UiO : Det juridiske fakultet

Overføring av personopplysninger til tredjestater

Hvordan lovlig overføre personopplysninger til tredjestater og rekkevidden av overføringsbegrepet

Kandidatnummer: 531

Leveringsfrist: 9. mai 2023

Antall ord: 15924

Innholdsfortegnelse

1 Innledning

1.1 Presentasjon av tema og problemstilling

Temaet for avhandlingen er overføring av personopplysninger til tredjestater. Med «tredjestater» menes land utenfor EU/EØS-området, samt tredjestater, territorium eller en eller flere angitte sektorer i tredjestaten. Avhandlingens rettslige problemstilling er hvordan personopplysninger kan lovlig overføres til tredjestater etter personvernforordningen. En sentral underproblemstilling er hva som utgjør en overføring av personopplysninger til en tredjestat.

Den teknologiske utviklingen har muliggjort nye former for internasjonal handel. Personopplysninger deles nå verden rundt i et historisk høyt og sterkt voksende tempo.[1] Personopplysninger har blitt en integrert del av digitale tjenester, en viktig handelsvare og en forutsetning for den digitale økonomien.[2] Det har åpnet muligheter for innovasjon og forbedret produktivitet på tvers av landegrenser, og medført flere fordeler for næringsaktører så vel som enkeltpersoner. Parallelt med den positive utviklingen, har behovet for vern av personopplysninger økt betraktelig.[3] Fordelene med den teknologiske utviklingen kan virke fjerne sammenlignet med risikoen som misbruk av personopplysninger kan få for den enkelte, eksempelvis gjennom identitetstyveri, inngripende overvåkning, uønsket markedsføringskommunikasjon og diskriminering.[4]

På den bakgrunn etablerte EU forordning General Data Protection Regulation[5] (heretter «GDPR», «personvernforordningen» eller «forordningen») i 2018. Forordningen fastsetter regler om «vern av personer i forbindelse med behandling av personopplysninger samt regler om fri utveksling av personopplysninger», jf. GDPR artikkel 1 nr. 1. Reglene erstatter direktiv 95/46/EF[6] (heretter «personverndirektivet» eller «direktivet»). Direktivet ble ansett å ikke gi en tilstrekkelig beskyttelse av enkelt personers rettigheter med hensyn til moderne databehandlingsteknologier og en utilstrekkelig grad av harmonisering innad i EU, i tillegg til kontinuerlige

[1] Naef (2023) s. 19

[2] Se EU Kommisjonen (2023), analyse av det digitale markedet som forventer vekst.

[3] GDPR fortale punkt 6.

[4] Yakovleva (2020) s. 882.

[5] Forordning 2016/679 EU.

[6] Direktiv 95/46 EF.

utfordringer i håndteringen av globale dataflyter.[7] Ved å vedta reglene i forordningsform ble staters handlingsrom begrenset med formål å oppå rettslikhet i EU/EØS. Når personopplysninger overføres innad i EU/EØS er behandlingen underlagt reglene i GPDR samt regler på medlemsstatsnivå.[8] Når personopplysninger overføres ut av EU/EØS nyter de i utgangspunktet ikke samme vern.[9] Av den grunn inneholder kapittel V i personvernforordningen egne regler om overføring av personopplysninger til tredjestater. Bestemmelser i kapittelet oppstiller vilkår for å lovlig overføre personopplysninger til tredjestater, også kalt overføringsgrunnlag.

Avhandlingens tema fikk særlig stor oppmerksomhet etter at The European Court of Justice (heretter «EU-domstolen») i 2015 avsa dom i sak C-362/14 (heretter «Schrems I»).[10] Schrems I gjaldt overføring av personopplysninger til USA etter den tidligere Safe Harbour-avtalen. Safe Harbour var en adekvansbeslutning hjemlet i personverndirektivet som amerikanske selskap kunne sertifisere seg etter.[11] Klageren Maximilian Schrems anførte at overføringene var ulovlige begrunnet i utilstrekkelig beskyttelse av europeiske borgeres personopplysninger. EU-domstolen ga klageren medhold og krevde overføringene stanset. Safe Harbour-avtalen ble kjent ugyldig. I påvente av en ny adekvansbeslutningsavtale, ble standard personvernbestemmelser brukt som overføringsgrunnlag frem til EU Kommisjonen (heretter «EU Kommisjonen» eller «Kommisjonen») og USA inngikk Privacy Shield-avtalen i 2016.[12] Privacy Shield var igjen en adekvansbeslutningsavtale som amerikanske selskaper kunne sertifisere seg etter. Maximilian Schrems klaget saken inn for til EU-domstolen, og i sak C-311/18[13] (heretter «Schrems II») ble Privacy Shield-avtalen kjent ugyldig. Standard personvernbestemmelsene ble opprettholdt som overføringsgrunnlag, men de konkrete overføringene var ulovlige og måtte stanse.

Begrunnelsen for at overføringene ble funnet ulovlige i Schrems I og Schrems II til tross for overføringsgrunnlag hjemlet i direktivet og senere forordningen, var amerikansk lovgivning og praksis. Amerikanske myndigheters inngripende overvåkningslovgivning hjemlet i FISA 702[14]

[7] Naef (2023) s. 26 til 27.
[8] Regler på medlemstatsnivå i tråd med GDPR med visse tillatte unntak, se GDPR artikkel 23.
[9] Se EDPB Guidelines 05/2021 s. 5.
[10] Sak C-362/14.
[11] Decision 2000/520/EC vedlegg I.
[12] Decision 2016/1250/EU.
[13] Sak C-311/18.
[14] Foreign Intelligence Surveillance Act: Section 702, 50 U.S.C. § 1881 a.

og EO 12.333,[15] innebærer at amerikanske myndigheter kan pålegge selskaper i USA å utlevere personopplysninger i strid med adekvansbeslutninger og standard personvernbestemmelser. Nevnte overføringsgrunnlag er avtaler, og er som følge av deres kontraktsrettslige natur, ikke bindende for amerikanske myndigheter. EU-domstolen fant at amerikanske myndigheter i praksis ikke respekterte overføringsgrunnlagene som var utarbeidet for å sikre et tilstrekkelig beskyttelsenivå av personopplysninger til de registrerte.

Særlig Schrems II har medført diskusjoner i det juridiske fagmiljøet knyttet til avhandlingens tema ettersom EU-domstolen ikke bare ugyldiggjorde Privacy Shield-avtalen, men også fant standard personvernbestemmelser utilstrekkelige som overføringsgrunnlag. Etter avgjørelsen har EU Kommisjonen utarbeidet nye standard personvernbestemmelser.[16] Disse benyttes i dag i stor grad ved overføring av personopplysninger til USA. Dataeksportører er imidlertid usikre på hvordan slike overføringer kan utføres lovlig med hensyn til tredjestatsmyndigheter som ikke er bundet av overføringsgrunnlagene. Det har også skapt en diskusjon knyttet til rekkevidden av overføringsbegrepet.[17] Ettersom reglene i kapittel V kun kommer til anvendelse på overføringer av personopplysninger til tredjestater, er begrepets rekkevidde av stor betydning. Den teknologiske utviklingen innebærer at personopplysninger spres på utallige måter uten å overføres i tradisjonell forstand, eksempelvis ved opprettelse av datarom, publisering av personopplysninger på internett, fjerntilgang til systemer, mv. Teknologien utvikler seg raskt. Allerede neste år kan det foreligge nye verktøy og metoder som tas i bruk for å formidle personopplysninger på tvers av landegrenser. Lovgivningen på sin side har et tregere utviklingstempo. Dette har ført, og vil føre til, en rekke utfordringer da det forutsetter en regulering som hensyntar teknologier som ikke enda eksisterer. Avhandlingen vil med dette bakteppe søke å besvare to hovedproblemstillinger: (i) hva som utgjør en overføring av personopplysninger til tredjestater etter personvernforordningen og (ii) hvordan personopplysninger lovlig kan overføres til tredjestater etter personvernforordningen.

[15] Excecutive Order No. 12,333, 46 Federal Regulation 59,941-42 (4. desember 1981).
[16] Decision 2021/914/EU.
[17] Særlig om uenigheten mellom Digdir, DFØ og Datatilsynet se Datatilsynet (2022).

