringer til eventuelle underleverandører og tredjeparter.[109] Bruk av skytjenester og fjerntilgang til et tredjeland, for eksempelvis support, regnes også som en overføring. Målsettingen med dette steget er å skaffe seg oversikt over alle overføringene.

Det neste steget i veilederen til Personvernrådet går ut på å undersøke hvilket overføringsgrunnlag som benyttes i dag.[110] Som nevnt i kapittel 2.2.1 finnes det tre ulike overføringsgrunnlag. Som illustrert i figur 3 vil overføringer som faller inn under art. 45 til land som gir personopplysningene et «tilstrekkelig beskyttelsesnivå», kunne gå direkte til steg seks.[111] Dette vil eksempelvis gjelde de landene EU-kommisjonen har fattet beslutning om forhåndsgodkjenning av.[112] Dette innebærer at det kan overføres personopplysninger fra EU/EØS til disse landene uten at de videre stegene er gjennomført.[113]

Ved overføring av personopplysninger til tredjeland som ikke gir «tilstrekkelig beskyttelsesnivå», kreves det at det foreligger et overføringsgrunnlag som er listet opp i GDPR art. 46 eller art. 49.[114] Eksempler på et overføringsgrunnlag etter art. 46 er SCC og BCR.

Hvis overføringen ikke er til et forhåndsgodkjent tredjeland, skal man i steg tre av veiledningen vurdere om overføringsgrunnlaget sikrer den samme beskyttelsen som GDPR gir.[115] Dette inkluderer også overføringer til eventuelle underleverandører og tredjeparter. Formålet med denne vurdering er å sikre at beskyttelsesnivået ikke senkes ved overføring til tredjeland. Hver av mottakerlandenes lovgivning og praksis må vurderes. I dokumentet Recommandations 02/2020 har Personvernrådet gjort rede for hvordan behandlingsansvarlig skal gjennomføre denne vurderingen.[116]

---

[108] European Data Protection Board 2020a, s. 8.
[109] European Data Protection Board 2020a, s. 9.
[110] Ibid.
[111] European Data Protection Board 2020a, s. 9–10.
[112] Oversikt over de forhåndsgodkjente landene er publisert på EU-kommisjonens nettside. Lenke: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (lest 01.03.21).
[113] European Data Protection Board 2020a, s. 9–10.
[114] European Data Protection Board 2020a, s. 11.
[115] European Data Protection Board 2020a, s. 12.
[116] European Data Protection Board 2020b.

Personvernrådet har satt noen minimumskrav for vurderingen av lovverket til tredjelandet: a) behandlingen skal ha grunnlag i klare, presise og tilgjengelige regler, b) behandlingen må være nødvendig og forholdsmessig, c) det må eksistere et uavhengig kontrollorgan som skal sikre etterfølgelsen av reglene og d) muligheter for effektiv håndheving av regelverket for enkeltindivider.[117]

I tillegg til minimumskravene må det vurderes hvilket lovverk tredjelandet er underlagt og hvordan personvernet ivaretas. I Schrems II-dommen vurderte EU-domstolen overvåkningslovene FISA 702 og EO 12.333, og konkluderte med at disse lovene ikke ga tilstrekkelig beskyttelse tilsvarende innenfor EU/EØS.

Hvis konklusjonen etter steg tre er at mottakerlandet ikke oppfyller kravet om tilsvarende beskyttelsesnivå som innenfor EU/EØS, må det vurderes om ytterligere tiltak må iverksettes.[118] Formålet med dette steget er at vurderingen av de ytterligere tiltakene skal sikre tilstrekkelig beskyttelsesnivå. Dette er en konkret vurdering som må vurderes fra sak til sak.[119] De ytterligere tiltakene kan være kontraktuelle, tekniske eller organisatoriske. Kontraktuelle og organisatoriske tiltak er ikke i seg selv nok. Flere tiltak samlet kan derimot bidra til tilstrekkelig beskyttelsesnivå.[120] Eksempler på slik tiltak er nevnt i vedlegg to til Recommandations 01/2020 og vil videre redegjøres for i avhandlings kapittel 6.3.4.[121]

Femte steg i veiledningen er inkorporering av de ytterligere tiltakene i avtaleforholdet mellom partene.[122] Dette innebærer både at selve databehandleravtalen oppdatertes og at det innføres organisatoriske tiltak som sikrer at tiltakene inkorporeres i den daglige driften av skytjenesten. Personvernrådet presiserer at tiltakene ikke må være i strid med vilkårene i SCC.[123]

Det siste steget er å re-evaluere og gjennomføre disse vurderingene med jevne mellomrom for å sikre at beskyttelsesnivået er tilsvarende innenfor EU/EØS.[124]

[117] European Data Protection Board 2020b, s. 8.
[118] European Data Protection Board 2020a, s. 15.
[119] Ibid.
[120] Ibid.
[121] European Data Protection Board 2020a, Annex 2.
[122] European Data Protection Board 2020a, s. 17.
[123] Ibid.
[124] European Data Protection Board 2020a, s. 18.

5 Funnene av dybdeintervjuene med kommuner og skyleverandører

5.1 Innledende ord

I forbindelse med denne masteroppgaven har det blitt gjennomført dybdeintervjuer av informanter som representerer ti kommuner og en skyleverandør. Dybdeintervjuene har blitt gjennomført for å kartlegge bruken av skytjenester hos kommuner, vurderinger rundt hindringer Schrems II-dommen medfører, samt behov og vurderinger rundt markedsplassen. Disse dybdeintervjuene danner noe av grunnlaget for den videre drøftelsen.

5.2 Utvelgelsen av kommunene og skyleverandøren

5.2.1 Utvelgelsen av kommuner

Ved utvelgelsen av hvilke kommuner som skulle intervjues, ble særlig lagt vekt på to grupper respondenter: 1) kommuner som har valgt å avstå fra å inngå nye avtaler om skytjenester eller brutt anskaffelse av skytjeneste på grunn av Schrems II, 2) kommuner som har endret systemer eller rutiner etter Schrems II for å kunne ta i bruk eller fortsette å bruke skytjenester.

De valgte kommunene er av ulike størrelse, har stor forskjell i innbyggertall og er plassert i ulike fylker.

5.2.2 Utvelgelsen av skyleverandører

Ved utvelgelsen av hvilke skyleverandører som skulle intervjues, har det blitt lagt vekt på om skyleverandøren selger skytjenester til kommuner. Det ble sendt ut forespørsel til en håndfull skyleverandører som fylte dette kravet om de ønsket å delta. Dessverre var det lav respons på disse henvendelsene. Dette resulterte i dybdeintervju med kun en skyleverandør.

5.3 Gjennomføringen av intervjuene

Når det gjelder gjennomføringen av intervjuene har informantene som representerte de ti kommunene blitt stilt de samme spørsmålene, se vedlegg 1. Intervjuene har også fulgt samme struktur. Spørsmålene som ble stilt informanten til skyleverandøren er vedlagt i vedlegg 2. Spørsmålene var vidt formulert slik at informantene fikk prate fritt innenfor temaet til de ulike spørsmålene.

Kontaktpersonene hos kommunene og skyleverandøren ble på forhånd tilsendt spørsmålene samt en beskrivelse av målet med dybdeintervjuet for å sikre at de riktige personene ble intervjuet og at informantene kunne samle inn datamateriale for å kunne svare på alle spørsmålene.

På grunn av Covid-19 kunne ikke dybdeintervjuene foregå fysisk. Intervjuene ble dermed foretatt over Teams. Før intervjuet startet, presenterte alle seg og problemstillingen til avhandlingen ble gjentatt. Det ble informert om at samtalen ville bli tatt opp og at notatene fra intervjuet og opptaket ville slettes etter at avhandlingen er levert. Informantene til kommunene og skyleverandøren ble informert om at personopplysninger til informantene vil bli anonymisert og navnene på kommunene og skyleverandøren vil bli utelatt i avhandlingen.

Under dybdeintervjuene ble ett og ett spørsmål stilt, og informanten fikk prate fritt innenfor temaet til spørsmålet. Informantene bidro med grundige og utfyllende svar på spørsmålene. Resultatene av intervjuene er presentert i delkapittel 5.4 og 5.5.

5.4 Analyse og resultater av dybdeintervjuene med kommunene

I dette kapittelet vil datamaterialet fra dybdeintervjuene med de ti utvalgte kommunene presenteres gjennom en kategorisk fremstilling. Kategoriene er delt inn etter spørsmålene som ble stilt under dybdeintervjuene. Det er informantens erfaringer og oppfatninger som danner grunnlagene for svarene.

Spørsmålene var som følger:

- Hvor godt kjenner kommunen til Schrems II-dommen på en skala fra 1 til 10 (der 1 er svært dårlig og 10 er svært godt)? Hvilke møteplasser diskuteres dommen?

- Ta utgangspunkt i Personvernrådet sin veileder. Hvilket steg i prosessen vil du si at kommunen befinner seg på?

