Overføring av personopplysninger til USA i kjølvannet av Schrems II-saken

I hvilken utstrekning kan virksomheter hensynta den faktiske risikoen for å bli utsatt for offentligrettslige innsynsbegjæringer ved vurderingen av om tredjestaten sikrer et tilstrekkelig beskyttelsesnivå ved bruk av standardkontraktsbestemmelser som overføringsgrunnlag?

Kandidatnummer: 70

Antall ord: 14 986

JUS399 Masteroppgave

Det juridiske fakultet

UNIVERSITETET I BERGEN

10. desember 2021

Innholdsfortegnelse

Innholdsfortegnelse 1
1 Innledning 3
1.1 Tema og problemstilling 3
1.2 Temaets historikk og aktualitet 5
1.3 Rettskildebildet og dets særegenheter 6
1.3.1 Gjennomføring av Personvernforordningen i norsk rett 8
1.4 Videre fremstilling 9
2 Overføring av personopplysninger fra Europa til USA 10
2.1 Hovedregler og utgangspunkt for overføring av personopplysninger til en tredjestat 10
2.2 Hva er en "overføring" av personopplysning? 12
2.3 Schrems II C-311/18 14
2.4 Spenningsforholdet mellom europeisk og amerikansk personvernrett 16
3 Bruk av standardkontraktsbestemmelser som overføringsgrunnlag 19
3.1 Personvernforordningen artikkel 46 (2) (c) 19
3.1.1 Standardkontraktsbestemmelsene 21
3.1.2 Personvernrådets vurdering i seks steg 24
3.2 Betydningen av Personvernforordningens geografiske anvendelsesområde for bruk av de nye standardkontraktsbestemmelsene 26
3.2.1 EU-kommisjonens syn - kommet til uttrykk i standardkontraktsbestemmelsene 28
3.2.2 Et meget begrenset anvendelsesområde? 33
4 Er det rom for en risikobasert tilnærming ved vurderingen av adgang til overføring av personopplysninger til tredjestater? 35
4.1 EU-domstolens syn på en risikobasert tilnærming 36
4.2 Personvernrådets syn på en risikobasert tilnærming 38
4.3 EU-kommisjonens syn på en risikobasert tilnærming 42
4.4 I hvor stor grad kan en risikobasert tilnærming benyttes? 44
4.5 Mulige konsekvenser av en for streng praktisering 46
5 Avslutning 48
5.1 Er det praktisk mulig å anvende standardkontraktsbestemmelsene som overføringsgrunnlag ved overføring til USA? 48

5.2 Behov for en politisk løsning 50
6 Litteraturliste 53
6.1 Litteratur 53
6.1.1 Bøker 53
6.1.2 Artikler 54
6.1.3 Nettsider 54
6.1.4 Rapporter og offisielle uttalelser 57
6.2 Norske rettskilder 58
6.2.1 Lovgivning 58
6.2.2 Lovforarbeider 58
6.2.3 Domsregister 58
6.2.4 Offentlige dokumenter 58
6.3 Internasjonale rettskilder 59
6.3.1 Traktater 59
6.3.2 EU-direktiver, forordninger m.m. 59
6.3.3 Implementeringsbestemmelser 60
6.3.4 Veiledere, utkast m.m. 60
6.3.5 Internasjonalt domsregister 62
6.4 Utenlandske (nasjonale) rettskilder 63
6.4.1 Amerikansk lovgivning 63
6.4.2 Amerikansk domsregister 63

1 Innledning

1.1 Tema og problemstilling

Det er ingen tvil om at man i 2021 lever under en digital revolusjon hvor individers personopplysninger utgjør en verdifull valuta.[1] Til dette er det mange årsaker, herunder målet om målrettet markedsføring, samt å utvikle konkurransedyktige løsninger.[2] Dette er, sammen med forståelsen av at retten til privatliv over sine personopplysninger er en grunnleggende menneskerettighet, grunnen til at man gjennom EUs forordning 2016/679, heretter Personvernforordningen, har forsøkt å regulere den digitale økonomien i et voksende digitalt samfunn.[3] Overordnet kan man si at regelverket er bygget på to hovedpilarer; at virksomhetene pålegges et større ansvar samtidig som borgerne sikres sterkere rettigheter.[4] En av hovedoppgavene til Personvernforordningen er å verne fysiske personers grunnleggende rettigheter og friheter ved behandling av personopplysninger, uavhengig av hvor behandlingsaktiviteten finner sted.

Personvernforordningen skaper en trygg sfære i de stater som har implementert forordningen, ved at individene er sikret et gitt beskyttelsesnivå for sine personopplysninger. Det er imidlertid et voksende behov for å overføre personopplysninger til stater som ikke sikrer et tilnærmet likt beskyttelsesnivå for personopplysninger, hvilket i det videre omtales som tredjestater.[5] Som følge av at slike land i stor grad står bak den teknologiske utvikling, innehar også selskaper i slike tredjestater eierrettigheter til de mest brukervennlige og økonomisk fordelaktige tekniske løsningene.[6]

Land som ikke har et regelverk som sikrer individene et tilnærmet likt beskyttelsesnivå, utgjør en trussel mot det vern Personvernforordningen sikrer.[7] Personvernforordningen har av den grunn bestemmelser som skal beskytte individene mot trusler fra slike stater. Hovedmekanismene er Personvernforordningens regler om dens geografiske virkeområde i artikkel 3, hvilket omhandler vilkårene for anvendelsen av Personvernforordningen som

[1] Meld. St. 23 (2012-2013) pkt. 1.1 En agenda for den digitale revolusjonen
[2] Archick, Kristin, Fefer, Rachel (2021) s. 5
[3] Prop. 56 LS (2017-2018) s. 9
[4] Skullerud mfl. (2019) s. 9
[5] Personvernforordningen fortalepunkt 101
[6] Hill, Derek (2014) kapittel 6
[7] Kuner, Christopher (2021) s. 3

sådan, og overføringsreglene i kapittel V, hvilket regulerer situasjonen hvor personopplysningene overføres til en tredjestat.[8] Det er særlig reglene i kapittel V om overføring og overføringsgrunnlag som skal behandles nærmere i denne oppgaven.

Hva gjelder USA, så vedtok EU-kommisjonen i 2016 et slikt overføringsgrunnlag i form av et rammeverk. Rammeverket ble omtalt som The EU – U.S. Privacy Shield.[9] Enkelte stilte spørsmålstegn ved hvorvidt dette overføringsgrunnlaget sikret et tilstrekkelig vern i praksis, hvilket førte til at EU-domstolen sommeren 2020 behandlet en sak knyttet til gyldigheten av rammeverket.[10] Sak C-311/18, Schrems II-avgjørelsen, ugyldiggjør Privacy Shield som et overføringsgrunnlag. Bakgrunnen for hvorfor overføringsgrunnlaget ble kjent ugyldig av EU-domstolen, behandles nærmere i oppgavens kapittel 2.3.

Det faktum at USA er et av de ledende landene i den teknologiske utviklingen, fører til at en overvekt av europeiske virksomheter benytter seg av amerikanske tjenesteleverandører. Microsoft teams eller Outlook kan her trekkes frem som eksempel.[11] I tråd med Personvernforordningens kapittel V, vil virksomhetene i slike situasjoner kunne ha behov for et overføringsgrunnlag. Standardkontraktsbestemmelsene ble fremhevet av EU-domstolen i Schrems II-saken som et nærliggende overføringsgrunnlag,[12] og av den grunn vil særlig standardkontraktenes funksjon som overføringsgrunnlag vurderes nærmere i denne oppgave.

Temaet for oppgaven er de praktiske konsekvensene spenningsforholdet mellom europeisk og amerikansk personvernrett har for overholdelsen av Personvernforordningen, hvorav hovedproblemstillingen er:

> I hvilken utstrekning kan virksomheter hensynta den faktiske risikoen for å bli utsatt for offentligrettslige innsynsbegjæringer ved vurderingen av om tredjestaten sikrer et tilstrekkelig beskyttelsesnivå ved bruk av standardkontraktsbestemmelser som overføringsgrunnlag?

[8] Kuner, Christopher (2021) s. 3-4
[9] EU-U.S. Privacy Shield C/2016/4176
[10] C-311/18 *Facebook Ireland and Schrems*
[11] Case, John (2020)
[12] C-311/18 *Facebook Ireland and Schrems* avsnitt 149

1.2 Temaets historikk og aktualitet

Ettersom USA er ledende både på feltene for teknologisk utvikling og etterretningstjeneste, har det i lang tid eksistert en debatt knyttet til hvordan en trygt skal kunne overføre personopplysninger fra EU/EØS til USA.[13] Dette fører til at det eksisterer et selvsagt behov og ønske om å lovlig kunne overføre personopplysninger hit ved bruk av slike løsninger. Debatten ble ytterligere forsterket som følge av Snowden-avsløringene i 2013, hvilket ga allmennheten holdepunkter for at metodene benyttet av amerikansk etterretningstjeneste var i strid med retten til privatliv.[14]

I den forbindelse er det verdt å merke at det står to nokså viktige hensyn mot hverandre i denne vurderingen, nemlig hensynet til at en skal få utfolde seg uten innblanding fra myndighetene med mindre utfoldelsen er egnet til å være til skade eller fare for andre eller samfunnet, og bekjempelse av terror og alvorlig kriminalitet. Retten til vern av privatlivet er ingen absolutt rettighet, slik at det kan eksistere grunnlag for å gjøre inngrep i rettigheten som følge av andre, mer tungtveiende hensyn, som for eksempel bekjempelse av terror.[15] Utfordringen med amerikansk rett kan overordnet sies å knytte seg til kontrollmekanismene og mulighetene for individene til å prøve grunnlaget for inngrepet, eller mangelen på sådanne. Oppgaven vil berøre dette noe nærmere nedenfor.

Personvernforordningen er som følge av dens ekstraterritorielle virkning egnet til å påvirke både utviklingshastighet, kostnader og forretningsmodeller. Disse forholdene er egnet til å være av avgjørende betydning for en virksomhets suksess i det indre marked.[16] Med ekstraterritorielt virkeområde menes at Personvernforordningen må overholdes av behandlingsansvarlige/databehandlere lokalisert utenfor EU/EØS dersom deres virksomhet relaterer seg til tilbud av varer og tjenester eller overvåking av adferden til registrerte i EU/EØS.[17] For europeiske virksomheter bør overholdelse av disse pliktene være av nokså stor betydning ved valg av samarbeidspartnere lokalisert utenfor EU/EØS.

[13] Archich, Kristin, Fefer, Rachel (2021) s. 2
[14] Foss, Kristian (2021) s. 18
[15] Aall, Jørgen (2018) s. 115
[16] Foss, Kristian (2021) s. 17
[17] Personvernforordningen artikkel 3(2)

Er det tale om en overføring til tredjestater, er det ikke tilstrekkelig at dataimportøren i kraft av Personvernforordningens ekstraterritorielle virkeområde er forpliktet til å overholde Personvernforordningen. Ved overføring må en foreta en konkret vurdering av tredjestatens faktiske beskyttelsesnivå.[18] Vurderingen skal basere seg på om det eksisterer forhold ved dataimportørens nasjonale rett som er egnet til å krenke datasubjektenes grunnleggende rettigheter og friheter. I visse tilfeller kan det være nødvendig å iverksette særskilte beskyttelsestiltak for å oppnå ønsket beskyttelsesnivå.[19] Hvilke beskyttelsestiltak som vil være nødvendige i det enkelte tilfellet, beror på en konkret vurdering.

Selv om EU-domstolen gjennom Schrems II-saken ugyldiggjorde det mest benyttede overføringsgrunnlaget for europeiske virksomheter som ønsket å overføre personopplysninger til USA, så eksisterer det fremdeles et behov for å kunne benytte seg av amerikanske tjenesteleverandører. Standardkontraktsbestemmelsene ble fremhevet av EU-domstolen i Schrems II-saken som et nærliggende overføringsgrunnlag.[20] I hvilken utstrekning disse bestemmelsene kan anvendes som overføringsgrunnlag, er fremdeles et usikkert element.

1.3 Rettskildebildet og dets særegenheter

På bakgrunn av EØS-samarbeidet, har Norge implementert Personvernforordningen. Implementering av en forordning i sin helhet, skal sørge for en enhetlig rettstilstand innad i EU/EØS.[21] Utgangspunktet for fortolkningen er ordlyden, med mindre det ikke finnes legaldefinisjoner.[22] For å forhindre variasjoner i tolkningsresultatet basert på ulikheter i de 23 offisielle versjonene av samme rettsakt, skal en i EU-retten foreta en kontekstuell og formålsorientert tolking.[23]

Personvernforordningen erstatter EUs personverndirektiv fra 1995.[24] En stor forskjell mellom regelverkene, er at Personvernforordningen i stor grad legger opp til vurderinger basert på reell risiko.[25] Blant annet er det den behandlingsansvarliges risikovurderinger som er utgangspunktet for vurderingen av hvorvidt Personvernforordningen er overholdt, og da med

[18] Recommendations 01/2020 vol. 2.0 avsnitt 30
[19] C-311/18 *Facebook Ireland and Schrems* avsnitt 133
[20] C-311/18 *Facebook Ireland and Schrems* avsnitt 149
[21] TEU art. 4 (3)
[22] Arnesen, Finn, Stenvik, Are. (2015) s. 26
[23] Rt-2005-833 avsnitt 45
[24] Direktiv 95/46 EC, heretter "personverndirektivet"
[25] Gonçalves, Maria Eduarda (2020) fotnote 7

tilhørende ansvar for en eventuell uriktig risikovurdering.[26] Hvorvidt også reglene om overføring til tredjestater åpner for å benytte risiko som et moment i vurderingen av tredjestatens beskyttelsesnivå, analyseres nærmere i oppgaven.

Oppgavens problemstilling, og dens løsning, beror i stor grad på uttalelser i en avgjørelse fra EU-domstolen.[27] I Schrems II-saken, tolker EU-domstolen Personvernforordningen i lys av Den europeiske unions Charter om grunnleggende rettigheter.[28] Videre benyttes også bestemmelser i Traktaten om Den europeiske unions virkeområde (TEUV) ved fortolkningen av Personvernforordningen. Det følger av TEUV artikkel 267 at EU-statene har rett til å be EU-domstolen komme med forhåndsuttalelse på forespørsel fra EU-statene i en konkret sak. Schems II-avgjørelsen er en slik forhåndsuttalelse.[29]

Ettersom Norge er en EFTA-stat, vil ikke en slik forhåndsuttalelse være direkte bindende. Imidlertid følger det av homogenitetsmålsettingen som kommer til uttrykk i EØS-avtalen artikkel 6, at argumenter lagt til grunn i EU-domstolens praksis er "relevante og tungtveiende argumenter også ved løsningen av de tolkningsspørsmål som EØS-avtalen gir grunnlag for".[30] På denne bakgrunn plikter Norge å forholde seg til Schrems II-avgjørelsen ved praktiseringen av Personvernforordningen. I tråd med avgjørelsen, og uttalelser fra Datatilsynet, skal norske virksomheter også hensynta det europeiske charteret ved praktiseringen av Personvernforordningen. [31]

En annen rettskilde som preger oppgaven, er retningslinjer/anbefalinger utstedt av Personvernrådet. Personvernrådet har til hovedoppgave å sikre ensartet praktisering av Personvernforordningen i det indre marked, og søker å utføre denne oppgaven ved blant annet å utforme slike dokumenter for praktiseringen av enkelte deler av Personvernforordningen.[32] Slike retningslinjer/anbefalinger er ikke direkte rettslig bindende for virksomheter. Derimot er nasjonale tilsynsmyndigheter, i Norge Datatilsynet, forpliktet til å hensynta retningslinjene i vurderingen av overholdelsen av Personvernforordningen. Dermed gis retningslinjene en indirekte effekt ved at de også må overholdes av behandlingsansvarlige for at de skal opptre i

[26] Personvernforordningen artikkel 83
[27] C-311/18 *Facebook Ireland and Schrems*
[28] C-311/18 *Facebook Ireland and Schrems*, se blant annet avsnitt 1, 97-99 og 122
[29] C-311/18 *Facebook Ireland and Schrems*, se avsnitt 117
[30] Sejersted mfl. (2014) s. 237, med videre henvisning til sak E-2/94, SSGA; ODA-avtalen artikkel 3
[31] Datatilsynet (2021) s. 10
[32] Datatilsynet (2020) "Det europeiske Personvernrådet (EDPB)" under pkt. "Hva gjør Personvernrådet?"

tråd med Personvernforordningen.[33] Når det er få rettskilder på området, vil kilder som er utarbeidet av et råd med faglig kompetanse ende opp med å få betydning, gjerne i form av "best practice".[34]

1.3.1 Gjennomføring av Personvernforordningen i norsk rett

Lov om behandling av personopplysninger (personopplysningsloven) av 20. desember 2018 § 1 gjennomfører Personvernforordningen i norsk rett ved inkorporasjon, hvilket innebærer at forordningen er blitt gjort til del av den norske retten uten vesentlige endringer.[35] De tilpasninger som er blitt gjort i nasjonal rett, følger av tilpasningsteksten.[36] Dette skyldes at EØS-avtalen artikkel 7 (1)(b) fastsetter at forordninger "som sådan" skal gjøres til en del av avtalepartenes interne rettsorden.