1.2 Rettskilder og metodiske utfordringer

For å besvare avhandlingens problemstillinger vil det tas utgangspunkt i de rettigheter og plikter som fremgår direkte av personvernforordningen. Forordningen er bindende for EUs 28 medlemsstater, samt EFTA-landene Norge, Island og Liechtenstein, jf. EØS-avtalens vedlegg XI nr. 5e. EØS-avtalens hoveddel er gjennomført i norsk lov gjennom EØS-loven.[18] Forordningen er gjennomført i norsk rett ved inkorporasjon, jf. personopplysningsloven § 1.[19] I EU trådte forordningen i kraft den 25. mai 2018 og i Norge den 20. juli 2018.[20]

Tolkning av forordningen må ta utgangspunkt i EU-rettslig metode, slik den er etablert og utviklet gjennom EU-domstolens rettspraksis. Utgangspunkt må tas i en naturlig språklig forståelse av ordlyden, sammenholdt med dens kontekst og formål.[21] Ordlyden har stor vekt, med de begrensninger som følger av harmoniseringsprinsippet og ulike språkversjoner.[22] Alle språk regnes som autentiske, jf. EØS-avtalens artikkel 129. Den norske teksten er derfor likestilt med for eksempel engelsk og fransk, og vil benyttes i avhandlingen. Med formål siktes det til det objektive formålet, slik den særlig kan utledes av forordningens fortale.[23] Forordningens fortale er derfor sentral og redegjør for hvordan bestemmelser skal tolkes og forstås.[24] Dens funksjon er tilsvarende forarbeiders funksjon ved tolkning av norsk lovtekst. Tolkning av personvernforordningen er videre styrt av prinsippet om teknologisk nøytralitet med formål å hindre omgåelse av regelverket ved utvikling av nye teknologier.[25]

Forarbeider er av mindre betydning for tolkning av personvernforordningen enn vi er vant med i norsk rett, og skal anvendes med forsiktighet.[26] EU-domstolen viser ikke til forarbeider ved tolkning av traktater.[27] Ettersom personvernforordningen er innført i norsk rett gjennom inkorporasjon, er det begrenset med nasjonale forarbeider. Som følge av harmoniseringsprinsippet

[18] EØS-loven § 1.
[19] Med tilpasninger, se Protokoll 1 til EØS-avtalen artikkel 8 og 9.
[20] Skullerud mfl. (2019) s. 368.
[21] Se eksempelvis Sak C-480/10 avsnitt 33.
[22] Arnesen (2015) s. 31.
[23] Ibid s. 36.
[24] Sejersted (2011) s. 57.
[25] GDPR fortale punkt 15.
[26] Arnesen (2015) s. 37.
[27] Ibid s. 37.

vil ikke disse tillegges vekt. På europeisk nivå finnes det ikke forarbeider i tradisjonell forstand. Referater fra forhandlinger i Rådet og EU Kommisjonen ved utarbeidelse av forordningen er ikke tilgjengelige.[28]

Det er begrenset rettspraksis fra EU-domstolen tilknyttet personvernforordningen av 2018. Ettersom forordningen i stor grad viderefører direktivet, anses praksis fra EU-domstolen tilknyttet direktivet som relevant for avhandlingen.

EU-domstolen viser i økende grad til Den europeiske unions pakt om grunnleggende rettigheter og friheter[29] (heretter «EU pakten eller «Pakten») ved tolkning av EU-retten.[30] Det følger av artikkel 1 nr. 2 i personvernforordningen at forordningen skal sikre «vern av fysiske personers grunnleggende rettigheter og friheter». Det siktes her til de grunnleggende rettigheter og friheter hjemlet i EU pakten, særlig retten til personvern etter artikkel 8, jf. GDPR fortale punkt 1 til 4. Forordningens bestemmelser må i seg selv ses som et uttrykk for en forholdsmessig avveining mellom de ulike rettighetene og frihetene i EU pakten.[31] Ved tolkningstvil kan imidlertid andre hensyn hjemlet i Pakten tillegges vekt.

Personvernforordningen åpner for å begrense forordningens rekkevidde på bestemte områder, jf. GDPR artikkel 23. Det gjelder ikke reglene om overføring av personopplysninger til tredjestater i kapittel V, jf. artikkel 23 nr. 1. Følgelig vil ikke personopplysningens bestemmelser vies oppmerksomhet i avhandlingen. Nasjonal forvaltnings- og rettspraksis har som følge av harmoniseringsprinsippet begrenset betydning og vil først og fremst benyttes i den grad tolkning av forordningen er utført av faglig dyktige individer.

Det er begrenset med juridisk litteratur tilknyttet avhandlingens problemstillinger. Det kommer imidlertid stadig ut nye retningslinjer og uttalelser fra europeiske organer. Disse rettskildene er ikke juridisk bindende, men vil tillegges mer vekt enn det som følger av alminnelig juridisk metode, ettersom de er utarbeidet med formål å sikre en felles forståelse av personvernforordningen innad i EU/EØS.

[28] Skullerud mfl. (2019) s. 44.

[29] EU pakten.

[30] Se EU Kommisjonen (u.å.) a.; årlige rapporter om anvendelsen (og styrking) av EU pakten i EU.

[31] Skullerud mfl. (2019) s. 137.

Rettskildene det siktes til er særlig retningslinjer utarbeidet av European Data Protection Board (heretter «EDPB» eller «Personvernrådet»). Personvernrådet ble etablert 25. mai 2018 og erstattet Artikkel 29-gruppen (heretter «A29-gruppen» eller «A29WP»). A29-gruppen var EUs rådgivende organ i personvernspørsmål tilknyttet direktivet. Personvernrådet har gitt sin tilslutning til A29WP veiledere,[32] i tillegg til å utarbeide egne. EDPB har som oppgave å «sikre ensartet anvendelse» av personvernforordningen, jf. Artikkel 70 nr. 1 første punktum. Selv om rettskildene ikke er juridisk bindende, har de stor faktisk betydning da deres formål ikke bare er å gi veiledning til identifiseringer og overføring av personopplysninger etter GDPR, men også sørge for en konsistent tolkning og anvendelse av reglene av tilsynsmyndighetene i medlemsstatene.[33] Datatilsynet (den norske tilsynsmyndigheten)[34] har uttalt at de vil tolke personvernforordningen likt som EDPB i en eventuell tilsynssak.[35]

Rettskilder fra EU Kommisjonen vil benyttes i avhandlingen. Her siktes det særlig til de nye standard personvernbestemmelsene utarbeidet av Kommisjonen i 2021.[36]

1.3 Avgrensninger

Det foreligger en rekke beslektede problemstillinger knyttet til temaet overføring av personopplysninger til tredjestater. For å behandle de utvalgte problemstillingene grundig, må det foretas avgrensninger.

Avgjørelser fra EU-domstolen og EU pakten er ikke direkte bindende for Norge.[37] Homogenitetsprinsippet innebærer imidlertid at EØS-regelverk som er hentet fra EU-retten må tolkes og anvendes slik at rettstilstanden blir den samme i EØS som i EU.[38] Prinsippet kommer til uttrykk gjennom EØS-avtalens fortale hvor det heter at «avtalepartenes formål [..] er å nå frem til og opprettholde en lik fortolkning og anvendelse av denne avtale og de bestemmelser i

[32] "*During its first plenary meeting the European Data Protection Board endorsed the GDPR related WP29 Guidelines"*. Sitat hentet fra EDPB (u.å.).

[33] EDPB Retningslinjer 05/2021 s. 6.

[34] Personopplysningsloven § 20, jf. GDPR artikkel 51.

[35] «*Datatilsynet vil tolke loven likt som EDPB i en eventuell tilsynssak*». Sitat hentet fra Datatilsynet (2023).

[36] Decision 2021/914/EU.

[37] EU pakten er ikke en del av EØS-avtalen.

[38] Fredriksen og Mathisen (2018) s. 50.

Fellesskapets regelverk som i det vesentlige er gjengitt i denne avtale».[39] Videre har flere grunnleggende rettigheter i EU pakten sin parallell i Den europeiske menneskerettskonvensjon.[40] Da avhandlingen tar sikte på å analysere gjeldende EU-rett, vil det avgrenses fra å behandle særskilte EØS-rettslige spørsmål. Den europeiske menneskerettskonvensjonen vil heller ikke benyttes i avhandlingen.

Personvernforordningens regler om overføring av personopplysninger til tredjestater gjelder tilsvarende for overføring av personopplysninger til internasjonale organisasjoner, jf. artikkel 44 første punktum. Det avgrenses imidlertid mot å behandle overføringer av personopplysninger til internasjonale organisasjoner, da slike overføringer antas begrenset i antall sammenlignet med overføringer til tredjestater.

Kapittel V i personvernforordningen gir alternative overføringsgrunnlag. Utgangspunktet er adekvansbeslutninger etter artikkel 45. Dersom det ikke foreligger en adekvansbeslutning, kan overføringer skje i form av «nødvendige garantier», jf. artikkel 46. Foreligger det verken en adekvansbeslutning eller nødvendige garantier, kan overføring finne sted på grunnlag av rettslige avgjørelser avsagt av domstoler eller administrative myndigheter, forutsatt at avgjørelsen bygger på en internasjonal avtale, jf. artikkel 48. Helt unntaksvis kan overføring skje på grunnlag av samtykke- eller nødvendighetsbetraktninger etter artikkel 49.[41] Det avgrenses fra å behandle samtlige overføringsgrunnlag, til å behandle de overføringsgrunnlag som blir brukt mest i praksis. Avhandlingen vil derfor kun behandle adekvansbeslutninger etter artikkel 45 og standard personvernbestemmelser etter artikkel 46 nr. 2 bokstav c, som EU-domstolen drøftet i Schrems II.

Avslutningsvis avgrenses det mot rettsavgjørelser fra EU-domstolen, retningslinjer og uttalelser fra EDPB, uttalelser fra EU Kommisjonen og veiledere fra Datatilsynet som utgis etter den 31. mars 2023. Denne avgrensningen er foretatt som følge av at avhandlingen bygger på rettskildebildet før nevnte dato og rettstilstanden vil kunne endre seg basert på nye rettskilder etter nevnte dato.

---

[39] EØS-avtalens fortale, femtende betraktning.

[40] Retten til privatliv er forankret i EMK artikkel 8 og Grunnloven § 102. Personvernet er innfortolket i denne rettigheten. Se eksempelvis S. and Marper v. The United Kingdom avsnitt 67.