- Hva ser dere på som den største utfordringen med Schrems II-dommen i kommunen? Begrunn svaret.

- Har dere vurdert og/eller gjennomført endringer i deres systemer og/eller rutiner etter Schrems II-dommen?

Alle de intervjuede kommune bruker i dag skytjenester. Dybdeintervjuene viser at det finnes både kommuner som velger å avstå fra å inngå nye avtaler om skytjenester, som avslutter anskaffelser av skytjenester som allerede er igangsatt og som endrer rutiner og systemer for å kunne fortsette å ta i bruk skytjenester. Inntrykket etter dybdeintervjuene er at kommunene har ulike syn på hvordan de skal kunne fortsette å bruke skytjenester etter Schrems II.

5.4.1 Kommunenes kjennskap til dommen

Informantene ble spurt om hvor godt kommunen kjenner til Schrems II-dommen på en skala fra 1 til 10 (der 1 er svært dårlig og 10 er svært godt). I tillegg ble informanten spurt om hvilke møteplasser dommen diskuteres.

Kjennskapen til dommen i de utvalgte kommunene varierte, men samtlige informerte om at kjennskapen var på mellom en og fire på skalaen. Felles for kommunene er at informantene har opplyst om at det er generelt lav kjennskap til dommen blant de ansatte i kommunen. De som har arbeidsoppgaver som er relevante i forbindelse med dommen, kjenner stort sett til dommen og diskuterer dommen på arbeidsplassen.

Flere av informantene også har deltatt på kurs og deretter videreformidlet det som ble sagt til ledelsen og de som har arbeidsoppgaver som er relevante i forbindelse med dommen.

5.4.2 Hvor i stegene utarbeidet av Personvernrådet befinner kommunene seg?

I forkant av intervjuene hadde forfatteren av denne avhandlingen sendt en tekst til kommunene som kortfattet oppsummerte dommen og veilederne til Personvernrådet. Både

dommen og veilederne er beskrevet i avhandlingens kapittel 4. Informantene ble spurt om hvilket steg i prosessen de mente at kommunen befant seg på.

Flere av informantene opplyste om at de befant seg på steg 1 og 2. De jobbet med å skaffe seg oversikt over alle overføringene av personopplysningene til tredjeland og hvilke overføringsgrunnlag som brukes. Flere av informantene har opplyst om at kommunen i dag bruker mange ulike tjenester og at det er en omfattende prosess å kartlegge alle disse.

Omtrent halvparten av de intervjuede kommunene har en oppdatert behandlingsprotokoll som har gjort det betydelig lettere for kommunen å få oversikt over overføringene. En av kommunene har ikke tatt i bruk behandlingsprotokollen av organisatoriske årsaker. Denne kommunen opplyste under samtalen at kartleggingen av overføringene per midten av februar 2021 er mangelfull og at de sliter med å foreta en systematisk kartlegging på grunn av manglende behandlingsprotokoll.

To av de intervjuede kommunene er i gang med vurderingen av beskyttelsesnivået i tredjelandet, steg tre. Begge disse kommunene har informert om at de opplever dette som en tids- og ressurskrevende øvelse. Felles for disse to kommunene er at informantene ser på kommunenes forutsetninger for å foreta denne landevurderingen som marginale på grunn av mangelfulle juridiske ressurser.

5.4.3 Største utfordringen etter kommunenes mening

Dette spørsmålet setter fokus på hva informantene til de enkelte kommunene så på som den største utfordringen i forbindelse med Schrems II-dommen. De ulike kommunene er av ulik størrelse, har ulik grad av ressurser, diskuterer dommen på ulike møteplasser samt befinner seg på forskjellige steg etter veilederen fra Personvernrådet. Dette har betydning for hvilken utfordring kommunen så på som den største.

Over halvparten av kommunene så på vurderingen av om lovgivningen i tredjelandet gir tilstrekkelig beskyttelse (steg 3 i veilederen fra Personvernrådet), som den største utfordringen. Informantene mente at vurderingene er umulige for en kommune. De begrunnet dette med mangelen på konkrete retningslinjer fra Datatilsynet og EU, samt mangelen på ressurser, tid og verktøy til å foreta disse vurderingene i kommunen.

En av informantene nevnte usikkerheten rundt om systemene kommunen bruker er lovlige i lys av Schrems II, som den største utfordringen. Store deler av kommunens systemer bygger på enten Microsoft eller Azure sine tjenester. Informanten uttrykte bekymring for om kommunen må endre hele strukturen de bruker i dag.

En annen informant svarte at det er en utfordring å vurdere om standarden satt i Schrems II-dommen strider med andre lovkrav kommunen har. Informanten dro frem kravene kommunen har i forbindelse med smittesporing av Covid-19, som et eksempel. Folkehelseinstituttet krever at kommunen overfører dataen fra smittesporingen via et datasystem daglig. Disse systemene bygger på Azure sine tjenester. Schrems II-dommen stiller krav til at ytterligere tiltak innføres ved bruk av amerikanske leverandører. Dersom kommunen må kvitte seg med denne tjenesten på grunn av standarden satt i Schrems II, så oppfyller de ikke kravene til smittesporing.

5.4.4 Endring i systemer eller rutiner

Informantene ble stilt spørsmålet om de har vurdert og/eller gjennomført endringer i deres systemer eller rutiner etter Schrems II.

Den endringen som gikk igjen hos flere av kommunene var at de har laget nye rutiner ved anskaffelse av nye skytjenester. De skal blant annet bruke mer tid på å sjekke opp hvem som står som underleverandører, hvor dataen overføres og hvilket overføringsgrunnlag som brukes.

Flere av kommunene har vurdert om det er noen av de eksisterende avtalene kommunen har om skytjeneste, må avsluttes. Det var en av kommunene som kom frem til at en avtale om skytjeneste måtte avsluttes på grunn av Schrems II. Resten av kommunene har per midten av mars ikke avsluttet noen av de eksisterende avtalene de har.

En av de mindre kommunene har leid inn juridisk bistand for å sikre at anskaffelse av nye skytjenester er i tråd med regelverket.

5.5 Analyse og resultater av dybdeintervjuet med skyleverandøren

I dette kapittelet vil datamaterialet fra dybdeintervjuet med informanten som representerer skyleverandøren presenteres gjennom en kategorisk fremstilling. Kategoriene er delt inn etter spørsmålene som ble stilt under dybdeintervjuet. Det er informantens erfaringer og oppfatning som danner grunnlaget for svarene.

Spørsmålene var som følger:

- Hva ser dere på som den største utfordringen med Schrems II-dommen? Begrunn svaret deres.
- Sett fra deres ståsted, hvilken betydning har Schrems II-dommen for kommuner?
- Har dere som skyleverandør sett noen endring av kunders adferd?
- Har dere vurdert og/eller gjennomført noen endringer i deres systemer og/eller rutiner etter Schrems II-dommen?

Skyleverandøren leverer skytjenester til kommuner og brukes av flere av de intervjuede kommunene. De er kjent med problemstillingene som Schrems II-dommen har medført. Informanten informerte om at dommen diskuteres på en rekke møteplasser og at skyleverandøren som organisasjon kjenner godt til dommen.

5.5.1 Største utfordringen etter skyleverandøren sin mening

Informanten fortalte at Schrems II-dommen er en av flere tilbakemeldinger fra markedet på at det er et ønske om å håndtere personopplysninger på en annen måte. Problemstillinger rundt personvern og overføring av personopplysninger, er ikke nytt for skyleverandøren. Schrems II-dommen er nok et moment som gjør at skyleverandøren, må justere seg etter det som oppfattes som akseptabel håndtering av personopplysninger. Skyleverandøren ser derfor på Schrems II-dommen som en rettslig standard som de må forholde seg til.

Det er to utfordringer som skyleverandøren opplever som de største.

Den første utfordringen har vært at skyleverandøren har brukt mye tid på å forklare dommen og standarden satt i dommen på grunn av at informasjonen har vært vanskelig tilgjengelig for kundene til skyleverandøren. Dette tar mye tid og ressurser.

I tillegg nevner informanten at frem til de endelige veilederne fra Personvernrådet har kommet, befinner leverandører og brukere av skytjenester i et mellomstadium hvor ulike myndigheter, tilsyn og fagpersoner kommer med ulike anbefalinger. Skyleverandøren har innført noen ytterligere tiltak i forbindelse med veilederne fra Personvernrådet om Schrems II,[125] men de kan ikke endre for mye før de endelige veilederne har kommet.

5.5.2 Hvilken betydning har dommen for kommuner etter skyleverandøren sin mening

Dommen har betydning for kommuners bruk av skytjenester. Grunnen til dette er at skyleverandører ofte er globale, store aktører. Bruk av skytjenester innebærer derfor ofte at personopplysninger overføres over landegrensene.

Informanten til skyleverandøren mener at det må skje et kompetanseløft hos kommunene. Mange kommuner mangler ressursene og kompetansen for å forta de vurderingene som kreves etter Schrems II-dommen. Det er en stor jobb å kartlegge dataflyten av alle applikasjonene kommunen bruker i dag. Dommen krever at det gjennomføres en ny risikovurdering av alle disse applikasjonene.