Ved å etablere lovgivning i form av en forordning, bidrar man i større grad til en harmonisert regulering og etterlevelse i hele EØS-området.[37] En ønsker å sikre at virksomheter som behandler personopplysninger har like regler å forholde seg til, uavhengig av hvor behandlingen geografisk finner sted. Videre skal borgerne nyte samme vern innad i EØS-området. Overordnet vil dette bidra til økt handel på tvers av landegrensene i tråd med EØS-samarbeidets overordnede mål.[38] Selv om det er tale om en forordning, er de nasjonale statene erkjent et visst handlingsrom i implementeringsarbeidet.

Som følge av målet om en harmonisert rettstilstand, har den enkelte medlemsstat kun i begrenset grad mulighet til å fravike eller særregulere områder som omfattes av forordningen. Viser det seg at særreguleringen strider mot Personvernforordningen, vil den nasjonale reguleringen være ugyldig.[39]

[33] Judin, Thomas (2021) under pkt. "Europeisk enhet"
[34] Fredriksen Halvard, Mathisen, Gjemund (2014) s. 230
[35] Sejersted mfl. (2014) s. 237; det følger av praksis fra EFTA-domstolen at EØS-avtalen, og dens vedlegg, ikke er gjeldende i norsk rett uten nasjonal gjennomføring, se sak E-4/01 Karlsson
[36] Skullerud mfl. (2019) s. 49
[37] Fredriksen, Halvard, Mathisen, Gjermund (2014) s. 279
[38] Regjeringen (2021) pkt. "Felles regler – like konkurransevilkår"
[39] EØS-avtalen § 2

1.4 Videre fremstilling

Oppgaven består av fem deler. Kapittel 2 gjelder ulike aspekter knyttet til overføring av personopplysninger til tredjestater og en gjennomgang av Schrems II-saken.

Kapittel 3 omhandler bruk av Standardkontraktsbestemmelser vedtatt av EU-kommisjonen etter Personvernforordningen artikkel 46 (2)(c) som overføringsgrunnlag ved overføring til tredjestater, og da særlig USA. Oppgaven vil også se nærmere på forholdet mellom Personvernforordningens ekstraterritorielle virkeområde og bruk av EU-kommisjonens standardkontraktsbestemmelser.

Under kapittel 4 skal oppgaven se nærmere på spørsmålet knyttet til i hvor stor grad virksomheter kan hensynta den faktiske risikoen for å bli utsatt for innsynsbegjæringer ved vurderingen av beskyttelsesnivået i tredjestaten. Kapittelet vil også se nærmere hvor stort dette rommet eventuelt vil være.

Oppgavens kapittel 5 vil konkludere på spørsmålet om hvorvidt det er praktisk mulig for europeiske virksomheter å basere seg på standardkontraktsbestemmelser ved overføring av personopplysninger til USA. Kapittelet vil også ta for seg hvilke muligheter som kan eksistere på det politiske plan.

2 Overføring av personopplysninger fra Europa til USA

2.1 Hovedregler og utgangspunkt for overføring av personopplysninger til en tredjestat

Personvernforordningen har til formål å sikre et likt beskyttelsesnivå for behandling av personopplysninger i EU/EØS, altså en trygg sfære. Av hensyn til at man ønsker at rettighetssubjektene er sikret det samme vernet også i de situasjoner hvor behandling finner sted utenfor EU/EØS, har forordningen særlige regler knyttet til slike situasjoner. Artikkel 44 legger til grunn at personopplysninger kun kan overføres til stater utenfor EU/EØS hvis reglene i forordningens kapittel V overholdes. Utgangspunktet har til formål å forhindre at det felleseuropeiske beskyttelsesnivået undergraves ved bruk av tjenesteleverandører fra tredjestater.[40]

Et absolutt forbud vil ikke være hensiktsmessig ettersom de største tjenesteleverandørene er lokalisert utenfor EU/EØS. Fortalepunkt 101 fremhever at

> "Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation".

Artikkel 44 oppstiller videre et krav om at overføring kun kan finne sted dersom den behandlingsansvarlige kan påse at de øvrige bestemmelsene i forordningen overholdes. Behandlingen må blant annet, men ikke begrenset til, være i tråd med de generelle personvernprinsippene i artikkel 5, samt at behandlingen må ha et lovlig behandlingsgrunnlag etter artikkel 6 og eventuelt også etter artikkel 9 hvor det er tale om særlige kategorier av personopplysninger.[41] Kravet om behandlingsgrunnlag kommer i tillegg til kravet om at virksomheten må kunne påvise et overføringsgrunnlag i kapittel V.

[40] Skullerud mfl. (2019) s. 367
[41] Guidelines 2/2020 avsnitt 5

Artikkel 5 i Personvernforordningen inneholder de grunnleggende prinsippene for behandling av personopplysninger og fungerer særlig som tolkningselementer ved tolkning av de øvrige bestemmelsene i forordningen.[42] Prinsippene kan overordnet oppsummeres på følgende måte; behandlingen må skje på en lovlig, rettferdig og åpen måte, behandlingen må være begrenset til det formål det er samlet inn for, opplysningene må være korrekte og kun lagres i det omfang som er nødvendig, samt behandles på en måte som sikrer dens integritet og konfidensialitet. I tråd med artikkel 24 plikter den behandlingsansvarlige å dokumentere at disse prinsippene er overholdt. Disse prinsippene vil følgelig ligge til grunn for hvordan en kan fortolke reglene knyttet til overføring av personopplysninger til tredjestater.[43]

Av andre generelle bestemmelser i forordningen, er særlig artikkel 6 nærliggende å trekke frem. Her fremgår det at den behandlingsansvarlige må påvise et lovlig behandlingsgrunnlag for den aktuelle behandling. Dersom det er tale om behandling av særlige kategorier av personopplysninger, må den behandlingsansvarlige i tillegg kunne påvise et behandlingsgrunnlag i artikkel 9. Behandlingsgrunnlaget må foreligge på tidspunktet for innsamlingen, og det er som utgangspunkt ikke anledning for å endre behandlingsformål underveis.[44]

Overføring av personopplysninger til tredjestater reguleres i Personvernforordningen kapittel V. I tråd med artikkel 44, må en kunne påvise et overføringsgrunnlag. Et mulig rettsgrunnlag for overføring er en såkalt "adekvansbeslutning" hvor EU-kommisjonen har funnet at det aktuelle land eller internasjonale organisasjon har et tilstrekkelig beskyttelsesnivå.[45]. EU-kommisjonen har kompetanse til å godkjenne tredjestater som trygge mottakerstater. Videre har EU-domstolen kommet frem til at overføring til tredjestater kan anses legitime gjennom en internasjonal avtale, hvilket var tilfellet for Privacy Shield-rammeverket.[46] Kan en påvise at de alminnelige vilkårene for å behandle personopplysninger er oppfylt og det foreligger en slik beslutning, kan virksomheten trygt overføre personopplysningene til den aktuelle tredjestat.

[42] Skullerud mfl. (2019) s. 172
[43] Skullerud mfl. (2019) s. 171
[44] Skullerud mfl. (2019) s. 185
[45] Se artikkel 45
[46] Kuner, Christopher (2020) s. 775 fotnote 6

En rekke andre overføringsgrunnlag fremgår av artikkel 46. Etter artikkel 46 kan man foreta en overføring til en tredjestat hvor dataimportør har gitt de nødvendige garantier om overholdelse av Personvernforordningen gjennom et rettslig bindende instrument, jf. Annet ledd bokstav a, bindende virksomhetsregler, jf. Annet ledd bokstav b, EU-kommisjonens standardkontraktsbestemmelser, jf. Annet ledd bokstav c, nasjonalt vedtatte standardkontraktsbestemmelser, jf. Annet ledd bokstav d eller adferdsnormer eller sertifiseringsmekanismer, jf. Annet ledd bokstav e og f. Artikkel 49 inneholder særlig unntaksregler som kan komme til anvendelse ved sporadiske overføringer knyttet til et begrenset antall registrerte og er tvingende nødvendig.

Oppgaven har ikke rom for å behandle ytterligere hva som omfattes av de ulike overføringsgrunnlagene. Bruk av standardkontraktsbestemmelser vedtatt av EU-kommisjonen vil behandles nærmere under pkt. 3 og 4 hvor man ser nærmere på hva som må til for at dette skal utgjøre et lovlig og praktisk relevant overføringsgrunnlag i relasjon til USA.

2.2 Hva er en “overføring” av personopplysning?

I relasjon til denne oppgaven, er det nærliggende å se nærmere på hva som ligger i begrepet "overføring". Personvernforordningen definerer ikke begrepet selv. På denne bakgrunn vil en måtte undersøke ytterligere kilder, herunder ordlyden, for å komme frem til hva som er ment å omfattes av begrepet "overføring".

Ordlyden av vilkåret «overføring» kan tilsi at personopplysningene fysisk må sendes til en tredjestat, f.eks. via fildeling. Det må finne sted en form for forflytning av personopplysninger. Det er rimelig å anta at en slik fortolkning er for snever, sett ut fra formålet til overføringsreglene. Formålet om at de registrerte skal sikres et tilstrekkelig beskyttelsesnivå også i tredjestater, kan tilsi at vilkåret må forstås såpass bredt at fortolkningen ikke blir en bidragsyter til at de registrertes vern blir utvannet.[47] Dette taler for at vilkåret må forstås vidt.

[47] Kuner, Christopher, (2020) s. 762

EUs datatilsynsmyndighet anser begrepet "overføring" for å omfatte data som er «move[d] or allowed to move between different users».[48] Det europeiske tilsynsorganet uttalte dette i forbindelse med høringsutkastet til personvernforordningen, og etterspurte i samme omgang en legaldefinisjon av begrepet.[49]

Det er begrenset med rettspraksis fra EU-domstolen relatert til hva som ligger i begrepet «overføring». Fra det tidligere Personverndirektivet er spørsmålet drøftet i relasjon til artikkel 25 i Lindqvist-saken C-101/01. Fra nyere tid, har vi Schrems I-saken C-362/14, også vurdert på bakgrunn av Personverndirektivet. Begge saken belyses nedenfor.

Bodil Lindquist-saken omhandlet et aktivt kirkemedlem i Sverige. Hun hadde opprettet en nettside hvor hun hadde publisert personlig informasjon om de øvrige medlemmene av menigheten, herunder navn, telefonnummer og helseopplysninger. Nettsiden var opprettet i forbindelse med et datakurs hun hadde deltatt på. Hun ble av det svenske datatilsynet bøtelagt for manglende overholdelse av personverndirektivet, men anket beslutningen inn for EU-domstolen.[50]

EU-domstolen fant at det å plassere informasjon på en server lokalisert i EU/EØS, men som var tilgjengelig fra hele verden gjennom internett, ikke utgjorde en overføring. Dette skyldes at informasjonen ikke ble sendt automatisk fra serveren til andre internettbrukere, men det fordret en aktiv handling å få tilgang til informasjonen.[51] Informasjonen ble overført via infrastrukturen til hostingleverandøren hvor informasjonen ble lagret på dens servere. EU-domstolen oppstiller ved beslutningen et aktivitetskrav for å kategorisere noe som en overføring.

EU-domstolen forandrer noe retning i den senere Schrems I-saken.[52] Spørsmålet i saken knyttet seg til lovligheten av overføringsgrunnlaget Safe Harbour, forgjengeren til EU-U.S. Privacy Shield. Avgjørelsen illustrerer at det er behov for en høy grad av beskyttelse dersom data skal føres ut av EU/EØS. EU-domstolen legger i avgjørelsen til grunn at det ikke kreves en fastsatt definisjon av begrepet, ettersom vilkåret er ment å omfatte alle situasjoner hvor en risikerer at beskyttelsesnivået til de registrerte blir skadelidende. Dette tilsier at både faktisk overføring og tilgjengeliggjøring omfattes av vilkåret.

[48] Skullerud mfl. (2019) s. 367
[49] Det europeiske datatilsynet (2012) avsnitt 108, med videre henvisning til Lindqvist-saken C-101/01
[50] C-101/01 *Lindqvist* avsnitt 18
[51] C-101/01 *Lindqvist* avsnitt 60-61
[52] C-362/14 *Schrems* avsnitt 73

Datatilsynet initierer at vilkåret må fortolkes bredt. De uttaler at med en overføring så menes i tillegg til at personopplysninger sendes til noen utenfor EU/EØS, at "begrepet omfatter tilfeller hvor noen utenfor EØS får tilgang til personopplysninger lagret i EØS".[53] Dette med fjerntilgang er særlig aktuelt i europeiske virksomheter, ettersom det må antas å være nokså vanlig å ha supportsystemer lokalisert utenfor Europa. Følgelig vil situasjonen hvor man har supportsystemer i tredjestater aktualisere reglene om overføring hvis personopplysninger blir behandlet i denne relasjonen.

Gjennomgangen over viser at begrepet "overføring skal forstås meget vist, slik at enhver befatning eller tilgjengeliggjøring av persondata i tredjestater omfattes. Bakgrunnen for at begrepet må erkjennes en så vidt fortolkning er fordi det er tale om beskyttelse av individers grunnleggende menneskerettigheter, nemlig retten til privatliv. Skal Personvernforordningen sikre en reell beskyttelse, må forordningens bestemmelser, og særlig hvilke handlinger som skal kategoriseres som en "overføring", forstås såpass vidt at det ikke er anledning til å bevisst omgå regelverket.

Personvernrådet fremmet 19. november 2021 forslag om retningslinjer angående forholdet mellom artikkel 3 og kapittel V, hvor man har inntatt en definisjon av begrepet "overføring". Høringsfristen utgår 31. januar. Som følge av at retningslinjene ikke er vedtatt, vil de i begrenset grad bli behandlet nærmere. Det bemerkes at Personvernrådet i de foreslåtte retningslinjene legger til grunn at reglene om overføring skal overholdes uavhengig av om dataimportøren faller inn under Personvernforordningens geografiske område etter artikkel 3.[54]

2.3 Schrems II C-311/18

Schrems II-saken oppsto som følge av at Maximilian Schrems, en østerriksk personvernaktivist, klaget det irske datterselskapet til Facebook Inc, Facebook ltd., inn for den irske domstolen med påstand om at Facebook ltd. ulovlig overførte hans personopplysninger til morselskapet i USA. Etter henvendelse fra den irske domstolen, tok EU-domstolen stilling til gyldigheten av adekvansbeslutningen for USA, bedre kjent som EU-U.S. Privacy Shield-rammeverket.[55]

[53] Datatilsynet (2020) "Overføring av personopplysninger ut av EØS" under pkt. "Hva er en overføring?"
[54] Personvernrådet Guidelines 05/2021 s. 4
[55] C-311/18 *Facebook Ireland and Schrems*

Gjennom rammeverket kunne amerikanske virksomheter kontraktsrettslig garantere for at de overholdt syv sentrale personvernprinsipper, i tillegg til 16 valgfrie prinsipper.[56] Rammeverket hadde til formål å bevise at virksomhetene som hadde sertifisert seg, sikret et beskyttelsesnivå tilsvarende det som følger av Personvernforordningen. Imidlertid åpner amerikansk lovgivning for at myndighetene i stor grad kan gis tilgang til personopplysninger tilknyttet individer fra EU/EØS. Dette førte til at EU-domstolen fant Privacy Shield ugyldig.[57] De amerikanske etterretningshjemlene ble ansett for å være i strid med kravet til proporsjonalitet og nødvendighet som følger av EU-retten.[58]

Standardkontraktsbestemmelsene ble ikke ugyldiggjort som overføringsgrunnlag i Schrems II-saken. Ved bruk av standardkontraktsbestemmelsene vedtatt av EU-kommisjonen, søker virksomheten å oppnå en bekreftelse på at datasubjektene er sikret et tilstrekkelig beskyttelsesnivå, selv om behandlingsaktiviteten finner sted utenfor EU/EØS. Det er beskyttelsesnivået i praksis som er avgjørende for hvorvidt overføring lovlig kan finne sted.[59] Bakgrunnen for dette er at standardkontraktsbestemmelsene kun er en privatrettslig avtale inngått mellom dataeksportør og dataimportør. Avtalen vil måtte vike for tredjestatens alminnelige lovgivning ved motstrid.