[41] Personvernrådet har uttalt at unntaksadgangen skal tolkes strengt, se EDPB Guidelines 2/2018 s. 4.

1.4 Fremstillingen videre

Den videre fremstillingen vil søke å besvare avhandlingens problemstillinger ved først å redegjøre for forordningens sentrale begreper og grunnleggende prinsipper. Redegjørelsen vil foretas i kapittel 2 og danne grunnlag for den videre analysen. Kapittelet er ment å belyse relevante regler som foreligger ved behandling av personopplysninger, uten at overføringsreglene kommer til anvendelse. I avhandlingens kapittel 3 vil overføringsbegrepets rekkevidde analyseres. Formålet bak analysen er å redegjøre for hvilke operasjoner som er underlagt reglene i kapittel V i personvernforordningen. I kapittel 4 vil det søkes å besvare hvordan personopplysninger lovlig kan overføres til tredjestater ved bruk av adekvansbeslutninger eller standard personvernbestemmelser, i lys av Schrems II. I avhandlingens avsluttende del vil det konkluderes, samt gis betraktninger knyttet til funn i avhandlingen som det er særlig grunn til å trekke frem.

2 Personvernforordningen

2.1 Personopplysninger og rettighetssubjekter

Personvernforordningen fastsetter regler om «personopplysninger» jf. GDPR artikkel 1 nr. 1. Artikkel 4 legaldefinerer en rekke sentrale begreper i GDPR, inkludert begrepet «personopplysninger», som defineres som «enhver opplysning om en identifisert eller identifiserbar fysisk person».[42]

Med «enhver opplysning» menes all tenkelig informasjon uavhengig av art, innhold og form.[43] Objektive og subjektive opplysninger er omfattet.[44] Opplysningene må ikke være objektivt verifiserbare, subjektive meninger og feilaktige opplysninger er omfattet.[45] Opplysningenes format er uten betydning, de kan komme til uttrykk gjennom tall, tegninger, fotografier, lyd, biometriske tegn, mv.[46]

Tilknytningskravet «om» innebærer at opplysningene må handle om eller angå en fysisk person.[47] Det forutsetter ikke en direkte tilknytning, jf. artikkel 4 nr. 1. Også indirekte opplysninger kan knyttes til en fysisk person.

Begrepet «fysisk person» avgrenser personopplysningsbegrepet mot opplysninger om juridiske personer, eksempelvis selskaper. Opplysninger om juridiske personer kan imidlertid omfattes av personopplysningsbegrepet, i den grad opplysningene kan knyttes til fysiske personer.[48] Opplysninger om avdøde er i utgangspunktet ikke omfattet av begrepet, da avdøde ikke regnes som en fysisk person.[49] Opplysninger om avdøde kan likevel utgjøre personopplysninger om *andre* identifiserbare fysiske personer, eksempelvis opplysninger om arvelige sykdommer.[50]

---

[42] GDPR artikkel 4 nr. 1.
[43] Skullerud mfl. (2019) s. 151.
[44] Ibid.
[45] Ibid.
[46] Ibid.
[47] Ibid.
[48] A29WP Opinion 4/2007 s. 23 til 34.
[49] GDPR fortale punkt 27, 158 og 160.
[50] A29WP Opinion 4/2007 s. 22.

Å være «identifisert» innebærer at en fysisk person er gjort til kjenne gjennom opplysningene. Personopplysningsbegrepet omfatter også opplysninger om en «identifiserbar» fysisk person. Det innebærer at det ikke stilles krav til at den fysiske personen faktisk er identifisert. Mulighet for identifikasjon, direkte eller indirekte, er omfattet, jf. artikkel 4 nr. 1.

Gjennomgangen viser at personopplysningsbegrepet er vidt og omfatter en rekke opplysninger. Anonymiserte opplysninger er ikke personopplysninger, ettersom slike opplysninger ikke kan brukes til å identifisere en enkeltperson.[51] Hvorvidt det overhodet er mulig å anonymisere opplysninger er imidlertid en diskusjon, særlig i digitale sammenhenger.[52] Krypterte og pseudonymiserte[53] opplysninger er ikke anonymiserte opplysninger, da de gjennom bruk av krypteringsnøkkel eller indikatorer kan brukes til å identifisere en fysisk person.[54] I vurderingen av om den fysiske personen kan identifiseres, skal det tas hensyn til «alle midler som det med rimelighet kan tenkes» tas i bruk.[55] Det går følgelig en grense for hvilke midler som skal tas med i vurderingen. Muligheten for at noen begår forbudte handlinger for å identifisere en fysisk person, kan man se bort ifra.[56]

En identifisert eller identifiserbar fysisk person omtales som «den registrerte», jf. artikkel 4 nr. 1. Det er de/den registrerte som er personvernforordningens rettighetssubjekter. Juridiske personer og avdøde er ikke rettighetssubjekter, jf. ovenfor. Videre har personvernforordningen et geografisk virkeområde, jf. artikkel 3. Det innebærer at rettighetssubjektene er avgrenset fra enhver identifisert eller identifiserbar fysisk person i verden. Rettighetssubjektene er imidlertid ikke avgrenset til å kun omfatte statsborgere i EU- og EØS-land. Det følger av ordlyden i artikkel 3 nr. 2 at det avgjørende er om den registrerte «befinner seg i» EU/EØS. Det bekreftes av fortalen der det heter at beskyttelsen forordningen gir bør gjelde fysiske personer uansett nasjonalitet eller bosted.[57] Videre vil øvrige identifiserte eller identifiserbare fysiske personer som befinner seg utenfor EU/EØS nyte et indirekte vern, dersom behandlingen av deres

[51] GDPR fortale punkt 26.

[52] Skullerud mfl. (2019) s. 153.

[53] Definert i artikkel 4 nr. 5 som «behandling av personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til en bestemt registrert uten bruk av tilleggsopplysninger, forutsatt at nevnte tilleggsopplysninger lagres atskilt og omfattes av tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til en identifisert eller identifiserbar fysisk person».

[54] Datatilsynet (2015) s. 9 til 10 og GDPR fortale punkt 26.

[55] GDPR fortale punkt 26.

[56] Sak C-582/14 avsnitt 46.

[57] GDPR fortale punkt 14.

personopplysninger utføres i forbindelse med aktiviteten ved virksomheten til en behandlingsansvarlig eller databehandler i EU/EØS, jf. artikkel 3 nr. 1. Den behandlingsansvarlige eller databehandleren vil i så tilfelle være underlagt reglene i GDPR ved behandling av deres personopplysninger.

GDPR gir følgelig rettigheter til tredjestatsborgere. Det er en utvidelse av personkretsen og en betydelig forskjell fra andre staters lovgivning. Amerikansk personvernlovgivning gir eksempelvis bare rettigheter til amerikanske statsborgere.[58] Dette innebærer at dersom personopplysninger om en europeisk statsborger overføres til USA, vil ikke den europeiske statsborgerens personopplysninger være beskyttet av det regelverket som beskytter amerikanske borgeres personopplysninger.

2.2 Grunnleggende prinsipper

Personvernforordningens regler bygger på grunnleggende prinsipper som nedfelt i personvernforordningens kapittel II. Overføring av personopplysninger til tredjestater må være i tråd med de grunnleggende prinsippene, da overføring er en form for behandling av personopplysninger, jf. artikkel 4 nr. 2. Operasjoner som ikke utgjør en overføring er underlagt forordningen i den grad de utgjør en behandling.[59] Prinsippene utgjør sentrale tolkningselementer for øvrige bestemmelser i personvernforordningen.[60]

Etter artikkel 5 nr. 1 følger det at behandling av personopplysninger må være lovlig, åpen og rettferdig (bokstav a), formålsbegrenset (bokstav b), adekvat, relevant og begrenset til det som er nødvendig (bokstav c), korrekte og om nødvendig oppdaterte (bokstav d), lagringsbegrenset og samtidig sikre integritet og konfidensialitet til de registrerte (bokstav e) og behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysninger, herunder vern mot uautorisert eller ulovlig behandling (bokstav f).

Kravet om lovlighet innebærer at behandlingen må ha en hjemmel, jf. artikkel 6, 9 og 10. Forordningens artikkel 6 gir en uttømmende liste over alternative vilkår som må oppfylles for at

[58] Krzysztofek (2021) s. 246.
[59] Se kapittel 2.3.
[60] Skullerud mfl. (2019) s. 172.

behandlingen er lovlig, jf. artikkel 6 nr. 1. Behandling av «særlige kategorier» av personopplysninger forutsetter at ytterligere vilkår er oppfylt, jf. artikkel 9. Særlige kategorier av personopplysninger er opplistet i artikkel 9 nr. 1. Behandling av slike opplysninger er i utgangspunktet forbudt med mindre et av vilkårene i artikkel 9 nr. 2 er oppfylt, jf. artikkel 9 nr. 1. Begrunnelsen for ytterligere vilkår, er et sterkere behov for vern av særlige kategorier av personopplysninger.[61]

2.3 Behandling av personopplysninger og pliktsubjekter

Personvernforordningen regulerer «behandling» av personopplysninger, jf. artikkel 1 nr. 1. Etter GDPR artikkel 4 nr. 3 er «behandling» definert som «enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger». Bestemmelsen har en ikke uttømmende liste over behandlingsoperasjoner, deriblant «utlevering ved overføring, spredning eller andre former for tilgjengeliggjøring».