Når de endelige veilederne fra Personvernrådet kommer, så må kommunene ta standpunkt til om noen av leverandørene de bruker ikke oppfyller kravene. Da må kommunen endre portoføLgen sin med de leverandørene kommunen bruker. Informanten til skyleverandøren mener at de fleste av leverandørene til en kommune på en eller annen måte vil oppfylle kravene Schrems II-dommen oppstiller.

[125] Hvilke ytterligere tiltak skyleverandøren har innført, er redegjort for i kapittel 5.5.4. Eksempler på ytterligere tiltak som Microsoft har innført, er redegjort for i kapittel 6.3.4.

5.5.3 Endring av kundenes atferd

For de tjenestene kommunene tar i bruk i dag, har det ikke skjedd så stor endring. Informanten informerte om at skyleverandøren har sett at kundene er avventende når det gjelder å inngå nye avtaler om skytjenester. Flere kommuner setter ikke i gang nye prosjekter. Skyleverandøren tror at mange kommuner er usikre, vil unngå bøter og ikke har nok kompetanse eller kapasitet til å vurdere om skyleverandøren oppfyller kravene etter Schrems II.

5.5.4 Endring i systemer eller rutiner

Skyleverandøren er en av skyleverandørene som var tidlig ute med å gjennomføre endringer etter Schrems II og veilederne fra Personvernrådet.

Skyleverandøren har innført kontraktuelle, juridiske og organisatoriske tiltak etter veilederne fra Personvernrådet. Som nevnt i punkt 4.3 er skyleverandørene henvist til å forholde seg til veilederne som har vært på høring frem til Personvernrådet kommer med en endelig fastsatt standard. Skyleverandøren har derfor innført tiltak som er i tråd med disse veilederne.

6 Utfordringer ved bruk av skytjenester i lys av Schrems II

6.1 Innledende ord

Kommuner har et stort antall applikasjoner som de tar i bruk på de ulike tjenesteområdene.[126] Disse applikasjonen er i all hovedsak anskaffet av hver enkelt kommune i markedet. Hvilke utfordringer de ulike kommune har i lys av Schrems II, kan derfor variere. Det varierer også hvilket steg i prosessen som Personvernrådet har oppstilt, de ulike kommunene har kommet til. Hvor omfattende tiltak som må gjennomføres, vil variere.

Som nevnt under punkt 3.1 er det mange fordeler med å ta i bruk en skytjeneste, blant annet bedre fleksibilitet, større kapasitet og ofte bedre sikkerhet. For at leverandørene skal kunne tilby større kapasitet og fleksibilitet, har de ofte av sikkerhetsmessige grunner reservelagring i et annet land, i noen tilfeller et annet kontinent.[127] Skyleverandører flytter dataen etter behov for å kunne tilby høy kapasitet. Dette innebærer at kommunen ikke alltid vet hvor dataen befinner seg. Dette kan gjøre det vanskelig å forholde seg til standarden satt i Schrems II-dommen.

I det følgende vil avhandlingen gjøre rede for hvilke krav som stilles til kommunene etter Schrems II-dommen og hvilke begrensninger dommen kan sette for bruk av de ulike tjenestemodellene. Risikoområdene som er beskrevet i dette kapittelet er ikke uttømmende. Situasjonen til kommunen kan medføre at andre problemstillinger enn de som nevnes, er aktuelle.

[126] Dette kom frem under dybdeintervjuene med kommunene som ble gjennomført i februar og mars 2021.
[127] Advokatfirma Føyen Torkildsen AS (2015) s. 5.

6.2 I hvilken grad påvirkes de ulike tjenestemodellene av Schrems II-dommen?

Schrems II-dommen har betydning for overføring av personopplysninger til tredjeland. Som nevnt i kapittel 2.2.1 skal personopplysninger forstås vidt. Dommen har også betydning for metadata. Metadata er data som beskriver annen data eller som inneholder ekstra informasjon knyttet til data.[128] «[M]etadata derived from electronic communication may also reveal very sensitive and personal information".[129] Metadata kan dermed også brukes til å identifisere en fysisk person.

Det avgjørende for om Schrems II-dommen får betydning for den aktuelle tjenestemodellen er om behandling av personopplysninger eller metadata som kan identifisere en fysisk person, omfattes av tjenesten. Det er behandlingsansvarlig som bestemmer at en skytjeneste skal tas i bruk og til hvilket formål. Det er derfor behandlingsansvarlig som bestemmer formålet med behandlingen av personopplysningene.

Ofte vil bruk av en SaaS-tjenestemodell omfatte behandling av personopplysninger i større eller mindre grad som kan brukes til å identifisere en fysisk person. Under flere av dybdeintervjuene med kommunene ble bruk av skytjenester i skolesektoren dratt frem som eksempel. Det stilles krav til opplæring i digitale ferdigheter på skolen. Flere kommuner bruker da Office 365 eller Google for å inkludere opplæring i digitale ferdigheter. Eleven får da tildelt en egen bruker hvor behandling av elevens personopplysninger skjer i denne løsningen.

I en SaaS-tjeneste lagres det også metadata. Som nevnt kan metadata brukes til å identifisere en fysisk person. Siden Schrems II-dommen har betydning for overføring av opplysninger som kan identifisere en fysisk person, vil dommen også ha betydning for metadataen som lagres i SaaS-tjenestemodellen.

En PaaS- og IaaS-tjenestemodell kan også omfatte lagring av personopplysninger samt metadata som kan brukes til å identifisere en fysisk person. Siden Schrems II-dommen har

[128] Gjersdal (2019).
[129] Proposal for directive on privacy and electronic communications, Vedlegg 1 avsnitt 2.

betydning for overføring av opplysninger som kan identifisere en fysisk person, vil dommen også ha betydning for en PaaS- og IaaS-tjenestemodell.

Schrems II-dommen og veilederne fra Personvernrådet skiller ikke på om det brukes en SaaS-, PaaS- eller IaaS-tjenestemodell, men problemstillingene og omfanget av vurderingene som må gjennomføres, kan variere etter hvilken tjenestemodell som er i bruk og hvor mye ansvar som er overlatt til skyleverandøren og kommunen.

Under flere av dybdeintervjuene med kommunene kom det frem at kommunene ikke skiller mellom de ulike tjenestemodellene når de følger veilederne fra Personvernrådet. Kommunene kartlegger alle tjenestene de tar i bruk uavhengig av om det er en SaaS-, PaaS- eller IaaS-tjeneste.

Som et oppfølgingsspørsmål til dybdeintervjuet med skyleverandøren, ble det sendt en mail til informanten om det er ulike tiltak som er innført for de ulike tjenestemodellene og hva begrunnelsen er. Informanten svarte at det er innført ulike tiltak for SaaS-tjenestemodellen på den ene siden og PaaS- og IaaS-tjenestemodellen på den andre siden. Årsaken til dette er at det er ulike produkter som krever ulike tiltak for å være i tråd med lovverket.

6.3 Utfordringer knyttet til veilederne fra Personvernrådet for bruk av skytjenester for en kommune

6.3.1 Kartlegging av eksisterende overføringer

Siden kommunene selv har ansvar for hvilken type data de har lagt i skyen, formålet med bruken av skytjenesten, hvem som skal ha tilgang til dataen og hvilken type skytjeneste de har valgt å ta i bruk, er det kommunen selv som har ansvar for å få oversikt over eksisterende overføringer.

Kommuner tar i dag i bruk forskjellige skytjenester med ulike underleverandører. Skytjenester kan være etablert på tvers av flere land og det kan være vanskelig å ha oversikt over hvilke land som kan være involvert.[130] Mange av leverandørene er amerikanske skyleverandører

[130] Normen (2020) s. 16.

eller skyleverandører med amerikanske underleverandører. Det å få oversikt over disse lange, uoversiktlige verdikjedene, er et omfattende arbeid. Kommunen må få oversikt over om skyleverandørene og deres underleverandører behandler personopplysninger eller metadata som kan brukes til å identifisere en fysisk person i et tredjeland. Under dybdeintervjuene med kommunene i februar og mars kom det frem at flere av kommunene befinner seg på enten steg en eller steg to.

Kommunen må undersøke hvilket land databehandleren og dens underdatabehandlere er fra, hvilket land de overfører, prosesser og lagrer personopplysningene de behandler på dine vegne i og hvem som har tilgang. Hvilke land de lagrer personopplysningene i, bør fremkomme av behandlingsprotokollen. Hvem som har tilgang til personopplysningene, bør fremkomme av databehandleravtalen.

Det følger av GDPR art. 30 at «[h]ver behandlingsansvarlig […] skal føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar» (heretter behandlingsprotokoll). Bestemmelsen beskriver videre hva protokollen skal inneholde. Protokollen skal blant annet inneholde informasjon om «overføringer av personopplysninger til en tredjestat […], herunder identifikasjon av nevnte tredjestat» samt «dersom det er mulig, en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene», jf. GDPR art. 30 første avsnitt bokstav e og g.