Konsekvensen av at det er tale om kontraktsrettslige forpliktelser, vil være at det i visse situasjoner vil være behov for å iverksette særlige tiltak i den hensikt å sikre et tilstrekkelig beskyttelsesnivå i praksis.[60] Dette ble også fremhevet i Schrems II-saken på generelt grunnlag, hvilket innebærer at utgangspunktet om særlige tiltak gjelder for alle overføringer basert på et overføringsgrunnlag i artikkel 46.[61] Datatilsynet støtter den forståelse at krav om tilleggstiltak gjelder ved bruk av andre overføringsgrunnlag i artikkel 46 (2) utover standardkontraktsbestemmelsene.[62] Implementeringen av tilleggstiltakene må finne sted før overføringen har skjedd for at beskyttelsesnivået skal anses sikret.

Privacy Shield var en privatrettslig ordning som innebar at sertifiserte virksomheter ble ansett for å sikre et tilstrekkelig beskyttelsesnivå i tråd med Personvernforordningen artikkel 45.

[56] Fefer, Rachel, Archick, Kristin (2021) pkt. Privacy Shield Framework
[57] C-311/18 *Facebook Ireland and Schrems* avsnitt 156 og 201
[58] Sak C-11/70 *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel*
[59] C-311/18 *Facebook Ireland and Schrems* avsnitt 126
[60] C-311/18 *Facebook Ireland and Schrems* avsnitt 133
[61] C-311/18 *Facebook Ireland and Schrems* avsnitt 96
[62] Datatilsynet (2021) s. 10

Gjennomgangen foretatt av EU-domstolen i Schrems II-saken viste imidlertid at visse deler av amerikansk lovgivning ikke var i samsvar med de EU-rettslige kravene til proporsjonalitet, hvilket er lovmessige krav en ikke kan avtale seg vekk fra.[63] Det var særlig Foreign Intelligence Surveillance Act (FISA) Section 702 og Executive Order (E.O.) 12333 som førte til at Privacy Shield ble kjent ugyldig.

Med hjemmel i FISA 702 kan amerikanske virksomheter motta innsynsbegjæringer knyttet til bestemte personer fra amerikanske myndigheter. EU-domstolen anså denne lovgivningen som problematisk som følge av manglende kontrollmekanismer hva gjelder etterretningens målrettede informasjonsinnhenting på individnivå.[64] Hva gjelder bulklagring av data som sendes til USA, så gir E.O. 12333 hjemmel til slik innsamling uten rettslig prøving. I den relasjon ble det ansett problematisk att myndighetens tilgang til dataene ikke var i tilstrekkelig grad klart avgrenset.

2.4 Spenningsforholdet mellom europeisk og amerikansk personvernrett

Som Schrems II-saken viser, eksisterer det et spenningsforhold mellom europeisk og amerikansk personvernrett. Spenningsforholdet fordrer en særlig aktsomhet fra virksomheter som ønsker å benytte seg av amerikanske tjenesteleverandører i sin daglige virksomhet. Behovet for denne aktsomheten skyldes det faktum at EU-domstolen fant at amerikansk etterretningslovgivning er for inngripende overfor europeiske borgeres rett til privatliv.[65] For å kunne vurdere hvorvidt overføring til USA vil være problematisk, finner jeg det hensiktsmessig å undersøke spenningsforholdet mellom europeisk og amerikansk rett noe nærmere.

Personvernet nyter et sterkt vern i Europa, og det er tale om et unisont vern en har i kraft av å være menneske. Den grunnleggende menneskerettigheten er lovfestet i EMK artikkel 8 om retten til privatliv. Utgangspunktet er at individene har rett til en privat sfære uten innblanding fra andre individ eller myndigheter, forutsatt at man ikke er til skade for andre individ eller samfunnet.[66] Den europeiske menneskerettighetskonvensjon oppstiller relativt strenge krav

[63] C-311/18 *Facebook Ireland and Schrems* avsnitt 126
[64] C-311/18 *Facebook Ireland and Schrems* avsnitt 184
[65] C-311/18 *Facebook Ireland and Schrems* avsnitt 199
[66] Aall, Jørgen (2018) s. 214-215

for at et inngrep i retten til privatliv skal anses legitimt. Man må kunne påvise en lovhjemmel som gjør slikt inngrep lovlig.[67] Amerikansk lovgivning har et totalt motsatt utgangspunkt, ettersom de anser at inngrep i privatlivet er greit, såfremt man ikke har en hjemmel som gjør slikt inngrep ulovlig.[68]

I motsetning til europeisk lovgivning, skiller amerikansk rett mellom beskyttelsen av personopplysninger tilknyttet amerikanske personer og andre. Retten til personvern faller etter amerikansk rettspraksis inn under første, tredje, fjerde og femte grunnlovstillegg.[69] Rettighetene som følger av disse tilleggene, kan imidlertid ikke gjøres gjeldende av personer uten varig tilknytning til USA. Europeiske borgere har således ikke de samme, og nødvendige, virkemidlene for å kunne stå imot krenkelser av deres personvern fra amerikanske myndigheter. Dette ble også bemerket av EU-domstolen som en sentral årsak til spenningsforholdet mellom europeisk og amerikansk personvernrett i Schrems II-avgjørelsen.[70]

Europeisk lovgivning går nokså detaljert til verks hva gjelder det å fastlegge konkrete rettigheter for individene, samt å pålegge virksomhetene konkrete forpliktelser for å forhindre krenkelser av individenes rettigheter. Blant annet følger det av Personvernforordningens artikkel 5 (1)(b) at de innsamlede personopplysninger kun kan benyttes for de formål de er samlet inn for. Ser man til amerikansk lovgivning, har man utformet personvernet som er forbrukerrettighet uten tydelige og håndhevbare rettigheter. I Europa kan datasubjektet kreve at behandlingen skal opphøre som følge av at virksomheten bryter med prinsippet om formålsbegrensning, jf. artikkel 17 (1)(a). En tilsvarende rettighet vil ikke individene ha etter amerikansk rett.[71] Mangelen på håndhevbare rettigheter i amerikansk rett er blant annet årsaken til at man har sett behovet for å stille krav om et særskilt overføringsgrunnlag for europeiske virksomheter som ønsker å benytte seg av amerikanske tjenesteleverandører ved behandling av personopplysninger.

[67] Rainey, Bernadette, Wicks, Elizabeth, Ovey, Clare (2017) s. 341-342
[68] Thon, Bjørn Erik (2013)
[69] U.S. Supreme Court, Jane Roe v Henry Wade 410 U.S. 133
[70] C-311/18 *Facebook Ireland and Schrems* avsnitt 65
[71] Thon, Bjørn Erik (2013)

Et sentralt element ved skillet mellom amerikansk og europeisk personvernrett knytter seg til hva som skal kategoriseres som en behandlingsaktivitet. I tråd med definisjonen av "behandling av personopplysninger" i Personvernforordningen artikkel 4 (2) skal vilkåret i prinsippet forstås såpass vidt at det omfatter enhver befatning med eller prosessering av personopplysninger.[72] Etter amerikansk rett, finnes det ingen legaldefinisjon. Det har ført til at det eksisterer forskjellige forståelser av begrepet. Forståelsen som preger amerikansk etterretningslovgivning, er at en behandling/prosessering av personopplysninger som er gjort i den hensikt å kartlegge dataenes relevans ikke er egnet til å krenke retten til privatliv, og dermed ikke har behov for det vern en såkalt "behandling" er gitt etter amerikansk rett.[73]

Konsekvensen av det ovennevnte er at europeisk og amerikansk rett er prinsipielt uenig om når en behandling er startet og følgelig når det er behov for beskyttelse av individers interesser. Dette vises ved at amerikansk etterretningsmyndighet, på bakgrunn av den overnevnte forståelsen, har myndighet til å samle inn store mengder personopplysninger uten at de er av direkte relevans for etterretningstjenesten, såkalt innsamling av rådata i bulk. Slik innsamling er klart i strid med kravet om dataminimering og formålsbegrensning som følger av Personvernforordningen.[74] Slike prinsipper er ikke lovfestet i amerikansk rett.

[72] C-101/01 *Lindqvist* avsnitt 25 til tidligere personverndirektiv artikkel 2 (b)
[73] National Academies (2015) pkt. 2.2.1
[74] Se Privacy International C-623/17 og La Quadrature du Net and Others C-511/18 om vilkårlig overføring og oppbevaring av trafikk- og lokasjonsdata

3 Bruk av standardkontraktsbestemmelser som overføringsgrunnlag

3.1 Personvernforordningen artikkel 46 (2) (c)

Personvernforordningen kapittel V fastsetter for de tilfeller hvor en virksomhet ønsker å overføre personopplysninger til en tredjestat eller internasjonale organisasjoner at en må påvise et overføringsgrunnlag for at overføringen skal anses lovlig. Dette skyldes tanken om at de fleste land utenfor EU/EØS ikke sikrer individene et tilsvarende likt beskyttelsesnivå for deres personopplysninger.[75]

Virksomheter som ønsker å foreta overføringer av personopplysninger har et relativt stort arsenal av overføringsgrunnlag etter Personvernforordningens kapittel V å velge mellom. Det er kun nødvendig å bevise overholdelse av ett grunnlag for at den aktuelle overføring skal anses lovlig. I det følgende skal oppgaven se nærmere på overføringer i medhold av Personvernforordningens artikkel 46, og da særlig artikkel 46 (2)(c) om standardkontraktsbestemmelser. Innledningsvis finner jeg det hensiktsmessig å belyse enkelte generelle aspekter ved artikkel 46. Bruk av overføringsgrunnlagene i artikkel 46 er i henhold til bestemmelsen, kun aktuelt

> "in the absence of a decision pursuant to Article 45 (3)"

Artikkel 46 innehar tittelen "Transfers subject to appropriate safeguards", på norsk oversatt til nødvendige garantier. Ordlyden tilsier at overføringsgrunnlagene skal sikre personopplysningene et tilstrekkelig vern. Grunnlagene skal:

> "kompensere for den svekkede, eller kanskje i verste fall totalt fraværende, beskyttelsen av personopplysninger som rettsordenen i den aktuelle mottakerstaten gir"[76]

[75] Skullerud mfl. (2019) s. 377
[76] Skullerud mfl. (2019) s. 377

Videre følger det av bestemmelsens første ledd at tredjestaten, for at den kan kategoriseres som en stat som sikrer individene et tilstrekkelig beskyttelsesnivå, må sørge for at datasubjektet har rettigheter som kan håndheves gjennom effektive rettsmidler. Slike rettigheter må foreligge både under og etter at overføringen er gjennomført.

Artikkel 46 (2) (c) har følgende ordlyd:

> "The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorization from a supervisory authority, by; […] standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93 (2)"

Ordlyden av "appropriate safeguards" tilsier at EU/EØS forutsetter at tredjestater har et dårligere beskyttelsesnivå av personopplysninger sammenlignet med Unionslandende, hvilket fordrer et særskilt grunnlag for at overføringen skal være lovlig.[77] En finner støtte for en slik forståelse i forordningens fortalepunkt 108 hvor det uttales at

> "In the absence of an adequacy decision, the controller or processor should take measure to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject […]"

Fortalen tilsier at virksomheten må påse at datasubjektet har tilsvarende beskyttelse som i EU/EØS for at behandling lovlig kan finne sted. Basert på Personvernforordningens system, kan uttalelsen i fortalepunktet tilsi at det eksisterer et dokumentasjonskrav for virksomhetene.

Artikkel 46 (2)(c) gir hjemmel for å benytte standardkontraktsbestemmelser utarbeidet av Europakommisjonen som overføringsgrunnlag. Disse standardkontraktsbestemmelsene er utarbeidede standarddokumenter som skal anvendes hvor man bygger på det aktuelle grunnlag. Følgelig gir bestemmelsen i seg selv kun uttrykk for de generelle kravene som en virksomhet må overholde ved overførsel av personopplysninger. Dette innebærer blant annet at virksomheten må kunne påvise at tredjestaten sikrer individene et tilstrekkelig beskyttelsesnivå. For at standardkontraktsbestemmelsene, som etter sin art er et kontraktuelt grunnlag, skal sikre et tilstrekkelig beskyttelsesnivå, kan det være nødvendig å implementere tilleggstiltak.[78] I det følgende skal oppgaven se noe nærmere på avtaledokumentet som skal

[77] Kuner, Christopher, Bygrave, Lee, Dpcksey, Christopher (2020) s. 757
[78] C-311/18 *Facebook Ireland and Schrems* avsnitt 132

benyttes dersom virksomheten ønsker å anvende standardkontraktsbestemmelsene som overføringsgrunnlag.

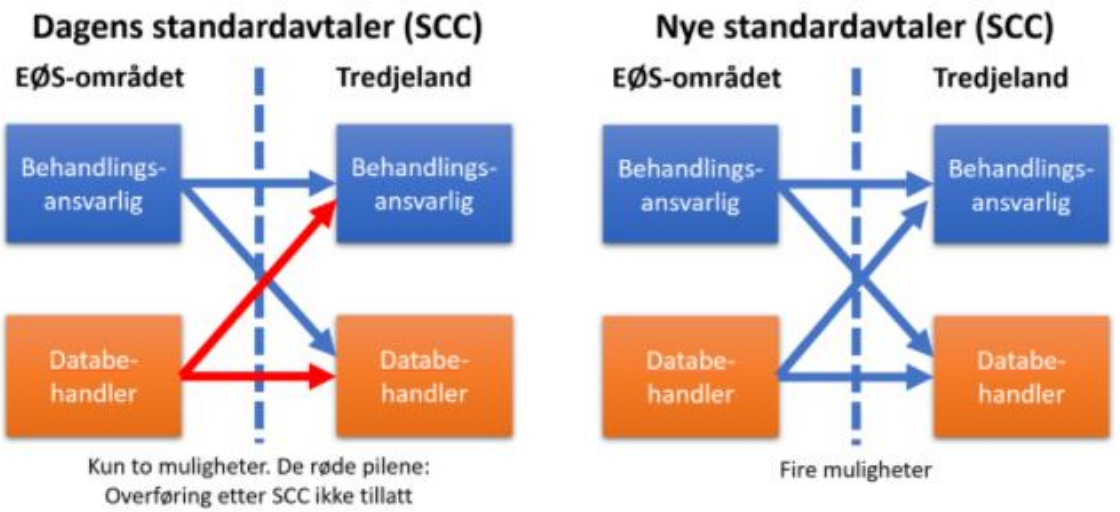
3.1.1 Standardkontraktsbestemmelsene

Standardkontraktsbestemmelser er et vel benyttet overføringsgrunnlag, og det var i tiden før avgjørelsen fra EU-domstolen falt, usikkert hvorvidt disse også ville bli opphevet av domstolen.[79] Overføring med hjemmel i standardkontraktsbestemmelsene ble ansett for å inneha en stor grad av de samme svakheter som Privacy Shield-rammeverket.[80] Bakgrunnen for dette er at standardkontraktsbestemmelsene er en avtalerettslig forpliktelse som kun er rettslig bindende for dens parter.[81] Det er ikke mulig for europeiske virksomheter å avtale seg vekk fra det faktum at amerikanske virksomhet vil kunne være underlagt lovgivning som reduserer det vern standardkontraktsbestemmelsene har til hensikt å sikre. I slike tilfeller vil standardkontraktsbestemmelsene måtte vike for lovgivningen, såfremt det er tale om ufravikelig lovgivning i tredjestaten.[82]

Schrems II-saken fordret en revisjon av de eksisterende standardkontraktsbestemmelsene, og et utkast ble sendt på høring i november 2020. Utkastet fikk bred oppslutning, hvor også Det europeiske datatilsynet og Personvernrådet kom med felles innspill.[83] EU-kommisjonen fattet beslutning om vedtakelse av nye standardkontraktsbestemmelser 4.juni 2021.[84]

De reviderte standardkontraktsbestemmelsene har tatt i bruk en modulbasert tilnærming. Modul 1 angår overføring fra behandlingsansvarlig til behandlingsansvarlig, mens Modul 2 angår overføring fra behandlingsansvarlig til databehandler. Modul 3 er en nykommer, ved at den angår overføring fra en EØS-lokalisert databehandler til en databehandler i en tredjestat, således de tradisjonelle underdatabehandleravtalene. Modul 4 regulerer overføring fra en EØS-lokalisert databehandler til en behandlingsansvarlig lokalisert i en tredjestat.