Det skal lite til før en aktivitet utført i tilknytning til personopplysninger er omfattet av behandlingsbegrepet.[62] I praksis vil behandling omfatte enhver tenkelig håndtering av personopplysninger der elektroniske hjelpemidler er involvert.[63] Teknologiske fremskritt sannsynliggjør utvikling av nye behandlingsoperasjoner. Forordningens dynamiske karakter og tolkningsprinsippet om teknologisk nøytralitet, gjør reglene i stand til å imøtegå den teknologiske utviklingen og regulere nye behandlingsoperasjoner.[64] Dette vil hindre omgåelse av regelverket.

Personvernforordningen opererer med begrepene «behandlingsansvarlig» og «databehandler». Skillet mellom behandlingsansvarlig og databehandler er ikke sentralt i denne sammenheng. Reglene i kapittel V retter seg både mot den behandlingsansvarlige og databehandleren, jf. artikkel 44 første punktum. Det er imidlertid den behandlingsansvarlige som er ansvarlig for å påvise at deres plikter er overholdt etter artikkel 5 nr. 2. Dette omtales som ansvarlighetsprinsippet.[65]

[61] GDPR fortale punkt 71.
[62] Skullerud mfl. (2019) s. 153.
[63] Hauglid (2022).
[64] Se kapittel 1.2.
[65] Datatilsynet (2019).

Utover de grunnleggende prinsippene oppstiller forordningen en rekke plikter for behandlingsansvarlige og databehandlere. Sentralt å belyse i denne sammenheng er pliktene som følger av artikkel 24, 28 og 32. Etter artikkel 24 plikter den behandlingsansvarlige å gjennomføre egnede tiltak ved behandling av personopplysninger i lys av «behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter». Etter artikkel 28 nr. 1 plikter den behandlingsansvarlige å bare bruke databehandlere som gir tilstrekkelige garantier «som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordning og vern av den registrertes rettigheter». Etter artikkel 28 nr. 3 plikter behandlingsansvarlige og databehandlere å inngå en databehandlingsavtale, som blant annet skal innebærer at databehandleren plikter å gjøre tilgjengelig all informasjon som er nødvendig for den behandlingsansvarlige for å vurdere at forpliktelser i bestemmelsen er oppfylt. Etter artikkel 32 plikter både den behandlingsansvarlige og databehandleren å gjennomføre egnede tiltak «for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen» ved behandling av personopplysninger.

De fleste behandlingsansvarlige og databehandlere som er underlagt personvernforordningen er etablert i EU/EØS, jf. artikkel 3 nr. 1. Artikkel 3 nr. 2 utvider imidlertid det geografiske virkeområdet til å omfatte behandlingsansvarlige og databehandlere etablert utenfor EU/EØS, dersom i) behandlingen er knyttet til tilbud av varer eller tjenester til de registrerte i EU/EØS eller ii) behandlingen innebærer monitorering av de registrertes atferd i den grad atferden finner sted i EØS-området.

De registrerte er i utgangspunktet verken behandlingsansvarlig eller databehandler, jf. artikkel 4 nr. 10 som oppstiller et skille mellom behandlingsansvarlige, databehandlere og den registrerte. De registrerte kan imidlertid være behandlingsansvarlige eller databehandler i næringssammenheng, eksempelvis ved enkeltpersonforetak. I juridisk teori er det lagt til grunn at den enkelte står fritt til å behandle opplysninger som utelukkende gjelder vedkommende selv, uavhengig av om opplysningene behandles for personlige eller familiemessige aktiviteter, eller for andre formål.[66] Det er ikke klart hvor grensen går. Behandling av personopplysninger utført av fysiske personer som ledd i rent personlige eller familiemessige aktiviteter, faller imidlertid utenfor personvernforordningens saklige virkeområde, jf. artikkel 2 nr. 2 bokstav c. Følgelig

[66] Skullerud mfl. (2019) s. 140.

kan fysiske personer fritt behandle og overføre personopplysninger om seg selv til tredjestater i rent personlige eller familiemessige aktiviteter uten å være underlagt personvernforordningens regler.

3 Hva utgjør en overføring av personopplysninger til en tredjestat etter personvernforordningen?

3.1 Innledende bemerkninger

Det rettslige utgangspunktet for reglene om overføring av personopplysninger til tredjestater er inntatt i kapittel V i personvernforordningen. Etter artikkel 44 første punktum gjelder reglene i kapittelet for «[e]nhver overføring av personopplysninger […] til en tredjestat». Hverken kapittelet eller forordningen inneholder en definisjon av begrepet «overføring». Overføring er kun beskrevet som en av flere måter å behandle personopplysninger på, jf. artikkel 4 nr. 2. Da reglene kommer til anvendelse på overføringer, er begrepets rekkevidde av stor betydning. I punkt 3.2 vil det søkes å besvare hva som utgjør en overføring av personopplysninger til tredjestater i lys av ordlyd, rettspraksis, formål, retningslinjer og hensyn. Artikkel 44 inneholder imidlertid flere elementer enn begrepet «overføring» som vil kommenteres innledningsvis.

Kapittel V regulerer overføringer av «personopplysninger», jf. artikkel 44. Det innebærer at anonymiserte opplysninger faller utenfor kapittelets virkeområde, så vel som forordningen som helhet.[67] Å utvikle et verktøy som oppnår fullstendig anonymisering av personopplysninger, vil være svært verdifullt for behandlingsansvarlige, databehandlere og de registrerte. Ettersom anonymiserte opplysninger ikke kan knyttes til en fysisk person, vil det ikke foreligge en risiko for personvernet til de registrerte. For behandlingsansvarlige og databehandlere vil et slikt verktøy være tids- og arbeidsbesparende, ettersom behandlingen ikke vil være underlagt forordningens regler.[68]

Artikkel 44 retter seg mot «den behandlingsansvarlige eller databehandleren». Det innebærer at overføringer utført av de registrerte selv, faller utenfor kapittelets virkeområde.[69] Det vil være tilfellet dersom en registrert bestiller varer direkte fra en tredjestat og i den sammenheng overfører egne personopplysninger.[70] Det må holdes atskilt fra de tilfeller der en registrert bestiller

[67] Se kapittel 2.1.

[68] Se kapittel 4, særlig kapittel 4.3.

[69] Se kapittel 2.3.

[70] Tilsvarende er lagt til grunn av Personvernrådet, se EDPB Guidelines 05/2021 s. 8. Behandling av personopplysninger utført av fysiske personer som ledd i rent personlige eller familiemessige aktiviteter faller videre utenfor forordningen som helhet, jf. GDPR artikkel 2. nr. 2 bokstav c.

varer fra et selskap i EØS, som har varelager eller lignende i en tredjestat, og selskapet overfører personopplysninger til varelageret i tredjestaten for å fullføre bestillingen. Forutsetningen er at den registrerte bestiller varen direkte fra tredjestaten.

Artikkel 44 regulerer overføringer til en «tredjestat». Som nevnt kan behandlingsansvarlige eller databehandlere utenfor EU/EØS være underlagt personvernforordningen etter artikkel 3 nr. 2.[71] Det har derfor blitt stilt spørsmål til hvorvidt overføring til en dataimportør i en tredjestat som er underlagt forordningen, er omfattet av reglene i kapittel V.[72] Dataimportøren vil da være underlagt GDPR for behandlingen av personopplysningene, på lik linje med selskaper etablert i EU/EØS. Personvernforordningens artikkel 44 skiller ikke mellom overføring til dataimportører som er underlagt forordningen og de som ikke er det. Overføringer til dataimportører i tredjestater som er underlagt GPDR er derfor omfattet av reglene i kapittel V.[73] Begrunnelsen for at reglene kommer til anvendelse selv om dataimportører er underlagt reglene i GDPR, er at tredjestatsmyndigheter ikke er det.[74] Det foreligger da en risiko for tredjestaters innblanding, som illustrert av Schrems I og Schrems II. Denne risikoen må imøtegås ved å benytte seg av overføringsgrunnlagene i kapittel V.

3.2 Overføringsbegrepet

3.2.1 Ordlyden

Etter en naturlig språklig forståelse innebærer overføring at det skjer en form for aktivitet der opplysninger blir flyttet fra et sted til et annet. Ordlyden tar ikke direkte sikte på fysisk overføring (eksempelvis fra en server til en annen), men omfatter også overføringer fra en person til en annen i form av ervervelse av kunnskap. I likhet med begrepet «behandling», er ikke selve operasjonen avgjørende for om det finner sted en overføring eller ikke.[75] Reglene må gjelde uavhengig av format, og inkluderer sending av personopplysninger via e-post, gi noen tilgang til en kundedatabase, samt utveksling av data i form av et skriftlig dokument.

[71] Se kapittel 2.3.
[72] University of Lyon (2022).
[73] Tilsvarende er lagt til grunn av Personvernrådet, se EDPB Guidelines 05/2021 s. 6.
[74] EDPB Guidelines 05/2021 s. 12.
[75] Se kapittel 2.2.

Etter artikkel 44 siste punktum følger det at «[a]lle bestemmelser i dette kapittelet skal få anvendelse for å sikre at nivået for vern av fysiske personer som garanteres i denne forordning, ikke skal undergraves». Overføringsbegrepet må tolkes i lys av nevnte formål. Et overføringsbegrep som innebærer at nivået for vern av fysiske personer undergraves vil være i strid med bestemmelsens ordlyd. I hvor stor grad formålet skal legge føringer for begrepstolkningen, er imidlertid usikkert.