Under dybdeintervjuene med kommunene kom det frem at de i varierende grad har en oppdatert behandlingsprotokoll. En av kommunene har ikke tatt i bruk behandlingsprotokoll, noen av kommunene informerte om at behandlingsprotokollen deres er fullstendig oppdatert og de resterende har ikke fått oppdatert behandlingsprotokollen etter Schrems II. Arbeidet med å få oversikt over overføringene vil være betydelig lettere for de kommunene som har en oppdatert behandlingsprotokoll.

Informasjon om overføringene, særlig bruk av underleverandører og eventuelle overføringsgrunnlag, kan også fremkomme av databehandleravtalene. Dersom en kommune ikke har en oppdatert behandlingsprotokoll, kan kommunen gå gjennom de ulike databehandleravtalene. Dette kan være mer tids- og ressurskrevende for kommunen enn hvis de hadde hatt en oppdatert behandlingsprotokoll.

Dersom kommunen verken har en oppdatert behandlingsprotokoll eller finner informasjon om overføringene i databehandleravtalene, bør kommunen kontakte de aktuelle skyleverandørene. Kommuner bruker ofte flere skyleverandører, som igjen tar i bruk underleverandører. Det å få oversikt over overføringene på denne måten, vil ta lengre tid.

Hvilke utfordringer hver enkelt kommune vil møte på under dette steget vil variere etter hvor god oversikt de har over de ulike overføringene og hvilke ressurser de kan ta i bruk. Dersom kommunen har god oversikt over overføringene, for eksempel ved hjelp av en oppdatert behandlingsprotokoll, vil ikke dette steget være særlig problematisk. Flere av kommunene uttrykte at de ikke vet hvor de skal starte med kartleggingen og at de mangler den riktige kompetansen for å utføre kartleggingen.

6.3.2 Identifisering av overføringsgrunnlagene

For at en kommune lovlig skal kunne overføre personopplysninger til et tredjeland kreves det at overføringen har et overføringsgrunnlag, jf. GDPR kapittel V. Overføringsgrunnlaget skal sikre at «nivået for vern av fysiske personer som garanteres i denne forordningen, ikke undergraves», jf. GDPR art. 44. I kapittel 2.2.3 ble SCC dratt frem som et eksempel på et overføringsgrunnlag.

Dersom tredjelandet befinner seg på listen over de forhåndsgodkjente landene, trenger ikke kommunen å gå videre i prosessen. Schrems II-dommen har særlig betydning for skytjenester som overfører personopplysninger til USA med Privacy Shield som overføringsgrunnlag. I disse tilfellene må overføringsgrunnlaget byttes til SCC umiddelbart. Dommen har også betydning dersom skytjenesten bruker SCC om overføringsgrunnlag. Kommunene må da gå videre til neste steg for å vurdere beskyttelsesnivået i tredjelandet og eventuelt iverksette ytterligere tiltak.

Hvilke utfordringer kommuner vil møte på under identifiseringen av overføringsgrunnlaget til de ulike skytjenestene, varierer etter hvor god oversikt de har over de ulike overføringene. De kommunene som har god oversikt over overføringene, vil lettere kunne identifisere overføringsgrunnlagene.

Et eksempel på hvor utfordrende de to første stegene i veilederen fra Personvernrådet kan være, er bruk av Google sine skytjenester. Datatilsynet har skrevet en veileder om

utfordringer knyttet til bruk av Google og andre skytjenester i grunnskolen.[131] Datatilsynet uttaler at det er flere forhold som gjør Google som til en utfordrende databehandler. Det er blant annet vanskelig å få full oversikt over alle elementene som databehandleravtalen med Google omfatter.[132] Grunnen til dette er at Google henviser til andre nettsider i avtalen og disse nettsidene henviser videre til andre nettsider. I tillegg er deler av avtaleverket vanskelig formulert og kun skrevet på engelsk.[133] Det er et omfattende arbeid for kommunene å få oversikt over hele avtaleverket, herunder bruken av underleverandører og overføringsgrunnlaget. Uten denne kompetansen, blir dette betydelig vanskeligere.

6.3.3 Vurdering av beskyttelsesnivået i tredjelandet

Kommunen må foreta en konkret objektiv vurdering av hvert enkelt tredjeland i hver enkelt sak for å vurdere om tredjelandet har et tilsvarende beskyttelsesnivå for personopplysninger som innenfor EU/EØS. Dette innebærer en vurdering av om dataimportøren er underlagt lov(er) eller praksis som ikke gjør det mulig for dataimportøren å overholde sine forpliktelser. Dette er en vurdering som må foretas konkret for hvert enkelt mottakerland samt må sees i sammenheng med overføringen.

Dersom kommunen kommer frem til at lovgivningen i tredjelandet har et tilstrekkelig beskyttelsesnivå, kan kommunen gå direkte til steg 6.[134]

Vurderingen av lovgivningen i landet er en kompleks øvelse som krever at kommunen har god innsikt i både overvåknings- og personvernlovgivningen i det aktuelle tredjelandet og lovgivningen i EU. Kompleksiteten og mangelen på ressurser var en bekymring som kom frem under samtlige av dybdeintervjuene. I tillegg uttalte flere kommuner at Schrems II-dommen og dens konsekvenser ikke diskuteres nok innad i kommunen. Gjennomgangen av landevurderingen i Recommendations 02/2020 oppleves av kommunene som for generell og gjør at kommunene sitter igjen med flere spørsmål enn svar.[135]

I Schrems II-dommen vurderte EU-domstolen beskyttelsesnivået til de to amerikanske overvåkningslovene FISA 702 og EO 12.333. Domstolen konkluderte med at disse

[131] Datatilsynet (u.å.b.).
[132] Datatilsynet (u.å.b.) punkt 5.
[133] Datatilsynet (u.å.b.) punkt 6.
[134] Se figur 3 i avhandlingen og beskrivelsen av figuren for nærmere redegjørelse av dette.
[135] European Data Protection Board 2020b.

amerikanske overvåkningslovene ikke ga tilstrekkelig beskyttelse tilsvarende innenfor EU/EØS.[136]

U.S. Department of Commerce har imidlertid uttalt at de færreste amerikanske virksomheter håndterer personopplysninger som er av interesse for etterretning av amerikanske myndigheter.[137] Videre har de uttalt at de færreste virksomheter har mottatt ordre om å innhente personopplysninger etter FISA 702.[138] De hevder at den teoretiske muligheten for at amerikanske myndigheter skal få tilgang til personopplysninger som overføres fra EU uten virksomhetens kunnskap, ikke er større enn den teoretiske muligheten for at andre utenlandske myndigheter kan få tilgang.[139]

6.3.4 Ytterligere beskyttelsestiltak

Dersom kommunen i steg tre kommer frem til at overføringsgrunnlag ikke gir en reell og tilstrekkelig beskyttelse i tredjelandet tilsvarende innenfor EU/EØS, må kommunen vurdere om ytterligere beskyttelsestiltak kan lukke disse gapene. Hvilke beskyttelsestiltak som må innføres for å gi personopplysningene tilstrekkelig beskyttelse, vil variere etter om kommunen bruker en SaaS-, PaaS eller IaaS-tjeneste. Dersom tiltakene ikke gir tilstrekkelig beskyttelsesnivå, må kommunen slutte å bruke den aktuelle skytjenesten.

Veilederen angir tre typer tiltak som kan være aktuelle å innføre: kontraktuelle, tekniske og organisatoriske.[140] Kommunen må foreta en konkret vurdering av hver enkelt overføring, en såkalt case-by-case vurdering.[141] EU-domstolen har uttalt at kontraktuelle og organisatoriske tiltak i seg selv ikke er tilstrekkelig. Det kreves i tillegg at tekniske tiltak innføres.[142]

Personvernrådet har nevnt følgende ikke uttømmende momenter som er av betydning ved vurderingen av hvilke tiltak som er mest effektive:[143]

- Formatet på dataen som skal overføres (eksempelvis kryptert[144], i ren tekst).

[136] Schrems II [GC] C-311/18, avsnitt 179 flg.
[137] United States Department of Commerce (2020) s. 2.
[138] Ibid.
[139] United States Department of Commerce (2020) s. 3.
[140] European Data Protection Board 2020a.
[141] European Data Protection Board 2020a, s. 15.
[142] Ibid.
[143] European Data Protection Board 2020a, s. 16.
[144] Vilkårene for kryptering vil bli gjennomgått på neste side.

- Arten til personopplysningene.

- Lengden og kompleksiteten i databehandlingsflyten, antall aktører som er involvert i behandlingen og forholdet mellom dem.

- Muligheten for at personopplysningene kan bli gjenstand for videre overføring innen samme tredjeland eller et annet tredjeland.