[79] Woods, Lorna (2019) under pkt. "Comment" første avsnitt
[80] C-311/18 *Facebook Ireland and Schrems* avsnitt 149
[81] Recommendations 01/2020 vol. 2.0 s. 7
[82] Boe, Erik Magnus (2010) s. 82
[83] EDPB-EDPS Joint opinion 2/2021
[84] 2021/914/EC



Illustrasjon av standardavtalene[85]

Ettersom det er tale om en felles avtale som regulerer de fire modulene, vil avtalen i større grad være preget av en "klipp ut"-funksjon. Partene må selv fjerne de deler som ikke er relevante. Dette gjør praktiseringen noe mer utfordrende, ettersom man risikerer å havne i ansvar etter Personvernforordningen dersom man fjerner større deler av avtalen enn det som er hensikten.[86] Det er den behandlingsansvarlige som har ansvaret for at avtalen ut fra valgte modul er dekkende for den aktuelle behandlingsaktivitet.[87]

De eldre standardkontraktsbestemmelsene er blitt oppfattet som statiske og utfordrende å anvende i de situasjoner hvor partskonstellasjonen forandrer seg etter inngåelsen.[88] En måtte inngå nye og separate avtaler dersom det oppsto endringer. De reviderte standardkontraktsbestemmelsene forsøker å løse utfordringen ved å legge til rette for flere parter, samt endring av partskonstellasjonen over tid.[89] Standardavtalen regulerer også adgangen for en importør til å dele informasjonen innad i tredjestaten, eventuelt med andre tredjestater.

[85] Sandtrø, Jan (2021)
[86] Se Personvernforordningen artikkel 86 nr. 5 c)
[87] Se Personvernforordningen artikkel 24
[88] Olsen, Thomas (2021) s. 4
[89] Standardkontraktsbestemmelsene klausul 7 (a)

I Schrems I-saken, ble det lagt til grunn av EU-domstolen et behov for å stille krav til virksomheter som ønsket å føre personopplysninger ut av den trygge sfæren i EU/EØS. Dette skyldes at man så behovet for beskyttelse av opplysningene også etter de var ført ut av EU/EØS, samt at overføring til en annen jurisdiksjon ikke skulle benyttes som en omgåelse av regelverket.[90] Det er blant annet frykten for omgåelse av regelverket som fordret en revidering av de eksisterende standardkontraktsbestemmelsene.

Betydningen av nye standardkontraktsbestemmelser vedtatt av EU-kommisjonen i norsk rett

Nåværende rettstilstand innebærer at de nye standardkontraktsbestemmelsene ikke er gitt direkte anvendelse i norsk rett, ettersom det dualistiske prinsipp fordrer en særskilt implementering av bestemmelsene.[91] Standardkontraktsbestemmelsene er per 02.12.2021 ikke inntatt i EØS-avtalen, men er til evaluering hos EFTA.[92] Dette fordrer følgelig spørsmålet om hvordan norske virksomheter skal forholde seg til de reviderte standardkontraktsbestemmelsene fra EU-kommisjonen.

Ser man til implementeringsvedtaket av Personvernforordningen i EØS-avtalen, uttales det eksplisitt at virksomheter kan, i relasjon til artikkel 45 (1), anvende tiltakene i rettsakten i påvente av en EØS-komitebeslutning.[93] Videre følger det at dersom EFTA-staten ikke har truffet en beslutning om at de ikke vil følge tiltakene i rettsakten i påvente av EØS-komitebeslutning som innlemmer gjennomføringsakten i EØS-avtalen, så skal "hver enkelt EFTA-stat anvende tiltakene i en gjennomføringsakt som er vedtatt i henhold til nr. 3 eller 5 i denne artikkelen [Personvernforordningen artikkel 45, egen presisering]".[94] Artikkel 45 EU-kommisjonens adekvansbeslutninger.

[90] Skullerud mfl. (2019) s. 367
[91] Sejersted mfl. (2014) s. 197-198
[92] EFTA (2021)
[93] 2018/EØS/46/04 (2018) artikkel 1 bokstav e
[94] 2018/EØS/46/04 (2018) artikkel 1 bokstav e tredje avsnitt

Systembetraktninger tilsier at en tilsvarende forståelse må legges til grunn for standardkontraktsbestemmelsene. Begge disse overføringsgrunnlagene har til formål å skulle sikre et tilsvarende likt beskyttelsesnivå for personopplysninger som er blitt ført ut av EU/EØS. Dette tilsier at norske virksomheter bør anvende de nye standardkontraktsbestemmelsene for overføringer til tredjestater i påvente av at bestemmelsene implementeres i EØS-avtalen.[95] Dette underbygges også av at Datatilsynet i sin veileder for overføring av personopplysninger ut av EØS henviser til standardkontraktsbestemmelsene fra 2021.[96]

3.1.2 Personvernrådets vurdering i seks steg

Standardkontraktsbestemmelsene er, som gjennomgangen over viser, et selvstendig overføringsgrunnlag utarbeidet av Europakommisjonen med hjemmel i Personvernforordningen artikkel 46 (2) (c). I kjølvannet av Schrems II-saken ble det et behov for klargjøring av hvilke forpliktelser EU-domstolen nå påla virksomheter som ønsket å foreta overføring av personopplysninger til tredjestater. For å bistå virksomhetene i denne prosessen, utarbeidet Personvernrådet egne anbefalinger. Anbefalingene er et ikke-rettslig bindende dokument utarbeidet av Personvernrådet, og gjelder generelt for overføring av personopplysninger til tredjestater i medhold av artikkel 46.

Formålet med anbefalingene er å gi en fremstilling av en hensiktsmessig metode for hvordan en virksomhet skal kunne overholde de forpliktelsene EU-domstolen har pålagt virksomheter gjennom Schrems II-saken.[97] Anbefalingene presenterer en sekstrinnsvurdering som skal foretas ved den enkelte overføring. Jeg finner det hensiktsmessig å gi en oversikt over den metodiske framgangsmåten som Personvernrådet anbefaler at virksomhetene skal anvende ved vurderingen av om overføring til en tredjestat lovlig kan finne sted, ettersom denne metodikken også ligger til grunn for anvendelse av EU-kommisjonens standardkontraktsbestemmelser.

[95] Personlig kommunikasjon i samtale med N.N. i Datatilsynet 07.10.2021
[96] Datatilsynet (2021) pkt. 4 – Standard personvernbestemmelser som overføringsgrunnlag
[97] Recommendations 01/2020 vol. 2.0 s. 8

Første steg er å gjøre seg kjent med de overføringene virksomheten foretar. I utgangspunktet skal dette være en nokså enkel øvelse, ettersom man etter Personvernforordningen artikkel 30 plikter å føre en protokoll over behandlingsaktivitetene sine. Deretter må man, under steg to, undersøke hvilket overføringsgrunnlag en baserer overføringen på. Også dette er informasjon som skal fremgå av den ovennevnte protokoll. Bygger man på Privacy Shield-rammeverket, har man følgelig et problem.

Steg tre innebærer en vurdering av hvorvidt overføringsgrunnlaget er effektivt i relasjon til tredjelandets rett, altså om det sikrer et tilstrekkelig beskyttelsesnivå. Dette vil følgelig avhenge av anvendelsesområdet til den enkelte lovgivning og den aktuelle behandlingsaktivitet.[98] Er resultatet av vurderingen at datasubjektet er sikret et nærmest tilsvarende beskyttelsesnivå som i EU/EØS, så kan man trygt overføre personopplysningene. Skulle vurderingen fordre et negativt resultat, vil man måtte gå videre til steg fire i vurderingen.

Steg fire innebærer en omfattende og kompleks vurdering av hvorvidt særlige tiltak kan iverksettes for å sikre et tilstrekkelig beskyttelsesnivå. Dette er tiltak som kommer i tillegg til de sikkerhetsmekanismene som finnes i artikkel 46.[99] Den enkelte overføring kan ha behov for tiltak av teknisk, kontraktuell eller organisatorisk art, hvor særlig de tekniske tiltakene er mest nærliggende.[100] En gjennomgang av disse tiltakene ville ha vært en oppgave i seg selv, slik at oppgaven vil ikke vie rom til en nærmere gjennomgang av disse og viser til anbefalingen.[101] Innebærer tiltakene at beskyttelsesnivået er tilnærmet tilsvarende det i EU/EØS, kan overføring finne sted. I noen tilfeller vil ikke tilleggstiltakene sikre et tilstrekkelig beskyttelsesnivå. I slike tilfeller må overføring opphøre på bakgrunn av standardkontraktsbestemmelser som overføringsgrunnlag.

[98] Recommendations 01/2020 vol. 2.0 avsnitt 30
[99] C-311/18 *Facebook Ireland and Schrems* avsnitt 133
[100] Recommendations 01/2020 vol 2.0 avsnitt 54-54.
[101] Recommendations 01/2020 vol. 2.0 avsnitt 50 flg.

Steg fem i anbefalingene er bare aktuelt når et tilstrekkelig beskyttelsesnivå er sikret. Her skal man vurdere iverksettelse av prosessuelle tiltak. Slike tiltak avhenger i stor grad av hvilket overføringsgrunnlag som benyttes.[102] Slik anbefalingene er å forstå, vil ikke prosessuelle tiltak være nødvendig ved bruk av standardkontraktsbestemmelsene som overføringsgrunnlag.[103] Avslutningsvis oppstiller anbefalingene i steg seks krav til jevnlig oppfølging av at beskyttelsesnivået er sikret.

Når det er tale om så komplekse vurderinger som steg tre og fire legger opp til, er også rommet for å gjøre feil stort. På bakgrunn av Personvernsforordningens sanksjonsbestemmelser, er det grunn for å møte denne vurderingen med respekt. Det er sentralt å kjenne til at tilsynsmyndigheten skal vektlegge hvilken innsats som er nedlagt for å overholde regelverket i utmålingen av en eventuell sanksjon.[104] Dette innebærer at dokumentasjon er særlig aktuelt, også hvor man har konkludert feil. Resultatet vil nok uansett være en sanksjon dersom man er i brudd, men omfanget vil være betydelig mindre.

3.2 Betydningen av Personvernforordningens geografiske anvendelsesområde for bruk av de nye standardkontraktsbestemmelsene

Schrems II-saken er et godt eksempel på at man i de senere år har hatt et større fokus rettet mot det å beskytte datasubjektenes rettigheter i de situasjoner hvor deres opplysninger føres ut av EU/EØS' trygge sfære.[105] Som Kuner legger til grunn, viser EU-domstolen at personvernet er gitt en så fremtredende posisjon at "EU data protection rights should be respected in international context, and that their application does not stop at the EU's territorial border".[106] Beskyttelse av de registrertes rettigheter ved overføring til tredjestater sikres gjennom reglene om forordningens geografiske område og reglene for overføring av personopplysninger til tredjestater.

[102] Recommendations 01/2020 vol. 2.0 (2021) avsnitt 59
[103] Recommendations 01/2020 vol 2.0 avsnitt 60
[104] Personvernforordningen artikkel 83
[105] C-311/18 *Facebook Ireland and Schrems*
[106] Kuner, Christopher (2021) s. 3

Reglene som knytter seg til Personvernforordningens geografiske område, virker bestemmende for når europeisk personvernlovgivning vil komme til anvendelse. Reglene som knytter seg til overføring av personopplysninger til tredjestater, setter begrensninger på når slik overføring lovlig kan finne sted. Regelsettene er ansett for å være av stor betydning, og basert på deres innhold og formål, må de anses å være bygget over samme lest.[107] Dette til tross, så har forholdet mellom reglene blitt viet svært lite oppmerksomhet i den juridiske litteraturen, avgjørelser fra domstolene og retningslinjer fra internasjonale og nasjonale tilsynsmyndigheter. Konsekvensen av dette har følgelig vært at det er utfordrende å skulle avgjøre hvorvidt de

> "achieve the protective objectives of EU law and whether their co-existence presents a problem."[108]

I nyere tid har det blitt fremmet initiativer, både fra Personvernrådet og EU-kommisjonen, i den hensikt å avklare forholdet mellom forordningens geografiske virkeområde og reglene om overføring. Blant annet ble det i et upublisert utkast til Personvernrådets retningslinjer om det geografiske virkeområdet fra september 2018 lagt til grunn at kapittel V i forordningen ikke kom til anvendelse hvor Personvernforordningen er gitt direkte anvendelse.[109] Denne avklaringen ble ikke inntatt i den endelige vedtatte versjonen av retningslinjene. I de vedtatte retningslinjene viste man til at det ville gis tilleggsveiledning om problemet dersom det skulle vise seg nødvendig.[110] Personvernrådet har i utkast til en ny veileder eksplisitt lagt til grunn at overføringsmekanismene aktualiseres av begrepet overføring, og ikke hvorvidt vedkommende omfattes av forordningens virkeområde.[111]

Enkelte av uttalelsene som gis i standardkontraktsbestemmelsene kan gi indikasjoner på at EU-kommisjonen har avklart forholdet for bruk av de vedtatte standardkontraktsbestemmelsene.[112] Uttalelsene vil vurderes uavhengig av forslaget fra Personvernrådet om forholdet mellom Personvernforordningen artikkel 3 og kapittel V, ettersom retningslinjene for tiden for innlevering ikke er gyldig vedtatt. Disse uttalelsene skal undersøkes nærmere i det følgende.

---

[107] Kuner, Christopher (2021) s. 4
[108] Kuner, Christopher (2021) s. 4
[109] Kuner, Christopher (2021) s. 17
[110] Personvernrådet guidelines 3/2018 avsnitt 42
[111] Personvernrådet guidelines 5/2021 s. 4
[112] Personvernrådet guidelines 5/2021; Europakommisjonen 2021/914/EC

3.2.1 EU-kommisjonens syn - kommet til uttrykk i standardkontraktsbestemmelsene

Utkastet til nye standardkontraktsbestemmelser artikkel 1 (1) inneholdt formuleringen

> "The standard contractual clauses set out in the Annex are considered to provide appropriate safeguards within the meaning of Article 46 (1) and (2)(c) of Regulation (EU) 2016/679 for the transfer of personal data from a controller or processor subject to Regulation (EU) 2016/679 (data exporter) to a controller or (sub) processor not subject to Regulation (EU) 2016/679 (data importer)"[113]

Ordlyden av sitatet tilsier at standardkontraktsbestemmelsene ikke sikrer et nødvendig beskyttelsesnivå for dataimportører, det være seg behandlingsansvarlig eller (under)databehandlere, som direkte omfattes av Personvernforordningen for den aktuelle behandlingsaktivitet. Formuleringen kan tilsi at standardkontraktsbestemmelsene ikke kan anvendes ved overføring til virksomheter som behandler personopplysninger under direkte anvendelse av personvernforordningen, men at andre overføringsgrunnlag er anvendelige.[114] Videre kan formuleringen "not subject to Regulation (EU) 2016/679" tilsi at anvendelsen av Personvernforordningen avhenger av partene og ikke behandlingsaktiviteten. Det var hevdet at det sistnevnte bygget på en skrivefeil, hvilket også ble bekreftet ved endringene som ble vedtatt i den endelige versjonen.[115]

I det vesentligste, ble det overnevnte videreført i artikkel 1 (1) i den vedtatte versjonen av standardkontraktsbestemmelsene. Implementeringsvedtaket inneholder videre en formulering i fortalepunkt 7 som har skapt diskusjon i det akademiske miljøet.[116] Det er dette fortalepunktet som danner utgangspunkt for den videre drøftelsen av forholdet mellom det generelle anvendelsesområdet til forordningen og standardkontraktsbestemmelsene. Før en går nærmere inn på det faktiske innholdet av fortalepunktet til implementeringsvedtaket, finnes det hensiktsmessig å undersøke nærmere den rettslige betydningen av et implementeringsvedtak og dens fortalepunkter.

[113] Europakommisjonen, Utkast til standardkontraktsbestemmelser publisert 13. november 2020
[114] Kuner, Christopher (2021) s. 19
[115] Kuner, Christopher (2021) s. 19
[116] De Santis mfl. (2021) under pkt. "Data importers subject to the GDPR are not covered"

Et implementeringsvedtak er en rettslig bindende handling fra EU-kommisjonen, og vedtaket er direkte anvendelig i alle medlemsstater i EU. Målet er å sikre en uniform implementering av unionslovgivningen, og dette er det eneste målet med et slikt implementeringsvedtak.[117] Slike vedtak omhandler som oftest meget spesifikke problemstillinger, og knytter seg gjerne til tekniske deler av en gitt lovgivning. For EØS-landene, vises det til gjennomgangen over for betydningen i EØS-landene hvor det ikke er fattet et implementeringsvedtak etter EØS-avtalen.

Implementeringsvedtak inneholder såkalte fortalepunkter, hvilket har til formål å bidra til en unison fortolkning av de aktuelle bestemmelser, slik at en oppnår en enhetlig rettstilstand på tvers av landegrensene i EU/EØS.[118] Dette tilsier at det er en rettskilde av nokså stor vekt, uten at slike fortalepunkter er ansett for å være rettslig bindende i seg selv.[119] EU-domstolen vil i vurderingen av hvordan en bestemmelse i en forordning eller annet dokument utarbeidet av EU-kommisjonen skal forstås, hensynta fortalepunktene slik at man foretar en fortolkning i regelverkets ånd.[120] Dersom det foreligger motstrid mellom et fortalepunkt og en bestemmelse, vil fortalepunktet måtte vike i tråd med lex specialis-prinsippet.