Artikkel 44 regulerer overføringer «til en tredjestat». Det innebærer etter en naturlig språklig forståelse at mottakeren av personopplysningene må befinne seg utenfor EU/EØS. Artikkel 44 bruker ikke begrepet «mottaker», men en overføring forutsetter en mottaker. Å være «mottaker» er definert i GDPR artikkel 4 nr. 9 som «en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som personopplysninger *utleveres til*, enten det dreier seg om en tredjepart eller ikke» (min kursivering). Det er ikke gitt at mottakeren av personopplysninger i en tredjestat skal forstås likt som en mottaker av personopplysninger etter artikkel 4 nr. 9.[76] Artikkel 44 bruker begrepet overført, ikke utlevert. Begrepene har imidlertid til felles at mottakeren får en form for kontroll eller mulighet til å behandle opplysningene.

Overføring forutsetter følgelig at mottakeren i tredjestaten får en form for kontroll eller tilgang til personopplysningene. Det innebærer at rene transitt-tilfeller faller utenfor kapittel V sitt virkeområde.[77] Med transitt menes her enheter som fungerer som et mellomledd for overføringer. Enheter i tredjestater kan fungere som transitt, ved at personopplysninger blir overført fra et land i EU/EØS til et annet i EU/EØS, via en ruter eller lignende som befinner seg i en tredjestat. Når enheten i tredjestaten kun fungerer som transitt, er ikke overføringen underlagt reglene i kapittel V. Mottakeren av personopplysningene vil befinne seg i EU/EØS. Enheten i tredjestaten er et mellomledd, under forutsetning av at enheten ikke får kontroll eller tilgang til personopplysningene. Bakgrunnen for dette er at dersom enheten verken får kontroll eller tilgang til personopplysningene, vil ikke risikoen for at personvernet til de registrerte realiseres som følge av utilstrekkelig beskyttelsesnivå i en tredjestat. Risikoen som foreligger når man overfører personopplysninger til en annen EU/EØS-stat via en ruter i en tredjestat er eksempelvis hackingforsøk. Denne risikoen foreligger også når personopplysninger behandler innad i EU/EØS.

[76] Krzysztofek (2021) s. 248.

[77] I slike tilfeller vil det heller ikke skje en «behandling» i tredjestaten, se kapittel 2.3.

3.2.2 Rettspraksis

Det foreligger som nevnt begrenset med rettspraksis fra EU-domstolen knyttet til overføringsbegrepet. I sak C-101/01[78] (heretter «Lindqvist») avgjorde EU-domstolen i 2003 spørsmålet om publisering av personopplysninger på en nettside i Sverige var en overføring av personopplysninger etter reglene i direktivets kapittel IV.[79] Domstolen konkluderte med at å publisere personopplysninger på internett, ikke utgjorde en overføring av personopplysninger til en tredjestat.[80]

Begrunnelsen for EU-domstolens konklusjon i Lindqvist-dommen, var for det første den tekniske karakteren av de operasjoner som ble utført. Det ble lagt vekt på at personopplysningene ikke automatisk ble sendt til tredjestater ved publiseringen på den svenske nettsiden, men forutsatte at individer i tredjestater aktivt gikk inn på nettsiden for å få tilgang til opplysningene.[81] Videre så domstolen hen til lovgiverintensjonen. Retten uttalte at med tanke på utviklingen av internett på det tidspunkt personverndirektivet ble utarbeidet, og mangel på kriterier for bruk av internett i kapittel IV, kunne man ikke anta at det var lovgivers intensjon at reglene skulle regulere publisering av personopplysninger på internett.[82] Domstolen så også hen til konsekvensbetraktninger, og uttalte at dersom publisering på internett skulle være omfattet av overføringsbegrepet, ville enhver gang personopplysninger publiseres på internett være en overføring til en tredjestat.[83] Det ville innebære at medlemsstater ville være forpliktet til å forhindre publisering av personopplysninger på internett dersom Kommisjonen finner at kun en tredjestat ikke sikret et tilstrekkelig beskyttelsesnivå.[84]

Det er grunn til å rette noe kritikk mot avgjørelsen, særlig uttalelsen om at medlemsstater ville være forpliktet til å forhindre all publisering av personopplysninger på internett dersom operasjonen skulle være omfattet av overføringsbegrepet. Uttalelsen er lite nyansert da personverndirektivets saklige virkeområde var begrenset. Etter direktivets artikkel 3 nr. 2 følger det at

[78] Sak C-101/01.
[79] Ibid avsnitt 52.
[80] Ibid avsnitt 71.
[81] Ibid avsnitt 60 til 61.
[82] Ibid avsnitt 68.
[83] De tredjestater med tekniske midler nødvendige for å få tilgang til opplysningene, se Sak C-101/01 avsnitt 69.
[84] Sak C-101/01 avsnitt 69.

direktivet ikke regulerer behandling av personopplysninger «som utføres i forbindelse med offentlig sikkerhet, forsvar, statens sikkerhet [...] og statens virksomhet på det strafferettslige området», samt behandling av personopplysninger «som utføres av en fysisk person som ledd i rent personlige eller familiemessige aktiviteter». Følgelig ville ikke publisering av nevnte personopplysninger være forbudt dersom publisering av personopplysninger på internett var omfattet av overføringsbegrepet.

Videre kan det argumenteres for at formålet som følger av artikkel 44 siste punktum taler for at reglene burde omfatte publisering av personopplysninger på internett. Å publisere personopplysninger på internett innebærer at langt flere individer får tilgang til opplysningene, sammenlignet med ordinære overføringstilfeller. Risikoen for at personvernet til de registrerte undergraves ved operasjonen er da langt større enn når dataeksportører overfører personopplysninger til en enkelt dataimportør i en tredjestat. Formålet som følger av ordlyden til artikkel 44 i forordningen, er imidlertid ikke nevnt i personverndirektivet.

Da avgjørelsen gjelder det tidligere direktivet får EU-domstolens tolkning ikke direkte anvendelse på overføringsbegrepet i forordningen. Selv om personvernforordningen i stor grad er en videreføring av det tidligere direktivet, ble forordningen utarbeidet med formål om å styrke personvernet, jf. punkt 1.1. Det er derfor ikke gitt at overføringsbegrepet skal forstås likt i personvernforordningen. Videre må avgjørelsens vekt ses i lys av dens alder og den teknologiske utviklingen som har funnet sted. I juridisk teori har det blitt tatt til orde for at domstolen sannsynligvis ville ha kommet til et annet resultat i dag.[85]

Når det er sagt, er avgjørelsen begrunnet i momenter som også gjør seg gjeldende under personvernforordningen. Dersom publisering av personopplysninger er omfattet av overføringsbegrepet, ville det innebære at operasjonen er forbudt ettersom enhver tredjestat ikke sikrer et tilstrekkelig beskyttelsesnivå. Dette med de begrensninger som følger av forordningens saklige og geografiske virkeområde. I GDPR artikkel 85 er forholdet til ytrings- og informasjonsfrihet regulert. Ytringsfrihet og retten til personvern kan i noen tilfeller komme i motsetning til hverandre. Etter artikkel 85 nr. 1 plikter medlemsstatene å balansere disse rettighetene mot hverandre. Et forbud mot publisering av personopplysninger på internett kan tenkes være i strid med ytringsfriheten som hjemlet i EU paktens artikkel 11.

[85] Kuner (2020) a s. 762 og 763.

Uttalelsen fra EU-domstolen om at publisering av personopplysninger på internett ville vært særskilt regulert dersom det var lovgivers intensjon at operasjonen skulle underlegges overføringsreglene er særlig sentral. Å stille krav om å uttrykkelig regulere en operasjon strider mot utgangspunktet om at GDPR er teknologisk nøytral og dynamisk.[86] Uttalelsen kan imidlertid forstås som en klar oppfordring fra EU-domstolen til lovgiver å uttrykkelig regulere publisering på internett i overføringskapittelet, dersom operasjonen skal være omfattet. Ved utarbeidelsen av forordningen, forelå denne oppfordringen. Verken personvernforordningens kapittel V eller forordningens fortale nevner publisering av personopplysninger på internett. Både i lys av den rettslige tvilen knyttet til rekkevidden av overføringsbegrepet, og oppfordringen fra EU-domstolen, er det nærliggende å konkludere med at publisering på internett ikke er omfattet av reglene i forordningens kapittel V.

Systembetraktninger kan videre begrunne at reglene ikke omfatter publisering av personopplysninger på internett. Overføringsreglene i direktivet og forordningen er egnet for overføring av personopplysninger til mer lukkede enheter. Overføringsgrunnlaget standard personvernbestemmelser innebærer eksempelvis at overføringen må ha en konkret mottaker for å kunne inngå avtalen.[87] Hvis mottakeren av personopplysningene er alle og enhver som har tekniske midler nødvendige for å få tilgang til personopplysningene, vil bruk av standard personvernbestemmelser som overføringsgrunnlag være nærmest umulig.