Personvernrådet stiller seks vilkår for hvordan krypteringen skal foregå.[145] Det kan være krevende å oppfylle disse vilkårene. Det første vilkåret er at det skal foreligge sterk kryptering før overføring. Vilkår to er at krypteringen skal være robust mot «angrep» fra tredjelands myndigheter. Det tredje vilkåret er at krypteringen må være effektiv i hele perioden som opplysningene trenger vern. Fjerde vilkår er at krypteringsalgoritmen er feilfritt implementert av vedlikeholdte programvarer. Det femte vilkåret er at krypteringsnøklene forsvarlig håndteres. Det siste vilkåret som stilles er at krypteringsnøklene kun skal være håndtert under kontroll av dataeksportøren eller andre tredjeparter som har fått tillitt til å utføre dette. I tillegg må dette foregå innenfor EØS. Per i dag få aktører som klarer å håndtere dette veldig godt, særlig for større datamengder.

Personvernrådet har uttalt eksempler på senarioer hvor det ikke er implementert tilstrekkelig effektive tiltak.[146] Et eksempel er i tilfeller der overføring av personopplysninger til en skyleverandør i et tredjeland, krever tilgang til opplysningen i klar tekst. Personvernrådet uttaler at overføring til en slik skyleverandør hvor opplysningene fremkommer i klar tekst, ikke gir tilstrekkelig beskyttelse. Hvis man skal tolke ordlyden strengt, betyr dette at enhver dataoverføring til en skyleverandør som krever tilgang til personopplysningene i klar tekst, ikke er lovlig.

Hvilke utfordringer kommuner vil møte på under identifiseringen av ytterligere tiltak som gir tilstrekkelig beskyttelsesnivå, varierer. Senarioene i veilederne fra Personvernrådet er spesifikke og inneholder omfattende vilkår som må være oppfylt, eksempelvis de seks vilkårene for kryptering. Kompleksiteten til tiltakene og mangelen på ressurser var en bekymring som kom frem under samtlige av dybdeintervjuene.

[145] European Data Protection Board 2020a, s. 23–24.
[146] European Data Protection Board 2020a, s. 26–27.

Særlig om overføring av personopplysninger til USA

Personvernrådet uttaler at dersom dataimportøren omfattes av FISA 702, kan dataeksportøren bruke SCC som overføringsgrunnlag dersom ytterligere tekniske tiltak gjør det umulig eller ineffektivt for amerikanske myndigheter å få tilgang til personopplysningene.[147]

Videre uttaler Personvernrådet om ytterligere tiltak at «US data importers that fall under […] FISA 702 are under a direct obligation to grant access to or turn over imported personal data that are in their possession, custody or control. This may extend to any cryptographic keys necessary to render the data intelligible».[148]

Dette innebærer at overføring av data til USA vil som hovedregel kreve kryptering for å oppfylle retningslinjene fra Personvernrådet, og at det ikke er mulig å treffe tekniske tiltak som gjør det lovlig å bruke amerikanske skyleverandører som trenger tilgang til personopplysninger i ukryptert form.

For å begrense amerikanske myndigheters tilgang til å innhente informasjon etter EO 12.333 kan en bruke en kombinasjon av kontraktuelle- og tekniske tiltak. Det kan for eksempel avtales at dataimportøren ikke frivillig hjelper amerikanske myndigheter med å innhente data og at personopplysningene er krypterte.

Eksempler på ytterligere tiltak som er innført av en skyleverandør

Skyleverandøren Microsoft var tidlig ute med å gjennomføre endringer etter Schrems II og veilederne fra Personvernrådet.

Den 16. juli 2020 kunngjorde Microsoft at overføringer av personopplysninger vil fra 21. juli 2020 følge SCC. Alle Microsoft sine onlinetjenester er etter 21. juli dekket av én og samme databehandleravtale, og et og samme overføringsgrunnlag der det er aktuelt med overføringer til tredjeland. De kunngjorde samme dag at Privacy Shield ikke lengre brukes som hjemmel for overføringer til USA.

I november kunngjorde Microsoft at de har innført en rekke tiltak som beskytter blant annet kommuner som ønsker å fortsette å ta i bruk eller ønsker å ta i bruk Microsoft sine skytjenester. Microsoft mener selv at disse tiltakene gir sterkere beskyttelse enn det

[147] European Data Protection Board 2020a, s. 15.
[148] European Data Protection Board 2020a, s. 22.

Personvernrådet har anbefalt. Disse nye tiltakene er som følger: Microsoft «are committing that [they] will challenge every government request for public sector or enterprise customer data from any government – where there is a lawful basis for doing so», og «provide monetary compensation to these customers´ users if [they] disclose their data in response to a government request in violation of the […] GDPR».

Videre skriver Microsoft at disse tiltakene vil komme i tillegg til de beskyttelsestiltakene Microsoft allerede tilbyr: sterk kryptering, at de ikke gir noen myndigheter uhindret tilgang til personopplysninger, gjennomsiktighet ved at de publiserer informasjon om krav fra myndighetene og at de har oversikt over juridiske suksess.

Ved å publisere blogginnlegg med oppdateringer om hvordan Microsoft forholder seg til Schrems II-dommen og veilederne fra Personvernrådet, kan prosessen virke mer transparent for brukerne av skytjenestene. Microsoft mener selv at disse tiltakene gir sterkere beskyttelse enn det Personvernrådet har anbefalt.[149]

Selv om Microsoft har innført disse ytterligere tiltakene, må kommunene selv vurdere om disse ytterligere beskyttelsestiltakene kan oppfylle beskyttelsesnivået som kreves. Microsoft er et amerikansk selskap som kan være underlagt de amerikanske overvåkningslovene. EU-domstolen har i Schrems II-dommen vurdert at beskyttelsesnivået for personopplysninger i USA ikke er tilstrekkelig.

Eksempler som illustrerer viktigheten av ytterligere tiltak

I mars avsa den franske domstolen Conseil dÉtat og datatilsynet i den tyske delstaten Bayern hver sin avgjørelse som illustrerer viktigheten av å innføre ytterligere tiltak der beskyttelsesnivået i mottakerlandet ikke er tilstrekkelig. Det er viktig å merke seg at en dom fra Frankrike og Tyskland ikke bindende for norske domstoler.

Den 12. mars 2021 avsa Conseil dÉtat[150] en dom om franske myndigheter lovlig kunne ta i bruk en skyleverandør, som hadde morselskap i USA, for booking av koronatester.[151]

[149] Microsoft (2020b).
[150] Frankrikes øverste forvaltningsdomstol.
[151] Dom avsagt av Conseil Détat den 12. mars 2021. Dommen har beslutningsnummer 450163. Link til dommen: https://www.conseil-etat.fr/Media/actualites/documents/2021/03-mars/450163.pdf. [AWS-dommen] (lest 15.03.21).

Leverandøren bruker tjenestene til det luxembourgske selskapet AWS Sarl som har datasentre i Frankrike og Tyskland.[152] Det ble ikke overført personopplysninger til USA.[153]

Den franske domstolen kom frem til at det var en risiko for at amerikanske myndigheter kunne kreve tilgang til personopplysninger selv om personopplysningene ikke ble overført til morselskapet i USA.[154] Domstolen måtte derfor vurdere, i tråd med standarden satt i Schrems II, om beskyttelsesnivået for behandlingen av personopplysningene var tilstrekkelig etter GDPR.

Domstolen konkluderte med at det var mulig for franske myndigheter å ta i bruk leverandøren, og begrunnet dette med at de tekniske og kontraktuelle tiltakene var tilstrekkelig for å sikre beskyttelsesnivået som kreves etter GDPR.[155] Domstolen bemerket at kontrakten ga en garanti om en spesifikk prosedyre dersom utenlandske myndigheter ba om tilgang til personopplysningene og at alle tilgangsforespørsler fra en offentlig myndighet ville utfordres.[156] I tillegg var personopplysningene kryptert, og nøkkelen lå hos en tredjepart i Frankrike.[157] Personopplysningene inneholdt heller ingen helsedata, kun identifikasjon av personer for å avtale tidspunkt for test.[158] Domstolen la også vekt på at dataene slettes etter tre måneder.[159] Domstolen kom dermed frem til at beskyttelsesnivået var tilstrekkelig.

Den 15. mars 2021 avsa The Bavarian DPA (BayLDA)[160] en avgjørelse om lovligheten av å ta i bruk et nyhetsbrevverktøy som bruker en amerikansk leverandør.[161] Klageren sendte inn en klage til BayLDA angående bruken av Mailchimp hos den tyske virksomheten.[162] Klageren begrunnet klagen med at virksomheten ulovlig overførte e-postadresser til abonnentene av nyhetsbrevet, til den amerikanske leverandøren av Mailchimp.[163]

---

[152] AWS-dommen, s. 6, punkt 7.
[153] Ibid.
[154] Ibid.
[155] AWS-dommen, s. 6, punkt 8.
[156] Ibid.
[157] Ibid.
[158] Ibid.
[159] Ibid.
[160] Datatilsynet i den tyske delstaten Bayern.
[161] Avgjørelse avsagt av The Bavarian DPA den 15. mars 2021. Avgjørelsen har beslutningsnummer LDA-1085.1-12159/20-IDV. Link til avgjørelsen: https://gdprhub.eu/index.php?title=BayLDA_-_LDA-1085.1-12159/20-IDV. [Mailchimp-dommen] (lest 17.03.21).
[162] Ibid.
[163] Ibid.