Det er særlig annet punktum i implementeringsvedtakets fortalepunkt 7 som er av interesse for den videre diskusjon. Fortalepunkt 7 annet punktum har følgende ordlyd

> "The standard contractual clauses may be used for such transfers **only** to the extent that the processing by the **importer** does **not fall within the scope** of Regulation (EU) 2016/679."[121] [uthevet her]

Ordlyden tilsier at det ikke vil være adgang til å anvende standardkontraktsbestemmelsene dersom vedkommende dataimportør må overholde Personvernforordningens forpliktelser som følge av at de direkte faller inn under Personvernforordningens geografiske virkeområde for den aktuelle behandlingsaktivitet. Ordlyden reiser spørsmål om det vil være nødvendig å benytte et annet overføringsgrunnlag enn standardkontraktsbestemmelsene i slike situasjoner, og ikke minst i hvilken utstrekning den behandlingsansvarlige vil være ansvarlig for å vurdere hvorvidt dataimportøren direkte faller inn under virkeområdet til forordningen.

---

[117] EU Monitor u.å. under pkt. "Implementing decision in detail"
[118] Jarbekk, Eva (2021)
[119] Sak C-7/11 *Caronna* avsnitt 40
[120] Fredriksen, Halvard, Mathisen, Gjermund (2014) s. 228
[121] Europakommisjonen 2021/914/EC fortalepunkt 7

Ser man fortalepunkt 7 i sammenheng med artikkel 1 (1), kan det tyde på at fortalepunkt 7 annet punktum er ment å forstås bokstavelig, i den forstand at standardkontraktsbestemmelsene ikke er anvendelige i slike situasjoner. Dette skyldes at fortalepunkt 1, hvilket omhandler formålet med standardkontraktsbestemmelsene, legger til grunn at disse bestemmelsene skal sikre at

> "the level of protection of natural persons guaranteed by Regulation (EU) 2016/679 is not undermined where personal data is transferred to third countries".

Ordlyden kan tilsi at målet med standardkontraktsbestemmelsene allerede er nådd ved at man generelt er forpliktet til å overholde forordningens bestemmelser i kraft av behandlingsaktivitetens natur, og at bruk av standardkontraktsbestemmelsene, og for så vidt øvrige overføringsgrunnlag, ikke er nødvendig. Dette er også i samsvar med forståelsen den juridiske litteraturen har lagt til grunn for artikkel 1 (1) som vist til over.[122]

På den annen side tilsier det at forordningen ikke regulerer forholdet til dataimportørens nasjonale rett, at det er nødvendig med et annet overføringsgrunnlag enn standardkontraktsbestemmelsene, såfremt det er tale om en "overføring". Som det ble fastslått i Schrems II-saken,[123] så vil det i slike situasjoner, uavhengig av overføringsgrunnlag, kunne være nødvendig med å innføre særlige tiltak for å påse at det er et tilstrekkelig beskyttelsesnivå. Det følger ikke av Personvernforordningen at slike tiltak skal implementeres, og uten å kategorisere en handling hvor dataimportør er underlagt Personvernforordningen direkte for den aktuelle behandlingsaktivitet som en "overføring", har behandlingsansvarlig ingen plikt til å vurdere dataimportørens nasjonale rett.

Denne forståelsen er også mest nærliggende dersom man ser fortalepunkt 7 i sammenheng med artikkel 44, hvilket omhandler de generelle prinsippene for overføring. Bestemmelsen legger til grunn at reglene i kapittel V kommer til anvendelse for "any transfer of personal data", hvilket tilsier at det er hvorvidt det er tale om en overføring som er avgjørende for om det er nødvendig med et overføringsgrunnlag etter Personvernforordningens kapittel V eller ikke.

[122] Kuner, Christopher (2021) s. 18-19
[123] C-311/18 *Facebook Ireland and Schrems*

Det at det er begrepet "transfer" som er avgjørende for hvorvidt det er nødvendig med et overføringsgrunnlag eller ikke, er også mest nærliggende sett på bakgrunn av avgjørelsen i Schrems II-saken.[124] Dersom motsatt forståelse av fortalepunktet er riktig, altså at det ikke er nødvendig med et overføringsgrunnlag for dataimportører som er omfattet av Personvernforordningen direkte, innebærer det i prinsippet at EU-domstolen har ugyldiggjort et overføringsgrunnlag, nemlig EU-U.S. Privacy Shield-rammeverket, på bakgrunn av en behandlingsaktivitet som ikke utgjør en overførsel.[125] Logikken bak EU-domstolens avgjørelse tilsier således at slike behandlingsaktiviteter utgjør en overføring og at det følgelig er behov for et overføringsgrunnlag etter artikkel 44.

Videre innehar artikkel 44 formuleringen "other provisions of the Regulation", hvilket tilsier at en forståelse som innebærer at Personvernforordningens kapittel V ikke kommer til anvendelse hvor behandlingsaktiviteten til dataimportøren omfattes av forordningens virkeområde direkte, er for snever. Det siterte må innebære at det geografiske virkeområdet til Personvernforordningen, ikke påvirker hvorvidt et overføringsgrunnlag etter kapittel V er nødvendig. Ser man regelverket og implementeringsbestemmelsen i sammenheng, må dette innebære at implementeringsbestemmelsen kun forbyr bruk av standardkontraktsbestemmelsene i slike situasjoner.

Et annet viktig poeng i spørsmålet knyttet til hvorvidt EU-kommisjonens uttalelse stenger for bruk av andre overføringsgrunnlag i slike saker, er det faktum at Personvernforordningen ikke kan anvendes i et vakuum.[126] Man vil måtte forholde seg til annen lovgivning. En alminnelig anvendelse av personvernforordningen bygger på tanken om at alle behandlingsaktiviteter som faller inn under virkeområdet til forordningen, er sikret det samme beskyttelsesnivået. Men dette regulerer ikke forholdet til dataimportørens nasjonale rett. Skal man kunne vurdere hvorvidt det er tale om et tilstrekkelig beskyttelsesnivå reelt sett, så er det nødvendig å påvise et overføringsgrunnlag. Følgelig må uttalelsen til EU-kommisjonen kun forstås som et forbud mot bruk av standardkontraktsbestemmelsene i slike situasjoner, og intet mer.

[124] C-311/18 *Facebook Ireland and Schrems*
[125] Duball, Joseph (2021)
[126] Recommendations 01/2020 vol. 2.0 s. 3

Enkelte hevder at EU-kommisjonen har inntatt denne setningen ved en feiltakelse, og er ikke ment å ha det innhold den naturlige språklige forståelsen skulle tilsi.[127] Dette begrunnes med at anvendelsen av artikkel 46 ikke avhenger av det geografiske virkeområdet til Personvernforordningen som sådan, men hvorvidt den aktuelle tredjestat er godkjent eller ikke etter artikkel 45. Denne forståelsen er også sammenfallende med den rettstilstand som har eksistert frem til vedtakelsen av de nye standardkontraktsbestemmelsene.

Rosenthal mener at standardkontraktsbestemmelsene faktisk kan anvendes til tross for uttalelsen fra EU-kommisjonen i implementeringsvedtaket. Han begrunner dette med at det for de behandlingsansvarlige vil være vanskelig å skulle holde oversikt over hvorvidt en databehandler som er lokalisert utenfor EU/EØS faktisk faller inn under det geografiske virkeområdet til forordningen for den aktuelle behandling.[128]

Personlig mener jeg at denne begrunnelsen er noe tynn. Ser man på de dokumenter som er blitt utformet i kjølvannet av Schrems II-saken, både ved anbefalingene til Personvernrådet og for så vidt de nye standardkontraktsbestemmelsene, så er man ikke fremmed for å pålegge den behandlingsansvarlige omfattende plikter. Det i seg selv kan følgelig ikke være den eneste grunnen til at standardkontraktsbestemmelsene skal kunne anvendes hvor dataimportøren omfattes av Personvernforordningens geografiske virkeområde. Ordlyden er for tydelig til å kunne fravikes på et så tynt grunnlag. Videre er det blitt bekreftet av Personvernrådet at Europakommisjonen skal utarbeide særlige standardkontraktsbestemmelser for situasjonen hvor dataimportøren faller direkte inn under Personvernforordningens geografiske virkeområde.[129]

[127] Rosenthal, David (2021) pkt. 8
[128] Rosenthal, David (2021) pkt. 8
[129] Det Europeiske Personvernråd (2021) pkt 2.1 *[ITS ESG] Guidelines on the interplay between Art. 3 and Chapter V – discussion*

3.2.2 Et meget begrenset anvendelsesområde?

Som gjennomgangen over viser, er det rent språklig tale om en noe usikker rettsstilling tilknyttet forholdet mellom Personvernforordningens regler om geografisk virkeområde og reglene om overføringer, og en avklaring fra EU-kommisjonen selv er følgelig ønskelig med tanke på hva de legger i de ovennevnte uttalelser. En mulig forståelse av fortalepunkt 7 er at det ikke er anledning til å benytte standardkontraktsbestemmelsene som overføringsgrunnlag dersom dataimportøren faller inn under Personvernforordningens geografiske virkeområde for den aktuelle behandlingsaktivitet, men at behandlingsansvarlig vil måtte påvise et annet overføringsgrunnlag i medhold av kapittel V. En annen mulig forståelse kan være at det i slike situasjoner ikke er påkrevd med et overføringsgrunnlag. Rent ordlydsmessig, er det sterkest holdepunkter for at den behandlingsansvarlige må påvise et annet overføringsgrunnlag i slike situasjoner.

En finner støtte for at det er behov for et overføringsgrunnlag i uttalelser fra Personvernrådets nylig vedtatte veileder, hvor det legges til grunn som et kumulativt vilkår at dataimportør må befinne seg i en tredjestat, og at dette vilkåret ikke avhenger av om vedkommende omfattes av Personvernforordningens geografiske virkeområde.[130] I et referat fra det 54. plenumsmøte i Personvernrådet fremgår det at Europakommisjonen har til hensikt å utarbeide en særlig versjon av standardkontraktsbestemmelsene for de situasjoner hvor dataimportøren direkte faller inn under det geografiske virkeområdet til Personvernforordningen.[131]

Slik referatet fra Personvernrådets møte er utformet, tilsier at det er Europakommisjonen selv som, på møtet, bekrefter at de skal utarbeide en særlig variant av standardkontraktsbestemmelsene for de tilfeller at dataimportøren faller inn under Personvernforordningens geografiske virkeområde. Dette indikerer at fortalepunkt 7 i implementeringsvedtaket kun har til formål å begrense bruken av standardkontraktsbestemmelsene, og ikke påvirke forholdet mellom forordningens geografiske virkeområde og kapittel V ut over disse tilfellene. Følgelig vil man frem til de nye standardkontraktsbestemmelsene er på plass, måtte påvise et annet overføringsgrunnlag etter

[130] Det Europeiske Personvernråd (2021) guidelines 05/2021 s. 7
[131] Det Europeiske Personvernråd (2021) pkt 2.1 *[ITS ESG] Guidelines on the interplay between Art. 3 and Chapter V – discussion*

kapittel V. Det er fremdeles "overføring av personopplysninger" som er det avgjørende vilkår for om kapittel V kommer til anvendelse.

Etter dette, er det sterke holdepunkter for å legge til grunn at standardkontraktsbestemmelsenes praktiske virkeområde er meget beskjedent. I de aller fleste tilfeller vil dataimportøren, på bakgrunn av sin rolle i den aktuelle behandlingsaktivitet, falle inn under det geografiske virkeområdet til personvernforordningen etter artikkel 3 (2). Dette innebærer at det overføringsgrunnlag som i stor grad har blitt anvendt etter Schrems II-avgjørelsen, ikke vil kunne benyttes. Videre pålegges behandlingsansvarlig et ansvar for å vurdere hvorvidt dataimportøren faller inn under forordningens virkeområde for den aktuelle behandlingsaktivitet. Behandlingsansvarlig risikerer å havne i ansvar dersom han vurderer situasjonen slik at de omtalte standardkontraktsbestemmelsene kan anvendes, men dette viser seg å være feil.[132]

[132] Se artikkel 83 nr. 5 c)

4 Er det rom for en risikobasert tilnærming ved vurderingen av adgang til overføring av personopplysninger til tredjestater?

Hovedproblemstillingen som EU-domstolen skulle ta stilling til I Schrems II-saken var om datasubjektene var sikret "a level of protection essentially equivalent to that guaranteed within the European Union by that Regulation, read in light of the Charter" ved overføring til tredjestater/internasjonale organisasjoner.[133] Hva som ligger i dette kravet, hvilket også da skal legges til grunn for den vurderingen virksomheter som ønsker å overføre personopplysninger til tredjestater skal foreta, er nokså usikkert og har blitt gjort til gjenstand for diskusjon.[134]

Den usikre rettstilstanden førte til at Personvernrådet utarbeidet noen anbefalinger. Anbefalingene hadde til hensikt å klarlegge hvilke ytterligere tiltak det kunne være aktuelt for virksomhetene å iverksette dersom en kom frem til at tredjestaten ikke hadde et beskyttelsesnivå samsvarende, eller tilnærmet samsvarende, med det som eksisterer i EU/EØS. Formålet med disse tiltakene er å utligne det manglende beskyttelsesnivået i tredjestaten og dermed sikre et vesentlig likeverdig beskyttelsesnivå i praksis.

Det faktum at virksomheten kan påvise et overføringsgrunnlag i Personvernforordningens kapittel V, innebærer nødvendigvis ikke at tredjestaten tilbyr et tilstrekkelig godt nok beskyttelsesnivå. Det skyldes at dataimportøren kan være underlagt visse forpliktelser i nasjonal lovgivning som er i strid med, og hvilket også har forrang over, de forpliktelsene som fremgår av Personvernforordningen.[135] Som gjennomgangen over viser, er det tilfellet for amerikansk lovgivning, hvilket ble tydeliggjort av EU-domstolen gjennom Schrems II-avgjørelsen.[136] Dette er årsaken til at dataeksportøren gjennom Schrems II-avgjørelsen er blitt begrenset til å kun overføre personopplysninger til tredjestater som i praksis kan sikre et beskyttelsesnivå som er vesentlig tilsvarende det som finnes i EU/EØS. Dataeksportøren

[133] C-311/18 *Facebook Ireland and Schrems* avsnitt 96
[134] Vanebro, Ove, Gjerstad, Marianne (2021) s. 9, Ottesten (2021)
[135] C-311/18 *Facebook Ireland and Schrems* avsnitt 125
[136] C-311/18 *Facebook Ireland and Schrems* avsnitt 132

plikter således å undersøke hvorvidt det eksisterer en lovgivning eller praksis i mottakerstaten som gir myndighetene en uforholdsmessig stor tilgang til opplysningene.

Forpliktelsene som følger av Schrems II-saken hva gjelder vurdering av hvorvidt tredjestaten tilbyr et tilstrekkelig beskyttelsesnivå, gjelder uavhengig av hvilket overføringsgrunnlag i artikkel 46 (2) som benyttes.[137] I denne oppgaven skal vi se nærmere på disse kravene opp mot standardkontraktbestemmelsene, og da særlig adgangen til å ta utgangspunkt i en risikobasert tilnærming når en skal vurdere beskyttelsesnivået i tredjestaten i praksis. Den vurdering som omtales nedenfor kan også omtales som en helhetsvurdering, hvilket er den formulering datatilsynet selv benytter.[138] I den følgende benyttes begrepet risikobasert tilnærming.

Et første element som det kan være grunn til å belyse noe nærmere, er hva som menes med en risikobasert tilnærming – hva skal det være risiko for? Ofte legger man til grunn at risikobegrepet består av to elementer, nemlig sannsynligheten for at noe skal skje og hvilke konsekvenser som kan oppstå dersom hendelsen finner sted.[139] I denne forbindelse henviser den faktiske risikoen til muligheten og sannsynligheten for at den aktuelle virksomhet blir utsatt for en innsynsbegjæring fra tredjestatens myndigheter.[140] Altså er spørsmålet hvorvidt sannsynligheten for at amerikanske myndigheter gis tilgang til informasjonen om datasubjektet, kan utgjøre et legitimt moment i vurderingen av USAs faktiske beskyttelsesnivå.

4.1 EU-domstolens syn på en risikobasert tilnærming

I Schrems II-saken kom EU-domstolen med enkelte uttalelser som kan indikere at det eksisterer et visst rom for å hensynta den faktiske risikoen for å bli utsatt for innsynsbegjæringer ved vurderingen av tredjestatens beskyttelsesnivå i praksis.[141] Disse uttalelsene skal i det følgende gjennomgås i den hensikt å fastslå om det faktisk eksisterer et slik rom, og hvis ja, hvor stor dette rommet kan sies å være.