Hensynet til personvernet kan også begrunne at reglene ikke omfatter publisering av personopplysninger på internett. Publisering av personopplysninger på internett skiller seg videre fra ordinære overføringstilfeller, ved at risikoen representert ikke først og fremst er at personopplysninger blir tilgjengelige for dataimportører i tredjestater, men at opplysningene er tilgjengelige for alle og enhver. Følgelig kan det argumenteres for at andre regler i personvernforordningen er bedre egnet til å ivareta personvernet til de registrerte. Å publisere personopplysninger vil være en behandling av personopplysninger og følgelig underlegges forordningens øvrige regler.[88] Personvernforordningens generelle prinsipper tilsvarer i stor grad direktivets artikkel 6. De grunnleggende prinsippene medfører blant annet at publisering må være lovlig,

[86] GDPR fortale punkt 15.

[87] Se kapittel 4.3.

[88] Sak C-101/01 avsnitt 27.

formålsbegrenset og ivareta dataminimeringsprinsippet.[89] For særlige kategorier av personopplysninger er behandlingens lovlighet underlagt ytterligere vilkår.[90] Ettersom publisering av personopplysninger på internett når ut til enhver med nødvendige tekniske midler, vil de grunnleggende prinsippene legge store begrensninger på hvilke personopplysninger som lovlig kan publiseres. Lindqvist-dommen kan tas til inntekt for at øvrige regler i direktivet og forordningen er bedre egnet til å ivareta personvernet ved enkelte operasjoner enn overføringsreglene.

Utover Lindqvist-dommen har ikke EU-domstolen tatt direkte stilling til hva som utgjør en overføring. Både i Schrems I og Schrems II var det uomtvistet at overføring til en tredjestat hadde funnet sted. I Schrems II uttaler imidlertid EU-domstolen seg om tolkningen av bestemmelsene i kapittel V.[91] Domstolen legger til grunn at bestemmelsene i kapittel V må forstås i lys av formålet slik det kommer til uttrykk i artikkel 44 siste punktum. Å tolke overføringsbegrepet for å ivareta de registrertes rettigheter følger dermed både av ordlyden i artikkel 44 og Schrems II.

3.2.3 Formål

Formålet bak reglene om overføring av personopplysninger til tredjestater er todelt, og følger av GDPR artikkel 44 samt forordningens fortale. På den ene siden skal reglene sikre at personvernet til de registrerte ikke undergraves når personopplysninger overføres ut av EU/EØS.[92] På den andre siden skal reglene fremme den frie flyten av personopplysninger innad i EU/EØS[93] og overføring til tredjestater for å utvide den internasjonale handelen og samarbeidet.[94] Personvernforordningens overordnede formål er bredere. Reglene skal bidra til frihet, sikkerhet og rettferdighet, samt en økonomisk union og økonomisk og sosial fremgang i det indre markedet og de registrertes velferd.[95] Forordningen skal også skape tillit til den digitale økonomien og styrke det indre markedets posisjon i det digitale verdensmarked.[96] Nevnte formål må balanseres mot hverandre. Reglene i kapittel V kan forstås som en balansering av forordningens

[89] Se kapittel 2.2.
[90] Ibid.
[91] Sak C-311/18 avsnitt 92 og 105.
[92] GDPR artikkel 44 siste punktum og GDPR fortale punkt 101.
[93] GDPR fortale punkt 6.
[94] Ibid punkt 101.
[95] Ibid punkt 2.
[96] Ibid punkt 7.

overordnede formål. De konkrete formålene bak overføringsreglene vil derfor tillegges mest vekt ved tolkningen av overføringsbegrepet. Det er imidlertid sentralt å merke seg at forordningen skal skape tillitt til den digitale økonomien. Å ha håndterbare og forutsigbare regler er nødvendig for å oppnå det formål.

Formålet om å sikre de registrertes personvern taler for en vid forståelse av overføringsbegrepet da flere operasjoner vil underlegges reglene i kapittel V. Å benytte seg av overføringsmekanismene i kapittel V fordrer imidlertid merarbeid. En for vid forståelse av begrepet kan medføre at næringslivet i EU/EØS blir svekket, forhindre internasjonal handel og samarbeid, samt begrense fremgang i det indre marked og europeiske borgeres velferd. Det taler for at overføringsbegrepet ikke bør tolkes for vidt.

Reglene i kapittel V skal sikre at de registrertes personvern ikke undergraves ved overføring av personopplysninger til tredjestater. Det taler for at det bør fortas en konkret risikovurdering knyttet til den aktuelle overføringen. Behandling av personopplysninger medfører i seg selv en risiko. Denne risikoen søkes å imøtegås gjennom øvrige regler i personvernforordningen.[97] Den konkrete risikoen som realiseres ved overføring av personopplysninger til tredjestater, er tredjestaters utilstrekkelige beskyttelsesnivå. Reglene i kapittel V bør avgrenses til å omfatte de operasjoner som medfører en risiko for vern av personopplysninger som følge av overføringsoperasjonen. Det kan argumenteres for at i likhet med vurderingen av hva som utgjør personopplysninger, bør man kunne se bort ifra at det foretas forbudte handlinger ved vurderingen av risiko.[98]

Formålet kan derfor tale for at de konkrete personopplysninger som overføres, bør være av betydning for om reglene kommer til anvendelse. Særlige kategorier av personopplysninger fortjener et sterkere vern.[99] Noen personopplysninger kan overføres til tredjestater uten at det foreligger en risiko for at personvernet til de registrerte undergraves. Dette gjelder særlig offentlig tilgjengelige personopplysninger. I Schrems II ble det blant annet lagt vekt på at amerikanske myndigheter har inngripende lovhjemler og kan pålegge selskaper å utlevere personopplysninger i strid med de avtaler som er inngått med dataeksportøren.[100] Et slikt pålegg vil

[97] Se kapittel 2.2 og 2.3.
[98] Se kapittel 2.1.
[99] Ibid.
[100] Sak C-311/18 avsnitt 178 til 191.

være lite aktuelt dersom personopplysningene er offentlig tilgjengelige. Det vil da være tidskrevende og unødvendig for myndigheter i tredjestater å gå veien om dataimportøren for å få personopplysninger utlevert. Det kan tale for at reglene bør gjøre unntak for overføringer av personopplysninger som ikke vil utgjøre en risiko for personvernet til de registrerte. Det vil medføre en fordel for næringslivet i EU/EØS da dataeksportører ikke vil være underlagt reglene i kapittel V, og en indirekte fordel for europeiske borgeres velferd.

3.2.4 Retningslinjer

Personvernrådet har utarbeidet retningslinjer med formål å klargjøre hvilke tilfeller som er omfattet av overføringsbegrepet og reglene i kapittel V.[101] Personvernrådet har identifisert tre kriterier, som når kumulert, indikerer at det er tale om en overføring av personopplysninger til tredjestater:

(i) en behandlingsansvarlig eller databehandler er underlagt GDPR for en bestemt behandlingsoperasjon,

(ii) (ii) denne bandlingsansvarlige eller databehandleren (dataeksportøren) tilgjengeliggjør eller sender de aktuelle personopplysningene til en annen behandlingsansvarlig, felles behandlingsansvarlige eller databehandler (dataimportøren), og

(iii) (iii) dataimportøren er i et land utenfor EØS eller en internasjonal organisasjon.[102]

Er alle kriteriene oppfylt, har det etter personvernrådets oppfatning funnet sted en overføring av personopplysninger til en tredjestat. Dersom kriteriene ikke er oppfylt, har det ikke funnet sted en overføring. Reglene i kapittel V kommer da ikke til anvendelse.

Personvernrådets tolkning av overføringsbegrepet er vid med bakgrunn i formålet. Det er ikke selvsagt at overføringsbegrepet omfatter å gjøre personopplysninger tilgjengelige for aktører i tredjestater. I slike tilfeller vil ikke personopplysningene forflytte seg til tredjestater, men dataimportører i tredjestater «forflytter seg inn» i databasene i EU/EØS. Først når aktører i tredjestater behandler personopplysningene, skjer det en fysisk forflytting. Begrunnelsen for at reglene omfatter tilgjengeliggjøring er at dataimportøren i tredjestaten for kontroll eller mulighet til å

[101] EDPB Guidelines 05/2021 s. 3.

[102] Ibid.

behandle opplysningene, og det følgelig foreligger en risiko for at vernet til de registrerte kan undergraves.[103]

Personvernrådets andre kriterium innebærer imidlertid en innskrenkning av artikkel 44 sitt virkeområde. Kriteriet om at personopplysningene tilgjengeliggjøres eller sendes *til en annen* behandlingsansvarlig, felles behandlingsansvarlig eller databehandler, følger ikke av artikkel 44. Det innebærer at forretningsreiser ikke er omfattet av reglene i kapittel V. Med forretningsreise menes de tilfeller en arbeidstaker i EU/EØS drar på reise til en tredjestat og benytter seg av fjerntilgang for å få tilgang til selskapets systemer. Personopplysninger blir i et slik tilfelle ikke flyttet fra en stat til en annen, men tilgjengeliggjort for den ansatte som befinner seg i en tredjestat. Ettersom tilgjengeliggjøring er omfattet av overføringsbegrepet, er i utgangspunktet slike tilfeller underlagt kapittel V. Bakgrunnen for at det ikke er tilfellet, er at arbeidstakeren på forretningsreise ikke er en annen behandlingsansvarlig, felles behandlingsansvarlig eller databehandler, men en integrert del av selskapet.[104] Den ansatte og selskapet utgjør samme behandlingsansvarlig eller databehandler. Følgelig finner det ikke sted en overføring.