Virksomheten responderte med at bruken av nyhetsverktøyet bare var sporadisk og at virksomheten hadde sluttet å bruke dette verktøyet.[164]

BayLDA mente at den tyske virksomhetens bruk av Mailchimp, og dermed overføringen av e-postadressene til den amerikanske leverandøren av Mailchimp, var ulovlig.[165] Overføringsgrunnlaget for overføringen var basert på SCC.[166]

Det tyske tilsynet kom frem til at leverandøren av Mailchimp kunne falle inn under «electronic communication service provider» i FISA702 og sto i fare for å bli overvåket av amerikanske myndigheter.[167] Det var en risiko for at amerikanske myndigheter kunne kreve innsyn i personopplysningene. Domstolen måtte derfor vurdere, i tråd med standarden satt i Schrems II, om beskyttelsesnivået for behandlingen av personopplysningene var tilstrekkelig etter GDPR.

Den tyske virksomheten hadde, til forskjell fra virksomheten i den franske dommen, ikke vurdert om ytterligere beskyttelsestiltak kunne sikre at personopplysningene var tilstrekkelig beskyttet mot overvåkning.[168] BayLDA kom derfor frem til at den tyske virksomhetens bruk av Mailchimp, og dermed overføringen av e-postadressene til den amerikanske leverandøren av Mailchimp, var ulovlig.[169]

6.3.5 Implementering av beskyttelsestiltakene

Dette steget går ut på at de ytterligere tiltakene må implementeres i avtaleforholdet mellom partene. Dette innebærer både at selve databehandleravtalen oppdateres (kontraktuelle tiltak) og at organisatoriske tiltak iverksettes for å sikre at tiltakene blir en integrert del av den daglige driften.

Dersom dataeksportøren vil innføre tiltak i tillegg til kravene i SCC, presiserer Personvernrådet at tiltakene ikke skal stride med vilkårene i SCC.[170] Dersom tilleggstiltakene

[164] Ibid.
[165] Ibid.
[166] Ibid.
[167] Ibid.
[168] Ibid.
[169] Ibid.
[170] European Data Protection Board 2020a, s. 17.

strider med vilkårene i SCC, må dataeksportøren søke om autorisasjon hos kompetent tilsynsmyndighet i samsvar med GDPR art. 46 nr. 3 bokstav a.[171]

Under dybdeintervjuene nevnte flere kommuner at de så på det som tidskrevende å gjennomgå databehandleravtalene for å se om de ytterligere tiltakene strider med vilkårene i avtalen. I tillegg er det fortsatt juridiske uklarheter rundt dommen. Kommunene må tilpasse seg eventuelle nye anbefalinger og veiledere.

6.3.6 Oppfølging av beskyttelsesnivået

Regelmessig gjennomgang av de nevnte kartleggingene og vurderingene er viktig for å avdekke eventuelle endringsbehov.[172] Lovgivningen eller praksisen som tiltakene er basert på, kan endre seg. Det kan bli nødvendig å innføre nye tiltak eller midlertidig stoppe bruken av den aktuelle skytjenesten.

Under dybdeintervjuene nevnte flere av kommunene at de bruker mange ulike applikasjoner og tjenester. Det å gjennomgå alle disse tjenestene regelmessig oppfattes som omfattende.

[171] European Data Protection Board 2020a.
[172] Ibid.

7 Avsluttende ord

7.1 Konklusjon

Denne avhandlingen har belyst at det er et mulighetsrom for kommuner å ta i bruk skytjenester også etter standarden satt i Schrems II-dommen, men at det er tids- og ressurskrevende å vurdere om skytjenester som overfører personopplysninger til tredjeland kan brukes. Datatilsynet har uttalt at kommuner bør «vente med å inngå nye avtaler med tredjelandsleverandører inntil man er helt sikker på at man fullt ut klarer å etterleve alle EU-domstolenes tilleggsvilkår».[173] Ved vurderingen av om en kommune kan ta i bruk en skytjeneste hvor databehandleren med underleverandører befinner seg i et tredjeland, er det en rekke vurderinger som må gjennomføres.[174] Det utslagsgivende for konklusjonen er om beskyttelsesnivået av personopplysningene er tilsvarende innenfor EU/EØS.

Det avgjørende for om Schrems II-dommen får betydning for den aktuelle tjenestemodellen kommunen har eller ønsker å ta i bruk, er om behandling av personopplysninger eller metadata som kan identifisere en fysisk person, omfattes av tjenesten. Under dybdeintervjuene med de utvalgte kommunene kom det frem at samtlige av kommunene for det meste bruker SaaS-skyløsninger. Enkelte av tjenestene kommunene bruker er eller inneholder også PaaS- eller IaaS-løsninger. Verken Schrems II-dommen eller veilederne fra Personvernrådet skiller på om kommunen brukes en SaaS-, PaaS- eller IaaS-tjenestemodell. Omfanget av vurderingene som må gjennomføres kan imidlertid variere etter hvilken tjenestemodell som er i bruk og hvor mye ansvar som er overlatt til skyleverandøren.[175]

Kommunene har i ulik grad tilpasset seg standarden satt i Schrems II-dommen. Dybdeintervjuene med de utvalgte kommunene viser at det finnes både kommuner som velger å avstå fra å inngå nye avtaler om skytjenester, som avslutter anskaffelser av skytjenester som allerede er igangsatt og som endrer rutiner og systemer for å kunne fortsette å ta i bruk skytjenester.[176] Inntrykket etter dybdeintervjuene er at kommunene har ulikt syn på om og hvordan de skal kunne fortsette å bruke skytjenester etter Schrems II-dommen.

[173] Datatilsynet (2020).
[174] Se kapittel 4.3 og 6.3 for en gjennomgang av hvilke vurderinger kommunen må gjennomføre.
[175] Se kapittel 6.3 for redegjørelse av disse forskjellene.
[176] Se mer om dybdeintervjuene i kapittel 5.

7.2 Hindringer og muligheter for at markedsplassen blir en suksess i lys av Schrems II-dommen

I den nasjonale strategien for bruk av skytjenester fremmet regjeringen et ønske om at det etableres en markedsplass for skytjenester rettet mot offentlig sektor i Norge.[177] I denne forbindelse er det uttalt at en slik markedsplass vil kvalitetssikre skyleverandørene samt tjenestene deres.[178] Schrems II-dommen har medført nye problemstillinger for skyleverandørene og kommuner som ønsker å ta i bruk en skytjeneste. For at markedsplassen skal bli en suksess etter Schrems II-dommen, bør DFØ ta hensyn til nye problemstillinger rundt roller og ansvar.

En viktig forutsetning for at markedsplassen skal bli en suksess, er at den blir brukt og oppleves som nyttig for både skyleverandører og kunder (eksempelvis kommuner). Som nevnt i kapittel 5.2.1 er det flere av kommunene som avventer med å anskaffe nye skytjenester blant annet på grunn av usikkerheten rundt lovligheten av de ulike skytjenestene etter Schrems II-dommen. DFØ sin ambisjon er at markedsplassen skal bli den prefererte møteplassen for anskaffelse av sikre, lovlige og kostnadseffektive skytjenester.

Kritiske suksessfaktorer for markedsplassen, er at kommuner finner informasjon med eksempler som gir trygghet, blant annet om hvordan kommunene skal gjennomføre risikovurderinger, eksempler på andre brukere av tjenesten, hva som er gode kravspesifikasjoner og hvilke rammeavtaler Statens innkjøpssenter har registrert på skytjenesten. Kommunene vil da lettere forstå egenskapene, funksjonene og brukervilkårene til de ulike skytjenestene uten å måtte ta kontakt med skyleverandøren.

En annen kritisk suksessfaktor for markedsplassen er at den fremstår som troverdig og attraktiv ovenfor skyleverandørene og kommunene. Dette kan blant annet oppnås ved å kun la troverdige og seriøse skyleverandører ta i bruk markedsplassen. Dette krever at markedsplassen fungerer som en form for kvalitetssikring av leverandørene og tjenestene blant annet i lys av Schrems II-dommen. Kommunene vil imidlertid fortsatt måtte foreta en risikovurdering av leverandøren og tjenesten.

[177] Kommunal- og moderniseringsdepartementet (2016) s. 26.
[178] Ibid.