[137] C-311/18 *Facebook Ireland and Schrems* avsnitt 92 og 105
[138] Judin, Thomas (2021) pkt. "Hva er greia?"
[139] Datatilsynet (2019) s. 4
[140] Simmons Simmons (2021) *Data transfers: Final recommendations by the EU Data Protection Board*
[141] C-311/18 *Facebook Ireland and Schrems*

Avgjørelsen legger opp til at dersom en skal benytte standardkontraktsbestemmelsene vedtatt av EU-kommisjonen som overføringsgrunnlag, så skal man

> "take into consideration both the contractual clauses agreed […] and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country."[142]

Ordlyden av det ovennevnte sitatet, tilsier at det skal foretas en helhetlig vurdering av rettsstillingen i tredjestaten. Sitatet inneholder ingen begrensninger på hva slags kilder det er relevant å hensynta, hvilket i prinsippet tilsier at det også er anledning til å innta virksomhetenes faktiske risiko for å bli utsatt for innsynsbegjæringer fra myndighetene i tredjestaten som et vurderingsmoment for tredjestatens beskyttelsesnivå i praksis for den enkelte behandlingsaktivitet.

Den ovennevnte forståelse underbygges av en rekke senere uttalelser i avgjørelsen. Blant annet så fremheves det at bruk av standardkontraktsbestemmelsene ikke kan gi garantier utover en ren kontraktsmessig karakter, hvilket innebærer at det er nødvendig å foreta en helhetsvurdering

> "depending on the prevailing position in a particular third country, the adoption of supplementary measures […] in order to ensure compliance with that level of protection".[143]

Ses de to sitatene i sammenheng, fremstår det som at EU-domstolen legger opp til at dataeksportøren skal foreta en konkret vurdering av hvilke tiltak som må iverksettes for at tredjestaten skal anses for å ha et tilstrekkelig beskyttelsesnivå. Når EU-domstolen uttaler at vurderingen skal basere seg på de relevante aspektene i rettssystemet sett ut fra den særlige situasjonen i den aktuelle tredjestaten, med det formål å vurdere hvorvidt et tilstrekkelig beskyttelsesnivå kan sikres i praksis, så tilsier det at EU-domstolen åpner opp for en helhetlig vurdering hvor alle relevante forhold i tredjestaten kan og skal hensyntas. Avgjørelsen kan ikke sies å oppstille noen kvalifikasjonskrav for hvor informasjonen stammer fra, slik at det dermed vil være aktuelt å hensynta den faktiske risikoen for den enkelte virksomhet.

[142] C-311/18 *Facebook Ireland and Schrems* avsnitt 105
[143] C-311/18 *Facebook Ireland and Schrems* avsnitt 133

EU-domstolens avgjørelse i Schrems II-saken taler for at det er rom for å hensynta den faktiske risikoen hos den enkelte virksomhet for å bli utsatt for innsynsbegjæringer når en skal vurdere beskyttelsesnivået for de aktuelle personopplysninger i den konkrete tredjestaten. I den følgende skal oppgaven se nærmere på om Personvernrådet og Europakommisjonen har lagt seg på en tilsvarende linje.

4.2 Personvernrådets syn på en risikobasert tilnærming

Basert på at Schrems II-avgjørelsen etterlot en nokså stor usikkerhet for den enkelte virksomhet som ønsket å overføre personopplysninger til tredjestater[144], og særlig til USA, publiserte Personvernrådet i november 2020 et utkast til anbefalinger for virksomheter som skulle foreta slike overførsler.[145]

Anbefalingene ble før vedtakelse sendt ut på høring hvor en rekke aktører ble gitt anledning til å uttale seg. Innledningsvis skal oppgaven belyse Personvernrådets opprinnelige standpunkt til å hensynta den faktiske risikoen ved vurderingen av beskyttelsesnivået i en tredjestat, før en ser nærmere på de endelig vedtatte anbefalinger. Bakgrunnen for at både utkast til og vedtatte anbefalinger vil være egnet til å illustrere at å hensynta den faktiske risikoen er den mest nærliggende løsningen på spørsmålet om hvilke momenter det er anledning til å hensynta i vurderingen av tredjestatens beskyttelsesnivå.

Utkastet til anbefalingene, publisert november 2020, overrasket en rekke akademikere og praktikere, ettersom utkastet i meget stor grad avvek fra det man trodde var gjeldende rett ut fra EU-domstolens avgjørelse.[146] I utkastet ble det eksplisitt lagt til grunn at i de tilfeller hvor en ikke kunne bygge vurderingen av tredjestatens faktiske beskyttelsesnivå alene på offentlig tilgjengelig lovgivning, så kunne man

> "look into other relevant and objective factors, and not rely on subjective ones such as the likelihood of public authorities' access to your data in a manner not in line with EU standards."[147]

[144] Vengadesan, Joanne, Lovett, Dan, Pook, Nora (2020)
[145] Recommendations 01/2020 vol. 1.0
[146] Vanebro, Ove, Gjerstad, Marianne (2021) s. 9-14, Rode (2021), Digital Europe (2020)
[147] Recommendations 01/2020 vol. 1.0 avsnitt 42

Ordlyden tilsier at det ikke er adgang for å hensynta den faktiske risikoen for innsynsbegjæring i den enkelte virksomhet ved vurderingen av overføringsgrunnlagets effektivitet. I stedet skal man foreta vurderingen på bakgrunn av hvorvidt lovverket i seg selv møter de krav som følger av Personvernforordningen og menneskerettighetscharteret. Utkastet fra Personvernrådet legger opp til en rettsstilling som er klart i strid med nokså tydelige uttalelser fra EU-domstolen. Hadde dette blitt vedtatt, ville man måtte ha forholdt seg ene og alene til uttalelsene fra EU-domstolen, ettersom denne må anses for å forrang over en ikke-bindende uttalelse fra Personvernrådet.

Av de nesten 200 virksomhetene, organisasjonene og akademikerne som avsa høringsuttalelse til forslaget, håpet en rekke av disse på at Personvernrådet skulle bevege seg vekk fra den dogmatiske posisjonen i de endelige anbefalingene.[148] Det er også tilfellet, ettersom Personvernrådet i de vedtatte anbefalingene i større grad har åpnet opp, iallfall til en viss grad, for en mer risikobasert tilnærmingsmåte. I de vedtatte anbefalingene uttales det at man i tillegg til offentlig tilgjengelig lovgivning, kan hensynta annen informasjon såfremt den er

> "relevant, objective, reliable, verifiable and publicly available or otherwise accessible to determine whether your Article 46 transfer tool can be effectively applied and you will have to assess and document that they are."[149]

Ordlyden tilsier at det er rom for å anvende andre kilder enn kun de som faller inn under kategorien offentlig tilgjengelig lovgivning. Allikevel tilsier sitatet at det er meget strenge krav som skal oppfylles for at kildene kan anses legitime. Anbefalingen legger således opp til en vurdering basert på objektive kilder som er offentlig tilgjengelig. Dette kan indikere en viss utfordring knyttet til det å skulle anvende egenutarbeidet statistikk, selv om denne skulle bevise at den faktiske sannsynligheten for at personopplysningene må utleveres til amerikanske myndigheter, og dermed at man opptrer i brudd med personvernforordningen, er meget liten.

[148] Rode mfl. (2021)
[149] Recommendations 01/2020 vol. 2.0 avsnitt 46

Ved å tillate at virksomheter kan hensynta den faktiske risikoen for innsynsbegjæring for den enkelte virksomhet, så åpner man opp for å tillate at flere overføringer kan finne sted, også hvor en ren ordlydsfortolkning av tredjestatens nasjonale rett skulle tilsi at landet ikke sikret et tilstrekkelig beskyttelsesnivå for datasubjektene.

Anbefalingen adresserer direkte bruken av den enkelte virksomhets individuelle statistikk over tilfellene hvor de er blitt utsatt for innsynsbegjæringer som kilde i vurderingen av den enkelte tredjestat sitt beskyttelsesnivå. Det legges til grunn at det er rom for å hensynta

> "documented practical experience of the importer with relevant prior instances of requests for access received from public authorities."[150]

Ordlyden tilsier etter dette at det er rom for å hensynta egne erfaringer med myndighetene i relasjon til innsynsbegjæringer. Imidlertid uttales det på samme sted i anbefalingene at slik dokumentasjon/statistikk kun skal fungere som en "additional source". Ses uttalelsene i sammenheng, tilsier de at slik dokumentasjon/statistikk ikke er egnet til å stå på egne bein. Det må følgelig være andre kilder som trekker i samme retning for at det skal være aktuelt å tillate overføring til slike land. Videre følger det av anbefalingene at det kun er anledning til å hensynta slik informasjon såfremt den aktuelle tredjestat ikke har gjort bruk av informasjonen ulovlig, f.eks. gjennom pålegg om munnkurv.[151] Ettersom amerikansk etterretningstjeneste med hjemmel i FISA § 1881a kan pålegge munnkurv, er det rimelig å legge til grunn at dette gjøres sedvanlig.[152]

Konsekvensen av dette vil kunne være at det i prinsippet aldri vil være aktuelt å hensynta den faktiske risikoen, ettersom det kun skal fungere som en tilleggskilde. Man kan se for seg en situasjon med en amerikansk virksomhet som i forkant av Schrems II-avgjørelsen[153] har mottatt store mengder personopplysninger fra europeiske virksomheter og aldri har vært utsatt for en innsynsbegjæring. Hadde det vært åpnet for at slik sannsynlighet var et selvstendig moment i vurderingen, kunne det føre til at overføring lovlig kunne finne sted. Basert på uttalelsene i Personvernrådet, kan det imidlertid vanskelig velte det inntrykk av amerikansk lovgivning som tilsier at myndighetene har ekstremt vide hjemler til å kunne innhente personopplysninger, ettersom den teoretiske muligheten er til stede og såpass klar. Det er

[150] Recommendations 01/2020 vol 2.0 avsnitt 47
[151] Recommendations 012020 vol 2.0 avsnitt 47
[152] Bloemen, Annemarie (2020) s. 4
[153] C-311/18 *Facebook Ireland and Schrems*

grunn til å stille spørsmål ved om Personvernrådet gjennom denne uttalelsen kun åpner for å hensynta subjektive momenter hvor den underbygger sannsynligheten for at krenkelse vil kunne finne sted.

I anbefalingenes bilag 3 fremgår det at man i vurderingen av tredjestatens faktiske beskyttelsesnivå, kan ta i betraktning

> "Reports based on practical experience with prior instances for requests for disclosure from public authorities, or the absence of such requests, from entities active in the same sector as the importer."[154]

Uttalelsen tilsier at det er åpnet for å vektlegge statistikk over hvor ofte slike innsynsbegjæringer fremmes, ikke bare i den faktiske virksomheten, men også fra andre virksomheter i samme bransje. Implisitt i det faktum at man kan benytte statistikk fra andre virksomheter i samme bransje, ligger at slik statistikk vil måtte være offentlig tilgjengelig. På bakgrunn av at, særlig amerikanske myndigheter, er nokså tilbakeholdne med å uttale seg om at slike begjæringer er fremsatt og ofte pålegger virksomhetene munnkurv, kan det være i nokså begrenset omfang at dette forholdet kan gis avgjørende betydning.[155]

Skal en foreta en oppsummering av hva Personvernrådet synes å mene omkring bruk av en risikobasert tilnærming i vurderingen av om tredjestaten sikrer et tilfredsstillende beskyttelsesnivå, er det på det rene at det språklig sett er adgang for å vektlegge slike faktorer. Allikevel skal slike faktorer også dokumenteres gjennom objektive og offentlig tilgjengelige kilder. I tråd med dokumentasjonskravene i personvernforordningen generelt, fremhever Personvernrådet at virksomhetens vurdering bør dokumenteres i skriftlige rapporter som innehar en beskrivelse av (1) lovgivningen og praksisen i tredjestaten som aktualiseres ved overføringen, (2) hvilken prosedyre man har anvendt for å vurdere tredjestatens beskyttelsesnivå, og (3) hvilken dato vurderingen ble foretatt og eventuelle påfølgende kontroller.[156]

[154] Recommendations 01/2020 vol 2.0 avsnitt 144
[155] Lee, Phil (2016) under pkt. "1. The Foreign Intelligence Surveillance Act (FISA) & the FISA Amendments Act"
[156] Recommendations 01/2020 vol 2.0 avsnitt 43.3

4.3 EU-kommisjonens syn på en risikobasert tilnærming

Schrems II-saken[157] fordret også en revisjon av gjeldende standardkontraktsbestemmelser, hvilket ble igangsatt fra EU-kommisjonens side omtrent i samme tidsrom som Personvernrådet satte i gang arbeidet med de ovennevnte anbefalinger. Også her ble et utkast først sendt på høring. Jeg finner det hensiktsmessig å se nærmere både på utkastet og det endelig vedtatte dokument.

I utkastet til de nye standardkontraktsbestemmelsene, hadde EU-kommisjonen inntatt en klausul som jeg i det følgende vil omtale som "erkjennelsesklausulen". Denne klausulen gjorde det mulig for dataeksportørene til å erklære at det ikke foreligger motstrid mellom dataimportørens nasjonale rett og Personvernforordningen. Dataeksportøren samtykker til at han har foretatt en vurdering av tredjestatens nasjonale rett og også hensyntatt

> "any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred"[158]

Ordlyden tilsier at det er fritt frem å hensynta enhver praktisk erfaring knyttet til eventuelle innsynsbegjæringer når en skal vurdere tredjestatens faktiske beskyttelsesnivå. Videre uttales det eksplisitt at også fravær av innsynsbegjæringer utgjør en relevant kilde i vurderingen. Kommisjonens syn må etter dette forstås som at rommet for en risikobasert tilnærming eksisterer, og er nokså stort.

EU-kommisjonens standpunkt førte til at Personvernrådet i fellesskap med Det europeiske datatilsynet fremmet en høringsuttalelse til utkastet.[159] De uttaler seg nokså kritisk til utgangspunktet om at man kan hensynta den faktiske risikoen ved vurderingen av tredjestatens nasjonale rett, og uttaler i den forbindelse at vurderingen

> "should be based on objective factors, regardless of the likelihood of access to the personal data"[160]

[157] C-311/18 *Facebook Ireland and Schrems*
[158] Utkast Standard contractual clauses klausul 2, bokstav b, (I) avsnitt 20
[159] EDPB-EDPS Joint Opinion 2/2021
[160] EDPB-EDPS Joint Opinion 2/2021 avsnitt 86

Høringsuttalelsen fra Personvernrådet og Det europeiske datatilsynet uttaler eksplisitt at det ikke bør være rom for å hensynta den faktiske risikoen for å bli utsatt for innsynsbegjæringer. Dette samsvarer jo med den holdning Personvernrådet hadde på tidspunktet, ettersom denne høringsuttalelsen tilsvarer det Personvernrådet som utgangspunkt la til grunn i utkastet til anbefalingene.

I den endelige versjonen fjernet EU-kommisjonen, erkjennelsesklausulen. Dette kan tyde på at EU-kommisjonen ser for seg at vurderingen av mottakerstatens beskyttelsesnivå alene skal basere seg på objektive momenter. Dette er nok ikke rett forståelse. Ser man til fotnote 12 i implementeringsvedtaket, så fremgår det at

> "As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experiences with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame"

Rent språklig tilsier dette punktet at det ved anvendelse av standardkontraktsbestemmelsene er rom for å foreta en helhetsvurdering, hvor risikoen for å bli utsatt for en innsynsbegjæring utgjør et relevant moment. Spørsmålet er bare i hvor stor grad. Leser man fotnote 12 i sin helhet, kan det fremstå som at den praktiske erfaringen alene ikke vil være nok for å kunne legitimere en overføring. Den må "be supported by other relevant, objective elements".[161] Det vil særlig være relevant for virksomheten å se på hvorvidt disse opplysningene er blitt bekreftet av annen offentlig tilgjengelig informasjon. Også oversikt fra bransjeorganisasjoner eller andre virksomheter i samme bransjer vil her være relevant, i likhet med rettspraksis og rapporter fra uavhengige tilsynsorganer.[162]

For virksomhetene innebærer dette at de må kontrollere hvorvidt deres egen erfaring kan underbygges av offentlig tilgengelige og pålitelige kilder.[163] Videre er det, i tråd med de alminnelige utgangspunkter i Personvernforordningen, krav om at denne vurderingen bør dokumenteres i utstrakt grad.

[161] 2021/914/EC s. 23
[162] 2021/914/EC s. 23 fotnote 12
[163] Mole, Ariane, Boardman, Ruth, Voisin, Gabriel (2021) under pkt. "What don't the Clauses cover?"

Samlet sett fremstår det fremdeles som at EU-kommisjonen åpner for en risikobasert tilnærming ved anvendelse av standardkontraktsbestemmelsene. Sammenlignet med utkastet, fremstår det endelige vedtaket som noe moderert ettersom det stilles nokså strenge kvalifikasjonskrav til opplysningens kilde. På denne måten kan man kanskje hevde at Personvernrådet har i større grad åpnet for bruk av en risikobasert tilnærming sammenlignet med det opprinnelige utkastet, mens EU-kommisjonen har begrenset anvendelsen noe. Totalt sett fremstår de to relevante dokumentene for nå å gi uttrykk for samme adgang.