Fravær av overføring er ikke ensbetydende med at det ikke foreligger en risiko for at de registrertes personvern vil undergraves. Det uttaler Personvernrådet i sine retningslinjer.[105] Behandlingen av personopplysninger utenfor EU/EØS vil være forbundet med økte risikoer, for eksempel på grunn av motstridende nasjonale lover eller uforholdsmessig tilgang til personopplysninger for myndigheter i tredjestater.[106] Disse risikoene må etter Personvernrådets oppfatning også vurderes når behandlingsansvarlige eller databehandler behandler personopplysninger i tråd med artikkel 5 (de generelle prinsippene), artikkel 24 (ansvar for behandlingsansvarlig) og artikkel 32 (sikkerhet ved behandling»).[107] Retningslinjene kan forstås slik at ikke enhver risiko som er begrunnet i tredjestaters innblanding skal imøtegås av reglene i kapittel V, men av øvrige regler i personvernforordningen.

[103] Se punkt 3.2.1.
[104] EDPB Guidelines 05/2021 s. 11.
[105] Ibid s. 3.
[106] Ibid.
[107] Ibid.

3.2.5 Hensyn

Personvernforordningen og særlig reglene om overføring av personopplysninger til tredjestater berører en rekke hensyn. GPDR Artikkel 44 er formulert som et forbud, og legger begrensninger på øvrige hensyn. Etter forordningens fortale punkt 4 heter det at behandling av personopplysninger «bør ha som formål å tjene menneskeheten». Det vises til at retten til vern av personopplysninger ikke er absolutt, men må ses i sammenheng med den funksjon den har i samfunnet og veies mot andre grunnleggende rettigheter i samsvar med forholdsmessighetsprinsippet.[108] Personvernforordningens regler er et utslag av en forholdsmessig avveining av grunnleggende rettigheter og friheter.[109]

Når øvrige hensyn ses hen til ved tolkningen av overføringsbegrepet, er det begrunnet i forordningens manglende definisjon av overføringsbegrepet. Følgelig er det ikke foretatt en avveining av grunnleggende rettigheter og friheter. I Lindqvist-dommen uttalte EU-domstolen at datatilsyn i Europa måtte se det svært vide omfanget av direktivet opp mot fundamentale rettigheter, i samsvar med forholdsmessighetsprinsippet.[110] Ettersom personvernforordningen har et bredere virkeområde, øker behovet for å se reglene opp mot andre hensyn.

Personvernforordningens beskyttelseshensyn må følgelig veies opp mot andre hensyn. I denne sammenheng er særlig hensynet til ytringsfrihet og retten til å drive næringsvirksomhet relevante.[111] Det kan ikke kan trekkes et klart skille mellom hensynene, da de i en viss grad glir over i hverandre. Et tilstrekkelig ivaretatt personvern er viktig både for ytringsfriheten og for retten til å drive næringsvirksomhet.

Hensynet til ytringsfriheten kan ta tale både for en vid og snever forståelse av overføringsbegrepet. Et dårlig ivaretatt personvern kan føre til at borgere begrenser sin deltakelse i åpen meningsutveksling og politisk aktivitet. Et for omfattende regelverk og forbud mot konkrete operasjoner kan imidlertid innebære at den frie meningsutveksling blir vesentlig innskrenket.

---

[108] GDPR fortalepunkt 4. Med grunnleggende rettigheter menes de grunnleggende rettighetene og frihetene i EU pakten, se sak C-507/17 avsnitt 60.

[109] Det følger av GDPR fortale punkt 4 at forordningen overholder alle grunnleggende rettigheter og friheter i EU pakten.

[110] Sak C-101/01 avsnitt 90.

[111] EU pakten artikkel 11 og artikkel 16.

Terskelen for å anse informasjon som personopplysninger er lav.[112] Hensynet kan være en av grunnene til at EU-domstolen i Lindqvist-dommen kom til at publisering av personopplysninger på internett ikke var omfattet av overføringsbegrepet i det tidligere direktivet.[113]

Hensynet til næringsvirksomhet kan også tale for en vid og snever forståelse av overføringsbegrepet. Et dårlig ivaretatt personvern kan hindre økonomisk vekst i EU/EØS. Hensynet taler imidlertid mest for at overføringsbegrepet ikke bør tolkes for vidt, da øvrige regler i forordningen til en viss grad ivaretar beskyttelseshensynet. Dagens økonomi er i stor grad datadrevet, og overføring av personopplysninger på tvers av landegrenser er en del av virksomheters daglige virke. Særlig for små bedrifter, vil overføringsreglene utgjør en stor belastning og gi et dårligere konkurransefortrinn i møte med andre bedrifter som ikke er underlagt GDPR. Flere bedrifter i EU/EØS benytter seg videre av skytjenester med skyparker i EU/EØS, men hovedvirksomhet i tredjestater. Om bedriftene ikke kan benytte seg av skytjenestene uten overføringsgrunnlag, vil europeisk næringsliv påføres et handikap i den internasjonale konkurransen. Det kan medføre at tjenester som gir økt kvalitet og produktivitet, ikke kan tas i bruk. Det vil også gå utover europeiske forbrukere som vil måtte betale mer for tjenester. Handels- og samarbeidsinteresser mellom EU/EØS og tredjestater, samt behovet for teknologisk innovasjon og internasjonal datautveksling taler for en snever tolkning av overføringsbegrepet.

Nødvendighetsbetraktninger kan videre ses hen til ved vurderingen av overføringsbegrepets rekkevidde. Det kan stilles spørsmål ved hvorvidt det er nødvendig med egne overføringsregler eller et vidt overføringsbegrep. Sikkerhet til personopplysninger er gjennomgående regulert i personvernforordningen. Behandlingsansvarlige og databehandleres plikter etter artikkel 24, 28 og 32 er særlig sentrale.[114] Disse pliktene foreligger uavhengig av om det finner sted en overføring av personopplysninger til en tredjestat. Reglene legger opp til risikovurderinger som behandlingsansvarlige og databehandlere må foreta, i lys av den konkrete behandlingen og risikoen for de registrertes personvern. Enkelte overføringsgrunnlag i kapittel V har vist seg å ikke gi en tilstrekkelig beskyttelse av personvernet til de registrerte, da overføringsgrunnlagene ikke er bindende for myndigheter i tredjestater.[115] Overføringsgrunnlagenes absolutte tilnærming påfører begrensninger for næringslivet og kan innebære en manglende beskyttelse i konkrete

[112] Se kapittel 2.1.
[113] Se kapittel 3.2.2.
[114] Se kapittel 2.3.
[115] Se kapittel 1.1 om Schrems I og Schrems II.

tilfeller. En mer pragmatisk og risikobasert tilnærming til overføringer vil bedre kunne ivareta personvernet til de registrerte, slik som øvrige bestemmelser i GDPR legger opp til. Det kan derfor argumenteres for at reglene i GDPR som åpner for en risikobasert tilnærming er bedre egnet for å regulere overføringstilfeller. Reglene i kapittel V kan heller fungere som et verktøy for behandlingsansvarlige og dataimportører. Hvorvidt det er mulig å håndheve regler som tilpasses den konkrete overføringen er imidlertid usikkert. Arbeidsmengden til tilsynsorganene i EU/EØS vil øke og i ytterstefall ikke være håndterbar. Det vil medføre en risiko for personvernet til de registrerte.

3.2.6 Tolkningsresultat

Rettskildene gir ikke et klart svar på overføringsbegrepets rekkevidde. Et utgangspunkt er imidlertid at begrepet er teknologisk nøytralt samt dynamisk, og må tolkes for å ivareta formålet bak bestemmelsen i GDPR artikkel 44. Av den grunn vil begrepet omfatte de fleste tilfeller der personopplysninger på en eller annen måte blir forflyttet ut av EU/EØS. Formåls- og hensynsbetraktninger taler imidlertid for at begrepets rekkevidde må begrenses for å ivareta andre grunnleggende rettigheter. Dette gjelder særlig tilfeller der risikoen for personvernet til de registrerte er liten sammenlignet med konsekvensene for ytringsfriheten og næringslivet.

Analysen gir imidlertid grunn til å konkludere med at noen typetilfeller vil falle utenfor kapittel V sitt virkeområde. Dette gjelder overføringer utført av de registrerte,[116] rene transitt-tilfeller,[117] publisering av personopplysninger på internett,[118] og forretningsreiser.[119] I den videre fremstillingen vil det redegjøres for særlige typetilfeller som det er grunn til å problematisere er omfattet av overføringsbegrepet. Typetilfellene er delt inn i kategoriene «faktiske overføringer», «tilgjengeliggjøringer» og «risiko for mulige overføringer». Skillet mellom hva som utgjør en faktisk overføring, tilgjengeliggjøring og risiko for mulig overføring er ikke nødvendigvis skarp. Inndelingen er først og fremst gjort av pedagogiske grunner.

[116] Se kapittel 3.2.1.
[117] Ibid.
[118] Se kapittel 3.2.2.
[119] Se kapittel 3.2.4.