I Direktoratet for forvaltning og ikt (Difi) sin forprosjektrapport for markedsplassen viser de til en undersøkelse der det fremkommer at en gjennomsnittlig kommune bruker nærmere 200 IKT-systemer daglig.[179] Selv om mange av kommunene bruker de samme systemene fra de samme leverandørene, har de ofte ulike versjoner og spesialtilpasninger.[180] Mangelen på standardiserte produkter og anskaffelsesprosesser satt sammen med utfordringene Schrems II-dommen medfører, er en av grunnene til at kommuner ikke går til anskaffelser av nye skytjenester. I rapporten til Difi uttrykkes det at markedsplassen sitt mandat er å forenkle anskaffelse av nye skytjenester, og stimulere leverandørene til å videreutvikle og standardisere sine tjenester.[181]

Totalt sett er det essensielt at kommunene opplever markedsplassen som nyttig og troverdig, at den reduserer risikoen ved inngåelse av avtale om skytjeneste, fungerer som en form for kvalitetssikring av skyleverandørene samt innfrir oppsatte budsjetter ved anskaffelse av skytjenester.

7.3 Avsluttende bemerkninger *de lege ferenda*

Bruken av skytjenester i det offentlige er stadig økende, og vil trolig fortsette å øke. Det økende politiske søkelyset på skytjenester i Norge oppfordrer kommunene til å ta i bruk skytjenester. Schrems II-dommen har satt ny standard for bruk av skytjenester som overfører personopplysninger til tredjeland.

På bakgrunn av dette og den rettskildeanalysen som er foretatt i kapittel 2 og 4, foreligger det en sterk oppfordring til lovgivende myndigheter om å ta grep. Nødvendige lovendringer må enten foretas internasjonalt og deretter gjennomføres i norsk lov, eller foretas nasjonalt.

Under dybdeintervjuene uttrykte kommunene at vurderingen av om beskyttelsesnivået i tredjelandet er tilstrekkelig, er for krevende for en kommune. Det følger av GDPR art. 5 nr. 2 at det er kommunen som er «ansvarlig for og skal kunne påvise» at reglene i GDPR følges. Når EU-kommisjonen godkjenner overføringer av personopplysninger til et bestemt land etter GDPR art. 45, bruker de flere måneder på å vurdere beskyttelsesnivået i dette landet. Schrems II-dommen medfører at alle kommuner skal foreta samme vurdering som EU-kommisjonen

[179] Direktoratet for forvaltning og ikt (2018) s. 9.
[180] Ibid.
[181] Direktoratet for forvaltning og ikt (2018) s. 10.

rundt beskyttelsesnivået til alle tredjeland kommunen tar i bruk. Nasjonale eller internasjonale myndigheter bør komme med en klar veileder om hvilke land som oppfyller dette kravet da denne vurderingen er tilnærmet umulig for en kommune.

Den 16. desember 2020 konkluderte Skates[182] arbeidsutvalg at det skulle opprettes en koordineringsgruppe i arbeidet med Schrems II-dommen.[183] Koordineringsgruppen jobber med å identifisere felles utfordringer med Schrems II-dommen og diskutere disse, få felles informasjon fra de store skyleverandørene og ha dialog med blant annet Datatilsynet.[184] Dette arbeidet kan gi nyttig informasjon til kommunene.

[182] Skate er et strategisk samarbeidsråd og rådgivende organ til Digitaliseringsdirektoratet.
[183] Digitaliseringsdirektoratet (u.å.).
[184] Ibid.

8 Litteraturliste

8.1 Lovregister

Norsk lovgivning

Grunnloven	Lov 17. mai 1814 Kongeriket Norges Grunnlov (Grunnloven)
Arkivlova	Lov 4. desember 1992 nr. 126 om arkiv (arkivlova)
Bokføringsloven	Lov 19. november 2004 nr. 73 om bokføring (bokføringsloven)
Sikkerhetsloven	Lov 1. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven)
Kommuneloven	Lov 22. juni 2018 nr. 83 om kommuner og fylkeskommuner (kommuneloven)

Andre lands lovgivning

E.O. 12.333	Executive Order 12333, 4. Desember 1981
FISA 702	Foreign Intelligence Surveillance Act: Section 702, 50 U.S.C. § 1881 a

Lovgivning i EU

EUs Personverndirektiv	Europaparlamentet og Rådets direktiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger [OPPHEVET]

Proposal for directive on privacy and electronic communications	Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC
TEU	Traktaten om Den europeiske union (TEU), Lisboa, 01.12.2009
TEUV	Traktaten om Den europeiske unions virkeområde (TEUV), Roma, 07.06.2016
GDPR	Europaparlaments – og rådsforordning (EU) 2016/679 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt oppheving av direktiv 95/46/EF (personvernforordningen) [GDPR]
EU–US Privacy Shield	Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C (2016) 4176) (Text with EEA relevance), 12. Juli 2016

8.2 Rettspraksis

EU-domstolen

Probst, C-119/12	Dom av 22. november 2012 [A5], Probst, C-119/12, EU:C:2012:748
Schrems I, C-362/14	Dom av 6. oktober 2015 [GC], Schrems I, C-362/14, EU:C:2015:650

Nowak, C-434/16	Dom av 20. desember 2017 [Second Chamber], Nowak, C-434/16, EU:C:2017:994
Schrems II, C-311/18	Dom av 16. juli 2020 [GC], Schrems II, C-311/18, EU:C:2020:559

Andre lands rettsprakis

AWS-dommen	Dom avsagt av Conseil Détat den 12. mars 2021. Dommen har beslutningsnummer 450163. Link til dommen: https://www.conseil-etat.fr/Media/actualites/documents/2021/03-mars/450163.pdf
Mailchimp-dommen	Avgjørelse avsagt av The Bavarian DPA den 15. mars 2021. Avgjørelsen har beslutningsnummer LDA-1085.1-12159/20-IDV. Link til avgjørelsen: https://gdprhub.eu/index.php?title=BayLDA_-_LDA-1085.1-12159/20-IDV

8.3 Litteratur

Advokatfirma Føyen Torkildsen AS (2015)	Advokatfirmaet Føyen Torkildsen AS, *Utredning av juridiske forhold ved bruk av nettsky i kommunal sektor – en mulighetsstudie*, 2015, https://www.ks.no/contentassets/08fa81b873e54942ad6725f3089d8bee/endelig-rapport-om-bruk-av-skytjenester-i-kommunal-sektor.pdf (sist lest 01.02.21)
Datatilsynet (u.å.a.)	Datatilsynet, *Det europeiske Personvernrådet (EDPB)*, u.å., https://www.datatilsynet.no/regelverk-og-

verktoy/internasjonalt/personvernradet/ (sist lest 04.03.21)

Datatilsynet (u.å.b.) Datatilsynet, *Bruk av Google Cromebook og G Suite for Education (og andre skytjenester) i grunnskolen*, u.å., https://www.datatilsynet.no/personvern-pa-ulike-omrader/skole-barn-unge/bruk-av-google-chromebook-og-g-suite-for-education-og-andre-skytjenester-i-grunnskolen/google-som-databehandler/ (sist lest 16.03.21)

Datatilsynet (u.å.c.) Datatilsynet, *Datatilsynets oppgaver*, u.å., https://www.datatilsynet.no/om-datatilsynet/oppgaver/ (sist lest 09.04.21)

Datatilsynet (2018) Datatilsynet, *Skytjenester*, 2018, https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/skytjenester/ (sist lest 27.03.21)

Datatilsynet (2020) Datatilsynet, *Spørsmål og svar om nye regler for overføring av personopplysninger til land utenfor EØS*, 27.07.2020, https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/sos-om-nye-regler-for-overforing/ (sist lest 19.04.21)

Digitaliseringsdirektoratet (u.å.) Digitaliseringsdirektoratet, *Koordinering av arbeidet med Schrems II-dommen*, u.å., https://www.digdir.no/digitalisering-og-samordning/koordinering-av-arbeidet-med-schrems-ii-dommen/2387 (sist lest 07.05.21)

Eckhoff (1997) Torstein Eckhoff og Jan Erik Helgesen, *Rettskildelære*, 4. utg., Tano Aschehoug, 1997

European Commission (2007)	European Commission, *Opinion 4/2007 on the concept of personal data*, WP136, 20. Juni 2007
European Data Protection Board (u.å.)	European Data Protection Board, *About EDPB*, u.å., https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en (sist lest 24.03.21)
European Data Protection Board 2020a	European Data Protection Board, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, 10. November 2020, https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf (lastet ned 01.02.21)
European Data Protection Board 2020b	European Data Protection Board, *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, 10. November 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf (lastet ned 01.02.21)
Fredriksen og Mathisen (2014)	Halvard Haukeland Fredriksen og Gjermund Mathisen, *EØS-rett*, 2. utg., Fagbokforlaget 2014
Gjersdal (2019)	Aud Gjersdal, *Metadata* i Store norske leksikon, 11. november 2019, https://snl.no/metadata (sist lest 20.03.21)
Kommunal- og moderniseringsdepartementet (2016)	Kommunal- og moderniseringsdepartementet, *Nasjonal strategi for bruk av skytjenester*, 2016, https://www.regjeringen.no/contentassets/4e30afec51734d458596e723c0bdea0e/nasjonal_strategi_for_bruk_av_skytenester.pdf (sist lest 13.04.21)