4.4 I hvor stor grad kan en risikobasert tilnærming benyttes?

Gjennomgangen over viser at rettskildebildet åpner for å benytte en risikosom et moment i vurderingen av hvorvidt tredjestaten tilbyr et tilstrekkelig beskyttelsesnivå. Kildene er imidlertid tause hva gjelder i hvilken utstrekning den faktiske risikoen kan prege vurderingen. Dette er temaet i det følgende.

Ut fra formuleringene til Personvernrådet og EU-kommisjonen, kan det se ut til at det juridiske rommet for en risikobasert tilnærming er snevert. Det skyldes særlig kravene til informasjonens kilde, hvilket begrenser den faktiske risikoens faktiske betydning. Personvernrådet og EU-kommisjonen legger videre til grunn at denne type informasjon ikke kan anvendes dersom myndighetene i tredjestaten har gjort det forbudt å tilgjengeliggjøre denne informasjon.[164] Det er et velkjent fenomen at amerikanske myndigheter er tilbakeholdne med informasjonen om hvorvidt slike innsynsbegjæringer er utstedt, samt at virksomhetene ofte pålegges munnkurv. Konsekvensen av dette vil følgelig være at det juridiske rommet for anvendelse av en risikobasert tilnærming er meget lite.

Datatilsynet har på sin side uttalt at det faktum at virksomheten aldri er blitt utsatt for en innsynsbegjæring, alene ikke vil være tilstrekkelig som kilde for å påvise at tredjestaten sikrer et tilstrekkelig beskyttelsesnivå for den aktuelle behandling.[165] Følgelig vil den faktiske risikoen kun utgjøre et moment i en større helhetsvurdering, og dens vekt er blitt redusert i den forstand at momentet ikke kan gis avgjørende betydning hvor det står alene. Dette taler også i retning av at det juridiske rommet for bruk av faktisk risiko er meget lite, praktisk talt

[164] Recommendations 01/2020 vol 2.0 avsnitt 47 og 2021/914/EC s. 23 fotnote 12
[165] Datatilsynet (2021) s. 12

ikke-eksisterende. Dette fordi det må eksistere en annen kilde som underbygger den enkelte virksomhets praktiske erfaring med innsynsbegjæringer. Det er utfordrende å skulle se for seg hva slags kilder som eventuelt skulle oppfylle kravet til legitimitet og som også har tilstrekkelig tyngde til å stå imot en klar lovhjemmel.

På den annen side, tilsier systemet som ligger til grunn for Personvernforordningen, at rommet for å hensynta den faktiske risikoen bør være noe større enn det som er indikert over. Personvernforordningen viser at det er den behandlingsansvarliges risikovurderinger som ligger til grunn for vurderingen av hvorvidt det aktuelle selskap anses som compliant, og som også må bære risikoen for en eventuell feilvurdering. Som følge av at det ikke er tatt eksplisitt avstand fra at reglene om overføring skal benytte seg av den grunnleggende risikobaserte fremgangsmåten som Personvernforordningen er tuftet på, bør den faktiske risikoen erkjennes en viss betydning i vurderingen av om tredjestatens sikrer et tilstrekkelig beskyttelsesnivå.

Det kan stilles spørsmål ved om hvordan en rettsregel er blitt praktisert historisk er egnet til å illustrere hvordan praktiseringen vil være fremover, og dermed kunne anvendes som et legitimt vurderingsmoment i spørsmål knyttet til beskyttelse av individs grunnleggende rettigheter. Det faktum at slik praksis er egnet til å endre seg, kan tale for at momentet ikke bør tilkjennes all verden av betydning i vurderingen. På den annen side er skjer utviklingen på området i tråd med digitaliseringen, hvilket kan være egnet til å gi individene en noe større grad av forutberegnelighet. Når utviklingen skjer i takt med digitaliseringen, er man i noe større grad sikret forutberegnelighet, hvilket igjen kan tale i retning av at det bør være et visst rom for å hensynta den faktiske risikoen.

Dette underbygges av det faktum at det er tale om europeiske borgeres grunnleggende rettigheter og friheter. Personvernforordningen bygger i stor grad på Menneskerettighetskonvensjonen artikkel 8 og det europeiske Charteret artikkel 7 og 8 om retten til privatliv.[166] Dette innebærer at bestemmelsene i forordningen må fortolkes på denne bakgrunn.[167] Følgelig må en ved vurderingen av rommet for å hensynta den faktiske risikoen, se hen til hvilke konsekvenser det vil kunne få for den enkeltes rettigheter og friheter dersom en slik innsynsbegjæring fremsettes og tas til følge. Som følge av at amerikansk lovgivning ikke gir europeiske borgere håndhevbare rettigheter, vil det kunne argumenteres for at rommet

[166] Skullerud mfl. (2019) s. 36
[167] C-311/18 *Facebook Ireland and Schrems* avsnitt 94

for den faktiske risikoen må settes til det minimale og dermed kun fungere som et støttemoment.

Formålet med reglene om overføring er å "verne personopplysninger som i utgangspunktet har en tilknytning til virksomheter eller innbyggere i EU, også etter at opplysningene har forlatt EU".[168] Hvor det kun er tale om en teoretisk mulighet for at de registrertes rettigheter og friheter vil bli krenket, bør rommet for å hensynta den faktiske risikoen være av en viss størrelse. Dette skyldes at den reelle risikoen er såpass beskjeden at man i praksis ikke kan tale om noen trussel. Videre er det et anerkjent behov for å kunne overføre personopplysninger ut av EU/EØS, se blant annet fortalepunkt 101 til Personvernforordningen. Derav bør en ikke umuliggjøre en overføring som i siste omgang vil være fordelaktig også for datasubjektet selv. Dette taler følgelig at det bør være et visst rom for å kunne hensynta den faktiske risikoen for innsynsbegjæring hos den enkelte virksomhet.

Samlet sett kan det virke som om det juridiske rommet for å kunne hensynta den faktiske risikoen for innsynsbegjæringer er meget lite, mens det praktiske rommet fremstår som noe større. Helt konkret kan man legge til grunn de kildene som tilsier at den faktiske risikoen kun kan fungere som en tilleggskilde for å støtte opp under øvrige argumenter som taler i samme retning.

4.5 Mulige konsekvenser av en for streng praktisering

Den enkelte virksomhet som ønsker å overføre personopplysninger til tredjestater, er etter dette pålagt meget omfattende forpliktelser. Ettersom Personvernforordningen skal gjelde for alle virksomheter, uavhengig av størrelse og økonomisk tilgjengelighet, vil disse kravene, dersom praktisert enda strengere enn først forutsatt av EU-domstolen, definitivt kunne være spikeren i kisten for enkelte virksomheter. Flesteparten av europeiske virksomheter har behov for programvarer som er enkelt tilgjengelig og til en lav pris. Dette fører følgelig til at påvirkningsmulighetene det enkelte selskap har overfor utviklere, er minimale. Konsekvensen vil kunne være et større skille mellom store og små virksomheter, og utfordringene med å etablere en ny virksomhet i EU/EØS vil vokse.

[168] Skullerud mfl. (2019) s. 366

I et globalt perspektiv vil dette kunne føre til at europeiske virksomheter begrenser sin forretningsførsel og handel med store aktører i land som USA eller Kina. Rent samfunnsøkonomisk er dette svært negativt. En mulig konsekvens vil kunne være at land som USA og Kina "utestenges" fra det indre marked, hvilket igjen vil påvirke de tjenestene individene kan benytte. Bare tenk over hvor raskt og i hvilket omfang samfunnet har omveltet seg til en teknologisk verden som følge av COVID-19. En slik omveltning hadde ikke vært mulig uten amerikanske tjenesteleverandører som Microsoft.

En annen mulig konsekvens er følgelig at virksomhetene unngår å benytte standardkontraktsbestemmelsene som overføringsgrunnlag som følge av den komplekse vurderingen som skal foretas. Overføring vil følgelig fremdeles være nødvendig, slik at man ser seg nødt til å benytte andre overføringsgrunnlag og da gjerne de som fremgår av unntaksbestemmelsen i artikkel 49. Satt på spissen kan dette føre til at samtykke blir den nye hovedregel. Av hensyn til de registrertes rettigheter og friheter, bør dette unngås ved at bruken av en risikobasert tilnærming ikke blir for snever.

5 Avslutning

Gjennomgangen over viser at det eksisterer et spenningsforhold mellom europeisk og amerikansk personvernrett. Spenningsforholdet gjør at det reiser seg spørsmål om mulighetene for europeiske virksomheter til å benytte seg av amerikanske tjenesteleverandører. Oppgaven skal i det følgende konkludere på spørsmålet om det er praktisk mulig å benytte standardkontraktsbestemmelser som overføringsgrunnlag. Hvor aktuell anvendelsen anses for å være, vil blant annet avhenge av rommet for å hensynta den faktiske risikoen for å bli utsatt for innsynsbegjæringer. Avslutningsvis ser oppgaven noe nærmere på om nåværende situasjon er levedyktig, eller om det er mer hensiktsmessig å komme frem til en politisk løsning på situasjonen.

5.1 Er det praktisk mulig å anvende standardkontraktsbestemmelsene som overføringsgrunnlag ved overføring til USA?

I kjølvannet av Schrems II-avgjørelsen fryktet en rekke aktører at en ikke lenger kunne anvende amerikanske tjenesteleverandører. Tiden etter avgjørelsen har vist at dette ikke er tilfellet. Det er imidlertid ingen enkelt øvelse å skulle overføre personopplysninger til USA slik rettstilstanden er per nå. Virksomhetene er pålagt omfattende forpliktelser til å foreta komplekse vurderinger av beskyttelsesnivået i den tredjestat den aktuelle tjenesteleverandør befinner seg. EU-domstolen har ved Schrems II-saken skjerpet kravene for virksomheter som ønsker å benytte standardkontraktsbestemmelsene som overføringsgrunnlag.

Ugyldiggjøringen av Privacy Shield-rammeverket har medført at standardkontraktsbestemmelsene per nå er det mest hensiktsmessige overføringsgrunnlaget. Uttalelser i implementeringsvedtaket til de nye standardkontraktsbestemmelsene har imidlertid ført til at overføringsgrunnlagets virkeområde er blitt meget innsnevret sammenlignet med praksis før Schrems II-avgjørelsen.[169] Dette skyldes at det vanskelig kan tenkes tilfeller hvor en dataimportør i en tredjestat ikke direkte omfattes av

[169] *Commission Implementing Decision (EU) 2021/914 of 4 June 2021* C/2021/3972

Personvernforordningens geografiske virkeområde etter artikkel 3, ettersom dataimportøren mottar personopplysninger fra en europeisk virksomhet og utfører oppgaver på dens vegne.

Uavhengig av hvilket overføringsgrunnlag virksomheten benytter, er det visse ting enhver dataeksportør bør foreta seg dersom en ønsker å fortsette med overføring av personopplysninger til USA og andre tredjestater. Virksomhetene bør skaffe seg oversikt over virksomhetens internasjonale samhandlingspartnere, og i den forbindelse vurdere hvorvidt man i relasjon til den enkelte samhandlingspartner foretar overføring av personopplysninger som fordrer overføringsgrunnlag. Benyttes Privacy Shield, må den aktuelle overføringsprosess opphøre med mindre man kan påvise et annet legitimt overføringsgrunnlag. EU-domstolens avgjørelse i Schrems II-saken er ikke ensbetydende med at overføring til USA vil være ulovlig i ethvert tilfelle. Basert på en konkret helhetsvurdering, kan en komme frem til at den amerikanske lovgivningen ikke strider mot europeiske borgeres grunnleggende rettigheter.

Som gjennomgangen over viser, så eksisterer det i teorien et rom for å hensynta den faktiske risikoen for å bli utsatt for innsynsbegjæringer i vurderingen av om USA sikrer et tilstrekkelig beskyttelsesnivå. Rettslig sett er imidlertid dette rommet lite, ettersom, som gjennomgangen over viser, den faktiske risikoen kun skal fungere som tilleggskilde. En slik forståelse er også mest nærliggende som følge av at Personvernforordningen har til formål å sikre individenes grunnleggende rettigheter. Sett fra et næringslivsperspektiv, har man klart nok behov for et større rom for å hensynta den faktiske risikoen ettersom dette er en faktor som i stor grad viser at sannsynligheten for krenkelse av individenes rettigheter i visse tilfeller er marginal.

En potensiell nedside ved den komplekse vurderingen som preger dagens rettstilstand, er følgelig at virksomhetene søker å anvende unntaksbestemmelsene i artikkel 49 som overføringsgrunnlag på permanent basis. Dette vil imidlertid være ulovlig, som følge av at artikkel 49 ikke er anvendelig for virksomheter som gjentakende foretar overføringer til USA eller andre tredjestater. Benytter man artikkel 49 i større omfang enn tillatt,[170] vil man kunne havne i ansvar etter Personvernforordningen artikkel 83 nr. 5.

[170] Se C-72/07 og de forente saker C-293/12 og C-594/12 premiss 52

Selv om rettstilstanden legger til grunn meget kompliserte vurderinger, er det likevel mulig å foreta lovlige overføringer av personopplysninger til USA. Alle virksomheter, uavhengig av størrelse og omsetning, er pålagt omfattende forpliktelser til selv å skulle vurdere om dataimportøren faller inn under amerikanske etterretningshjemlers virkeområde for den aktuelle behandlingsaktivitet i praksis. I denne vurderingen er den faktiske risikoen for å bli utsatt for en innsynsbegjæring fra amerikanske myndigheter, kun blitt erkjent en plass som støttemoment.

5.2 Behov for en politisk løsning

Det at man to ganger har forsøkt å ha avtalebasert overføringsgrunnlag for overføring av personopplysninger fra Europa til USA, tilsier at EU også anerkjenner behovet, slik den tekniske virkelighet er per nå, for å kunne foreta overføringer til USA. Behovet for å kunne overføre personopplysninger fra Europa til USA har resultert i at man både på amerikansk og europeisk side ser etter løsninger på hvordan man kan håndtere situasjonen. Det amerikanske handelsdepartementet ga sammen med EU-kommisjonen ut en felles pressemelding hvor de uttalte at de hadde bestemt seg for å:

> "intensify negotiations on an enhanced EU-U.S. Privacy Shield framework to comply with the July 16, 2020 judgement of the Court of Justice of the European Union in the Schrems II case"[171]

Hvordan en eventuell politisk løsning skal være, er komplisert. Det er ikke meg bekjent at EU er villige til å redusere sine krav til beskyttelsesnivå for at overføring til USA skal kunne finne sted. Historisk sett vil dette også vært noe unaturlig fra EUs side, ettersom det ligger mye arbeid bak det beskyttelsesnivået en har klart å skape gjennom vedtakelsen av Personvernforordningen. Konsekvensen av dette er følgelig at man enten må forholde seg til den noe kompliserte fremgangsmåten ved bruk av standardkontraktsbestemmelsene, eller så er det opp til USA alene, eller i fellesskap med EU, å komme frem til en løsning som tilfredsstiller EUs krav. Hvilke muligheter som eksisterer fra amerikansk side, skal behandles noe nærmere i det følgende, ettersom det fra amerikansk side ved Kongressen er blitt publisert en artikkel over mulige løsninger på problemet.[172]

[171] Europakommisjonen og det amerikanske handelsdepartementet (2021)
[172] Linebaugh, Chris, Liu, Edwards (2021)

Kongressen presenterer det å utstede en Executive Order med det formål å begrense overvåking over ikke-amerikanske borgere som første alternativ for å kunne sikre et tilstrekkelig beskyttelsesnivå ved behandling i USA.[173] En slik ordre vil måtte være omfattende dersom den skal løse alle utfordringer EU-domstolen fant ved amerikansk rett sett opp mot Personvernforordningen.

En annen mulighet vil kunne være å endre den amerikanske lovgivning ved å innarbeide krav om kjennelse fra domstolen for den enkelte overvåking og utlevering av informasjon som har kommet ut av en slik overvåking.[174] Særlig kravet om at den enkelte utlevering skal behandles av domstolene, vil kunne være egnet til å gi de registrerte effektive rettsmidler for å håndheve sine rettigheter. Denne løsningen risikerer å gripe inn i det maktfordelingsprinsippet som det amerikanske styresettet legger opp til, og vil dermed risikere å være grunnlovsstridig.