Kommunal- og moderniseringsdepartementet (2021)	Kommunal- og moderniseringsdepartementet, *Digitaliseringsrundskrivet,* 2021, https://www.regjeringen.no/no/dokumenter/digitaliseringsrundskrivet/id2826781/ (sist lest 17.02.21)
Kuner og Marelli (u.å.)	Christopher Kuner og Massimo Marelli, *Handbook on data protection in humanitarian action*, 2. utg, u.å., https://reliefweb.int/sites/reliefweb.int/files/resources/4305_002_DataProtection2020_web.pdf (sist lest 15.02.21)
Mell og Grance (2011)	Peter Mell og Timothy Grance, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*, U.S. Department of Commerce, NIST Special Publication 800-145, 2011, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (sist lest 02.03.21)
Microsoft (2020a)	Microsoft, *Assuring Customers About Cross-Border Data Flows*, 16. Juli 2020, https://blogs.microsoft.com/eupolicy/2020/07/16/assuring-customers-about-cross-border-data-flows/ (sist lest 27.02.21)
Microsoft (2020b)	Microsoft, *New steps to defend your data*, 19. November 2020, https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/ (sist lest 23.02.21)
Microsoft (2021)	Microsoft, *Shared responsibility in the cloud*, 03. Februar 2021, https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility (sist lest 17.02.21)

Nasjonal Sikkerhetsmyndighet (u.å.)	Nasjonal Sikkerhetsmyndighet, *Ofte stilte spørsmål om sky og tjenesteutsetting*, u.å., https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/ofte-stilte-sporsmal-om-sky-og-tjenesteutsetting/sporsmal-om-sky-og-tjenesteutsetting/ (sist lest 23.02.21)
Nasjonal sikkerhetsmyndighet (2020)	Nasjonal sikkerhetsmyndighet, *Helhetlig digitalt risikobilde*, 2020, https://nsm.no/getfile.php/134468-1604926904/Demo/Dokumenter/Rapporter/NSM_IKT-risikobilde_2020_enkeltside.pdf (sist lest 13.03.21)
Normen (2020)	Styringsgruppen for Normen, *Veileder i bruk av skytjenester til behandling av helse- og personopplysninger*, 2020, https://ehelse.no/normen/veiledere/veileder-i-bruk-av-skytjenester-til-behandling-av-helse-og-personopplysninger (sist lest 22.02.21)
Skullerud, Rønnevik, Skorstad og Pellerud (2018)	Åste Marie Bergseng Skullerud, Cecilie Rønnevik, Jørgen Skorstad og Marius Engh Pellerud, *Personvernforordningen (GDPR) Kommentarutgave*, Universitetsforlaget, 2018
Stemsrud (2015)	Odd Stemsrud, *EØS-rett i et nøtteskall*, Gyldendal Norsk Forlag 2015
Sævold (2019)	Heidi Sævold, «Fersk rapport: Dette er de svakeste leddende i store bedrifters nettverk», *digi.no*, 1. mars 2019, https://www.digi.no/artikler/fersk-rapport-dette-er-de-svakeste-leddene-i-store-bedrifters-nettverk-br/459169 (sist lest 23.02.21)
The National Security Agency (2013)	The National Security Agency, *The National Security Agency: Missions, Authorities, Oversight and Partnerships*, PA-026-18, 2013,

https://www.nsa.gov/news-features/press-room/Article/1618729/ (sist lest 20.03.21)

United States Department of Commerce (2020) — United States Department of Commerce International Trade Administration, *Information on U.S. Privacy Shield Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*, White Paper, 2020, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000kyhX (sist lest 11.02.21)

Lister over tabeller, figurer o.l.

Vedlegg 1

Notatet som ble sendt ut til kommunene i forbindelse med dybdeintervjuene

Tusen takk for dere ønsker å stille til dybdeintervju. Samtalen vil handle om Schrems II og hvilke hindringer og muligheter dommen gir for bruk av skytjenester. Egen opplevelse og refleksjoner rundt dette vil utgjøre en viktig del av samtalen. I masteroppgaven vil jeg bruke denne informasjonen til å eksemplifisere problemstillinger som ulike aktører møter på ved bruk av skytjenester.

I sommer avsa EU-domstolen Schrems II-dommen. Dommen har betydning for overføringer av personopplysninger til land utenfor EU/EØS (såkalte tredjeland). Domstolen ugyldiggjorde bruk av Privacy Shield som overføringsgrunnlag til USA med umiddelbar virkning. Domstolen begrunnet dette med at den amerikanske lovgivningen ikke sikrer tilstrekkelig beskyttelsesnivå i henhold til GDPR. Domstolen viste til at de amerikanske lovene FISA 702 og EO 12.333 åpnet for at amerikanske myndigheter kunne masseovervåke europeiske borgere uten samtykke. EU-domstolen konstaterte at Standard Contractual Clauses (SCC) fremdeles er gyldige, men at det i seg selv ikke er tilstrekkelig for at overføringer til tredjeland.

Personvernrådet i EU kom i november med to veiledere som skulle bidra med å oppklare noen av punktene i Schrems II-dommen. De presenterer en vurdering som består av seks steg som skal foretas ved overføringer av personopplysninger til tredjeland. Første steg går ut på å skaffe seg oversikt over alle overføringer til tredjeland. Andre steg går ut på å undersøke overføringsgrunnlaget som benyttes i dag. Steg tre er å vurdere hvorvidt overføringsgrunnlaget sikrer den samme beskyttelsen som innenfor EU/EØS. Steg fire er å vurdere ytterligere beskyttelsestiltak, som eksempelvis kryptering og anonymisering. Steg fem går ut på å inkorporere disse tiltakene i avtaleforholdet. Siste steg er å re-evaluere og gjennomføre disse vurderingene med jevne mellomrom.

Her er spørsmålene som vil bli stilt under intervjuet:

1. Hvor godt kjenner din virksomhet til Schrems II på en skala fra 1 til 10 (der 1 er svært dårlig og 10 er svært godt)? Hvilke møteplasser diskuteres dommen?

2. Ta utgangspunkt i Personvernrådet sin veileder. Hvilket steg i prosessen vil du si at din virksomhet befinner seg på?

3. Hva ser dere på som den største utfordringen med Schrems II i deres virksomhet? Begrunn svaret deres.

4. Har dere vurdert og/eller gjennomført endringer i deres systemer og/eller rutiner etter Schrems II?

Vedlegg 2

Notatet som ble sendt ut til skyleverandøren i forbindelse med dybdeintervjuet

Tusen takk for at dere ønsker å stille til dybdeintervju. Samtalen vil handle om Schrems II og hvilke hindringer og muligheter dommen gir for bruk av skytjenester. Egen opplevelse og refleksjoner rundt dette vil utgjøre en viktig del av samtalen. I masteroppgaven vil jeg bruke denne informasjonen til å eksemplifisere problemstillinger som ulike aktører møter på ved bruk av skytjenester.

I sommer avsa EU-domstolen Schrems II-dommen. Dommen har betydning for overføringer av personopplysninger til land utenfor EU/EØS (såkalte tredjeland). Domstolen ugyldiggjorde bruk av Privacy Shield som overføringsgrunnlag til USA med umiddelbar virkning. Domstolen begrunnet dette med at den amerikanske lovgivningen ikke sikrer tilstrekkelig beskyttelsesnivå i henhold til GDPR. Domstolen viste til at de amerikanske lovene FISA 702 og EO 12.333 åpnet for at amerikanske myndigheter kunne masseovervåke europeiske borgere uten samtykke. EU-domstolen konstaterte at Standard Contractual Clauses (SCC) fremdeles er gyldige, men at det i seg selv ikke er tilstrekkelig for at overføringer til tredjeland.

Personvernrådet i EU kom i november med to veiledere som skulle bidra med å oppklare noen av punktene i Schrems II-dommen. De presenterer en vurdering som består av seks steg som skal foretas ved overføringer av personopplysninger til tredjeland. Første steg går ut på å skaffe seg oversikt over alle overføringer til tredjeland. Andre steg går ut på å undersøke overføringsgrunnlaget som benyttes i dag. Steg tre er å vurdere hvorvidt overføringsgrunnlaget sikrer den samme beskyttelsen som innenfor EU/EØS. Steg fire er å vurdere ytterligere beskyttelsestiltak, som eksempelvis kryptering og anonymisering. Steg fem går ut på å inkorporere disse tiltakene i avtaleforholdet. Siste steg er å re-evaluere og gjennomføre disse vurderingene med jevne mellomrom.

Her er spørsmålene som vil bli stilt under intervjuet:

1. Hva ser dere på som den største utfordringen med Schrems II-dommen? Begrunn svaret deres.

2. Sett fra deres ståsted, hvilken betydning har Schrems II-dommen for norske kommuner?

3. Har dere som skyleverandør sett noen endring på kunders adferd?

4. Har dere vurdert og/eller gjennomført noen endringer i deres systemer og/eller rutiner etter Schrems II-dommen?