Et tredje alternativ presentert fra den amerikanske kongressen er at man utarbeider en avtale eller lignende juridisk dokument på bakgrunn av diplomatiske forhandlinger mellom USA og EU. Dette alternativet vil nok i stor grad minne om det nå ugyldige Privacy Shield-rammeverket. Kongressen ser det dithen at en mulig avtale kan fremforhandles av EU/EØS på den ene siden og den utøvende makt i USA på den andre.[175]

Dette er kanskje den mest nærliggende løsningen, ettersom EU-kommisjonen og det amerikanske handelsdepartementet allerede har innledet samtaler.[176] Det er imidlertid grunn til å stille spørsmål ved om dette er en mulig løsning uten at det skjer endringer på amerikansk side. EU-kommisjonen har nå ved to forsøk, Safe Harbour og Privacy Shield, forsøkt å komme frem til en diplomatisk løsning som begge gangene ble ugyldiggjort i EU-domstolen. Det er vanskelige å skulle se at en privatrettslig avtale står seg mot någjeldende amerikansk lovgivning, og derav er det nærliggende at også en ny avtale vil oppheves med tiden som følge av at den er inkompatibel med Personvernforordningen eller menneskerettighetscharteret.

[173] Linebaugh, Chris, Liu, Edwards (2021) s. 12
[174] Linebaugh, Chris, Liu, Edwards (2021) s. 12
[175] Linebaugh, Chris, Liu, Edwards s. 12
[176] Europakommisjonen og det amerikanske handelsdepartementet (2021)

Utarbeidelse av diplomatiske avtaler er egnet til å være tidkrevende. Dette gjør seg særlig gjeldende i situasjonen som den foreliggende, ettersom man har tilfeller hvor tidligere diplomatiske avgjørelser om det samme har blitt kjent ugyldig, og man vil nødig unngå et tilsvarende resultat denne gangen. I den prekære situasjonen vi står i nå, hvor lovgivning og praksis legger opp til omfattende vurderinger som selv de med juridisk bakgrunn kan finne utfordrende, er dette tid man kan diskutere om man rent faktisk har. Man snakker i prinsippet flere år før en slik avgjørelse vil være på plass, og i tråd med Personvernforordningen så må virksomheter som ønsker å overføre opplysninger til USA begi seg ut på den omfattende vurderingen og risikere ansvar dersom noe er misforstått.

Et fjerde alternativ, hvilket kanskje er det mest ønskelige sett med europeiske øyne, er at USA endrer lovgivningen sin på en slik måte at den i stor grad sammenfaller med det beskyttelsesnivået Personvernforordningen sikrer. Dette vil da kunne føre til at USA vil vurderes som et godkjent tredjeland i form av en adekvansbeslutning etter Personvernforordningen artikkel 45. Som følge av den verdien slik informasjon har for amerikansk etterretning, er det fjerde alternativet kanskje minst sannsynlig. Det vil også fremstå som svært urimelig dersom det kun er USA som må foreta endring ettersom lite av det minner om et samarbeid.

Slik situasjonen er per nå, så er det behov for overføring av personopplysninger til USA ettersom det er der de mest brukervennlige og mest tilgjengelige tjenesteleverandørene befinner seg. Hvordan en eventuell politisk løsning skal være, vil fordre en rekke diskusjoner og arbeidet med dette er overhodet ikke over. Slik jeg vurderer situasjonen vil det nok være nødvendig med endring i lovverket på amerikansk side, men det er noe usikkert om hele byrden er noe som skal bæres av USA alene. Frem til en slik eventuell politisk løsning er på plass, vil virksomheter som ønsker å foreta en overføring til USA foreta den vurdering som er gjennomgått over. Hvorvidt det lovlig kan overføres personopplysninger til USA, vil måtte bero på en konkret helhetsvurdering.

6 Litteraturliste

6.1 Litteratur

6.1.1 Bøker

Arnesen, Finn. Stenvik, Are *Internasjonalisering og juridisk metode – særlig om EØS-rettens betydning i norsk rett*. 2. utg. Oslo: Universitetsforlaget, 2015

Boe, Erik Magnus *Innføring i juss – juridisk tenkning og rettskildelære* 3. utg., Oslo: Universitetsforlaget, 2010

Bygrave, Lee A. *Data Privacy Law – An international Perspective*, 2. Utg., Oxford: Oxford University Press, 2014

Fredriksen, Halvard Haukeland. Mathisen, Gjermund *EØS-rett*. 2. utg. Bergen: Fagbokforlaget, 2014

Kuner, Christopher "Article 45. Transfers on the basis of an adequacy decision" i *The EU General Data Protection Regulation – A Commentary* Kuner, Christopher. Bygrave, Lee A., Docksey, Christopher red. 1. Utg. Oxford: Oxford University Press, 2020

Rainey, Bernadette. Wicks, Elizabeth. Ovey, Clare *Jacobs, White and Ovey: The European Convention on Human Rights*. 7. Utg. Oxford: Oxford University Press, 2017

Sejersted, Fredrik. Arnesen, Finn. Rognstad, Ole-Andreas m.fl. *EØS-rett*. 3. utg. Oslo: Universitetsforlaget, 2014

Skullerud, Åste Marie Bergseng, Rønnevik, Cecilie, Skorstad, Jørgen m.fl. *Personopplysningsloven og Personvernforordningen (GDPR) Kommentarutgave*. Oslo: Universitetsforlaget, 2019.

Aall, Jørgen *Rettsstat og menneskerettigheter* 5. utg. Bergen: Fagbokforlaget 2018

6.1.2 Artikler

Fefer, Rachel F., Archick, Kristin "U.S.-EU Privacy Shield*" *Current Politics and Economics of Europe; Hauppauge* Vol. 32, nr. 2/3 (2021) s. 263-269

Foss, Kristian. «Fra konsesjon til Schrems II – eksport av personopplysninger i det 21. århundre» *Lov & Data* årg. 21 nr. 1 (2021) s. 17-25 [Lest i lovdata.no]

Gonçalves, Maria Eduarda "The risk-based approach under the new EU data protection regulation: a critical perspective" Journal of Risk Research (2020) s. 139-152

Kuner, Christopher "Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection" Legal Studies Legal Studies Research Paper Series, University of Cambridge, Paper no. 20/2021 (April 2021)

Vanebro, Ove A., Gjerstad, Marianne "Schrems II: Faktisk risiko bør spille en rolle ved overføring av personopplysninger til tredjestater" Lov&Data nr. 145 (Mars 2021)

6.1.3 Nettsider

Bloemen, Annemarie "US surveillance practices and its legal system – a short history in light of Schrems II" (2021) https://www.advocatie.nl/content/uploads//Artikel-EU-US-Privacy-law-Annemarie-Bloemen-02.pdf Hentet 08.11.2021

Case, John "Zoom, Microsoft Team, and Slack have exploded due to the COVID-19 Pandemic. Can they hold onto this growth?" (2020) https://glginsights.com/articles/zoom-microsoft-teams-and-slack-have-exploded-due-to-the-covid-19-pandemic-can-they-hold-onto-this-growth/ Hentet 18.10.2021

Datatilsynet "Risikovurdering" (2019) https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/risikovurdering/ Hentet 21.10.2021

Datatilsynet. «Utfyllende veiledning om Schrems II» (2020) https://www.datatilsynet.no/regelverk-og-verktoy/internasjonalt/retningslinjer-og-uttalelser-fra-personvernradet/utfyllende-veiledning-om-schrems-ii/ Hentet 19.07.2021

Datatilsynet "Det Europeiske Personvernrådet (EDPB)" (2020) https://www.datatilsynet.no/regelverk-og-verktoy/internasjonalt/personvernradet/ Hentet 23.09.2021

Datatilsynet. «Overføring av personopplysninger ut av EØS» (2020) https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/sos-om-nye-regler-for-overforing/ Hentet 24.08.2021

De Santis, Federica, McCluskey, Curtis, Scott, Gretchen og Segalis, Boris "Europe OPTS for Pragmatism with New SCCS and ICO Opens Consultations on UK SCCS – What Companies Need to Do Next" (2021) https://www.jdsupra.com/legalnews/europe-opts-for-pragmatism-with-new-3698848/ Hentet 21.10.2021

Digital Europe "Response to draft EDPB Recommendations on supplementary measures for personal data transfers" https://www.digitaleurope.org/resources/response-to-draft-edpb-recommendations-on-supplementary-measures-for-personal-data-transfers/ Hentet 04.11.2021

Duball, Joseph "Getting acclimated with updated SCCs" (2021) https://iapp.org/news/a/getting-acclimated-with-updated-sccs/ Hentet 21.10.2021

EFTA "Commission Implementing Decision (EU) 2021/914 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council" (u.å.) https://www.efta.int/eea-lex/32021D0914 Hentet 22.11.2021

EU Monitor "Implementing decision" https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vkh7chz09fy8 Hentet 13.09.2021

Hill, Derek "Science and Engineering Indicators 2014" (2014) https://www.nsf.gov/statistics/seind14/index.cfm/front/f3.htm Hentet 18.10.2021

Jarbekk, Eva "Maybe you don't need the SCC?" (2021) https://www.schjodt.no/en/news--events/newsletters/maybe-you-dont-need-the-scc/ Hentet 13.09.2021

Judin, Thomas "Stressa for Schrems II? https://www.personvernbloggen.no/2021/09/03/stressa-for-schrems-ii/ Hentet 05.11.2021

Lee, Phil "Part 1: Getting to grips with US government requests for data" (2016) https://www.fieldfisher.com/en/insights/part-1-getting-to-grips-with-us-government-requests-for-data Hentet 11.10.2021

Linebaugh, Chris D. Liu, Edwars, C. “Congressional Research Service; EU Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield” (2021) https://crsreports.congress.gov/product/pdf/R/R46724 Hentet 05.11.2021

Mole, Ariane, Boardman, Ruth, Voisin, Gabriel "Replacement Standard Contractual Clauses (SSCs): European Commission publishes final text" (2021) https://www.twobirds.com/en/news/articles/2021/uk/replacement-standard-contractual-clauses Hentet 22.11.2021

Olsen, Thomas "Ny EU standardavtale for overføringer (SCC) – oppbygging, innhold og anvendelse i praksis" (2021) https://www.finansnorge.no/siteassets/kurs-og-konferanser/2021/nettverkssamling-september/presentasjoner/thomas-olsen-svw.pdf Hentet 08.11.2021

Regjeringen, "Hva EØS-avtalen omfatter" (2021) https://www.regjeringen.no/no/tema/europapolitikk/eos1/hva-avtalen-omfatter/id685024/ Hentet 11.11.2021

Rode, Ane, Sætre, Kjetil Wick, Ramse, Jostein, Ransedokken, Øyvind Eidissen "Endelig veileder om Schrems II fra Personvernrådet – større opning for risikobasert tilnærming" (2021) https://foyen.no/nyheter/endelig-veileder-om-schrems-ii-fra-personvernradet-storre-apning-for-risikobasert-tilnaerming/ Hentet 11.10.2021

Rosenthal, David "New EU Standard Contractual Clauses for Data Transfers to Non-Whitelisted Third Countries" (2021) https://www.rosenthal.ch/downloads/VISCHER-faq-scc-en.pdf Hentet 10.09.2021

Sandtrø, Jan «Oppdatering personvern, GDPR og teknologirett mv. (#6.2021)» (2021) https://sandtro.no/2021/06/15/oppdatering-personvern-gdpr-og-teknologirett-mv-6-2021/ Hentet 31.08.2021

Simmons + Simmons "Data Transfers: Final recommendations by the EU Data Protection Board (2021) https://www.simmons-simmons.com/en/publications/ckq84yqcg1cb40948jlahze5n/data-transfers-final-recommendations-by-the-eu-data-protection-board Hentet 11.10.2021

Thon, Bjørn Erik "Personvern i USA – part one" (2013) https://www.personvernbloggen.no/2013/02/11/personvern-i-usa-part-one/ Hentet 06.09.2021

Vengadesan, Joanne, Lovett, Dan, Pook, Nora "Schrems II: What now for international data flows?" (2020) https://www.penningtonslaw.com/news-publications/latest-news/2020/schrems-ii-what-now-for-international-data-flows Hentet 21.10.2021

Woods, Lorna "The AG Opinion in Schrems II: Facebook, national security and data protection law" (2019) http://eulawanalysis.blogspot.com/2019/ Hentet 21.10.2021

6.1.4 Rapporter og offisielle uttalelser

Archick, Kristin. Fefer, Rachel F. Fefer *U.S.-EU Privacy Shield and Transatlantic Data Flows* (R46917) (2021) på vegne av Congressional Research Service

Europakommisjonen og det amerikanske handelsdepartementet, *A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo* (2021)

National Academies, *Committee on responding to section 5 (D) of the Presidential Policy Directive 28: The feasibility of software to provide alternatives to bulk signals intelligence collection* (2015)

6.2 Norske rettskilder

6.2.1 Lovgivning

2018	Lov 15. juni 2018 nr. 38 om behandling av personopplysninger [Personopplysningsloven]
1992	Lov 27. november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) mv. (EØS-loven)

6.2.2 Lovforarbeider

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

6.2.3 Domsregister

Rt. 2005 s. 833

6.2.4 Offentlige dokumenter

Meld. St. 23 (2012-2013)	Digital agenda for Norge – IKT for vekst og verdiskaping

6.3 Internasjonale rettskilder

6.3.1 Traktater

EMK	*Konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter*, Roma 4. november 1950 [Offisiell norsk oversettelse].
TEU	*Traktaten om den Europeiske Union.* Konsolidert utgave 2016 (EUT 2016/C 202/01)
TEUF	*Traktaten om den Europeiske Unions funksjonsområde.* Konsolidert utgave 2016 (EUT 2016/C 202/01)

6.3.2 EU-direktiver, forordninger m.m.

Forordning 2016/679 EU	*Europaparlamentets- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveklings av slike opplysninger samt om oppheving av direktiv 95/46/EF* [GDPR] [Personvernforordningen]
EØS-avtalen	*Agreement on the European Economic Area.* Oporto, 2. mai 1992
ODA-avtalen	*Agreement between the EFTA States on the establishment of a surveillance authority and a court of justice, with protocols 1-7.*

6.3.3 Implementeringsbestemmelser

95/46/EC	*Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*
C/2016/4176	*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)
2018/EØS/46/04	*EØS-Komiteens beslutning nr. 154/2018 av 6. juli 2018 om endring av EØS-avtalens vedlegg XI (Elektronisk kommunikasjon, audiovisuelle tjenester og informasjonstjenester) og protokoll 37 om listen omhandlet i artikkel 101*
2021/914/EC	*Commission Implementing Decision (EU) 2021/914 of 4 june 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/697 on the European Parliament and of the Council* (Notified under document C/2021/3972) (Text with EEA relevance)

6.3.4 Veiledere, utkast m.m.

Recommendations 01/2020 vol. 1.0	*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (11. November 2020) (Høringsutkast – ikke vedtatt versjon)
Recommendations 01/2020 vol. 2.0	*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (18. Juni 2021) (Endelig vedtatt versjon)

Utkast Standard Contractual Clauses	*Commission implementing decision (EU) …/… of XXX on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council* (Text with EEA relevance)
EDPB-EDPS Joint opinion 2/2021	*EDPB-EDPS Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries for the matters referred to in Article 46 (2)(c) of Regulation (EU) 2016/679* (2021)
Guidelines 2/2020 version 2.0	*Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEa and non-EEA public authorities and bodies* (2020)
Guidelines 3/2018 version 2.1	*Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)* (2019)
Det europeiske datatilsynet	*Opinion of the European Data Protection Supervisor on the data protection reform package* (2012)
Det europeiske personvernrådet	*Minutes 54th Plenary meeting 14 September 2021, Remote* (2021)
Guidelines 05/2021	*Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR* (2021)

6.3.5 Internasjonalt domsregister

Sak C-101/01 Bodil Lindquist	ECLI:EU:C:2003:596
Sak C-362/14 Maximillian Schrems v Data Protection Commissioner	ECLI:EU:C:2015:650
Sak C-311/18 Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems	ECLI:EU:C:2020:559
Sak C-72/07 Blanco Pèrez and Chao Gòmez v Conserjaria de Salud y Santarios, Federaxon Empresarial de Farrmaceitocos Espanoles	ECLI:EU:C:2007:336
Forente saker C-293/12 og C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others	ECLI:EU:C:2014:238
Sak C-7/11 Fabio Caronna	ECLI:EU:C:2012:296
Sak E-2/94	*Scottish Salmon Growers Association Limited (SSGA) mot ESA*
Sak E-4/01	Karlsson mot Island
Sak C-11/70 Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Fyttermittel	ECLI:EU:C:1970:114
Sak C-623/17 Privacy International	ECLI:EU:C:2020:790
Sak C-511/18 La Quandrature du Net and Others	ECLI:EU:C:2020:791

6.4 Utenlandske (nasjonale) rettskilder

6.4.1 Amerikansk lovgivning

FISA	Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110-261 (kodifisert i spredte deler av 50 U.S.C.)
E.O. 12333	Federal Register Vol. 40, No. 235 (December 8, 1981), amended by E.O. 13284 (2003), E.O. 13355 (2004) og E.O. 13470 (2008)

6.4.2 Amerikansk domsregister

The United States Supreme Court	*Jane Roe v Henry Wade* 410 U.S. 113 (22.01.1973)