3.3 Særlige typetilfeller

3.3.1 Faktiske overføringer

Med faktiske overføringer menes de tilfellene der personopplysninger flyttes fra en database, person eller øvrig format innad i EU/EØS til en mottaker i en tredjestat. Det er i utgangspunktet ikke tvilsomt at faktiske overføringer er underlagt reglene i personvernforordningens kapittel V.[120] Utfordringen i slike tilfeller er som regel å identifisere overføringene, som kan illustreres av de høye overtredelsesgebyrene tildelt selskaper i Europa for bruk av Google Analytics det siste året.[121] Når det er sagt, foreligger det tilfeller av faktiske overføringer det er grunn til å problematisere om er eller bør være omfattet av overføringsreglene.

Det gjelder særlig ved tilbakeføring av personopplysninger. Med tilbakeføring av personopplysninger siktes det til de tilfeller der en databehandler i EU/EØS behandler personopplysninger på vegne av en behandlingsansvarlig i en tredjestat, og som ledd i arbeidsavtalen, tilbakefører personopplysninger etter endt arbeid. Det sentrale spørsmålet i denne sammenheng er hvor langt GDPR skal gå i å gi rettigheter til tredjestatsborgere på bekostning av næringslivet i EU/EØS. Databehandleren i EØS vil være underlagt GDPR ved behandling av personopplysningene, jf. artikkel 3 nr. 1.[122] For ordens skyld nevnes det at de aktuelle personopplysningene ikke omhandler europeiske borgere, og følgelig vil ikke den behandlingsansvarlige i tredjestaten være underlagt reglene i GDPR etter artikkel 3 nr. 2.[123] Problemstillingen er hvorvidt tilbakeføringen er en overføring av personopplysninger til tredjestater, med den følge at databehandleren er underlagt reglene i kapittel V for tilbakeføringen.

Etter en ren ordlydsfortolkning av artikkel 44 vil operasjonen omfattet av overføringsbegrepet, ettersom det overføres personopplysninger til en mottaker som befinner seg i en tredjestat.

---

[120] Bruk av skytjeneste kan være et eksempel på en faktisk overføring. Med skytjeneste menes en applikasjon, dataprosessering eller lagring som tilbys på en ekstern lokasjon, se Nätt (2022). Kjente eksempler er Dropbox, Google Drive, OneDrive og Office 365. Flere av nevnte skytjenester er amerikanske. Dersom enheten som behandler personopplysningene befinner seg i en tredjestat, vil bruk av den aktuelle skytjenesten innebære en faktisk overføring. Det er bakgrunnen til at de fleste amerikanske skytjenesteleverandører har serverparker i Europa, for å hindre at personopplysningene faktisk overføres ut av EØS. Se kapittel 3.3.3. om særlige problemstillinger.

[121] Ødegaard (2023).

[122] Se kapittel 2.2.

[123] Se kapittel 2.1.

Personvernrådet har videre lagt til grunn at operasjonen er underlagt reglene i kapittel V.[124] Formål og hensyn taler imidlertid for at operasjonen ikke er omfattet.[125] Dersom overføringsbegrepet omfatter tilbakeføring, betyr det at tilbakeføring av personopplysninger er forbudt med mindre det foreligger et overføringsgrunnlag.[126] Forordningen regulerer ikke overføringer *fra* tredjestater, da formålet bak reglene er å verne personopplysninger som enten har en tilknytning til virksomheter i EU/EØS eller personer som befinner seg i området. Opplysninger som overføres til EU/EØS vil reguleres av GDPR så snart personopplysningene faller inn under ett av alternativene i GDPR artikkel 3, og følgelig er det ikke nødvendig å legge restriksjoner på overføringer som skjer i denne retning. Reglene ivaretar i stor grad personvernet til europeiske borgere. Dersom reglene i kapittel V ikke kommer til anvendelse, vil ikke europeiske borgeres personvern undergraves. Det vil kun innebære at personopplysningene til tredjestatsborgere ikke underlegges personvernforordningens kapittel V. Følgene det får for tredjestatsborgeres personvern fremstår begrenset, da deres personvern først og fremst er ivaretatt av tredjestatslovgivninger. Det personvern som tredjestatsborgere i utgangspunktet nyter, vil følgelig ikke undergraves ved at reglene i kapittel V ikke kommer til anvendelse.

Dersom overføringsbegrepet omfatter tilbakeføring, vil det først og fremst gå på bekostning av næringslivet i EU/EØS og den internasjonale handel. Det vil innebære at databehandlere i EU/EØS må være bevisst på hvilke arbeidsoppdrag de påtar seg og sikre at de har overføringsgrunnlag for å kunne tilbakeføre opplysningene til tredjestaten i tråd med GDPR. Det kan innebære at databehandlere i EU/EØS ikke påtar eller kan påta seg arbeidsoppdrag, fordi reglene fordrer merarbeid eller vil innebære at en tilbakeføring er ulovlig.

I mangel på autoritative kilder er svaret uvisst. Med særlig vekt på formål og hensyn er det forfatterens oppfatning at tilbakeføring av personopplysninger ikke bør omfattes av overføringsbegrepet.

[124] EDPB Guidelines 2023 s. 12.

[125] Det er i juridisk teori også argumentert for en slik forståelse, se Krzysztofek (2021) s. 249.

[126] Se kapittel 4.1.

3.3.2 Tilgjengeliggjøringer

Å gjøre personopplysninger tilgjengelige for en mottaker i en tredjestat er i utgangspunktet omfattet av overføringsbegrepet da det innebærer at mottakeren får kontroll eller mulighet til å behandle personopplysninger.[127] Publisering av personopplysninger er imidlertid en form for tilgjengeliggjøring som ikke er omfattet av overføringsbegrepet.[128] Problemstillingen er derfor hvilke typer tilgjengeliggjøringer som omfattes av reglene i kapittel V. En første problemstilling er imidlertid hva som utgjør en tilgjengeliggjøring.

Begrepet tilgjengeliggjøring er i likhet med overføringsbegrepet ikke definert i personvernforordningen. Det benyttes imidlertid i en rekke andre regelverk i EU-retten, og EU-domstolen har tolket begrepet i flere sammenhenger. I henhold til EUs opphavsrettsdirektiv[129] følger det at tilgjengeliggjøring omfatter handlinger som «over tråd eller trådløst, [utføres] på en slik måte at allmenheten kan få tilgang til verkene fra et selvvalgt sted og på et selvvalgt tidspunkt», jf. artikkel 3 nr. 2.[130] EUs direktiv om tilgjengelighet av offentlige organers nettsteder og mobilapplikasjoner[131] fastlegger videre fire grunnleggende prinsipper for tilgjengelighet. Etter direktivets artikkel 4 må informasjon kunne oppfattes, betjenes, forstås og være robust. Forståelsen av begrepet tilgjengelig vil avhenge av det regelverk som tolkes og de hensyn det søker å ivareta. Tilgjengeliggjøringsbegrepet kan følgelig ha ulike betydning i de ulike regelsettene.

I Lindqvist-dommen la EU-domstolen til grunn at publisering av personopplysninger er en form for tilgjengeliggjøring.[132] Dette er i tråd med definisjonen av tilgjengeliggjøringsbegrepet i opphavsretten. I motsetning til opphavsretten, vil imidlertid også tilgjengeliggjøring omfatte de tilfeller der personopplysninger ikke gjøres tilgjengelige til allmennheten, men til en lukket enhet.[133] Det viser at forståelsen av tilgjengeliggjøringsbegrepet i personvernretten et videre enn forståelsen av begrepet i opphavsretten.

---

[127] Se kapittel 3.2, særlig kapittel 3.2.1 og 3.2.4.

[128] Se kapittel 3.2.2.

[129] Direktiv 2001/29/EF.

[130] Å gjøre verket tilgjengelig omfatter i utgangspunktet enhver formidling av verket, se sak 2015 C-325/14.

[131] Direktiv 2016/2102 EU.

[132] Sak C-101/01 avsnitt 25.

[133] Se eksempelvis Personvernrådets uttalelser om at fjerntilgang i EDPB Guidelines 05/2021 s. 8.

Videre er forståelsen av tilgjengeliggjøring annerledes i personvernretten enn det som følger av EUs direktiv om tilgjengelighet av offentlige organers nettsteder og mobilapplikasjoner. For det første stilles det ikke krav om at personopplysningene må kunne forstås eller oppfattes, krypterte og pseudonymiserte er personopplysninger.[134] Videre må ikke personopplysningene være robuste, da det ikke stilles krav om at personopplysningene er verken objektivt verifiserbare eller direkte kan knyttes til en fysisk person.[135] Kravet om at informasjonen må kunne betjenes har imidlertid sin parallell til behandlingsbegrepet i personvernretten. Personopplysninger som kan betjenes kan også behandles. Uten at en mottaker kan behandle opplysningene, foreligger det ikke en risiko for personvernet. Gjøres personopplysninger «tilgjengelig» for en mottaker i en tredjestat som er avgrenset fra å behandle personopplysninger, er det naturlig å konkludere med at det ikke har funnet sted en tilgjengeliggjøring. Hvorvidt det overhodet er praktisk mulig, er en annen sak. Så lenge mottakeren i tredjestaten kan se opplysningene, er det mulig for vedkommende å behandle dem, eksempelvis ved å notere dem ned. Uansett er det nærliggende å konkludere med at tilgjengeliggjøring innebærer å gjøre personopplysninger tilgjengelig for en mottaker i en tredjestat på en slik måte at vedkommende har mulighet til å behandle personopplysningene.

Problemstillingen om hvilke former for tilgjengeliggjøring som er omfattet av overføringsbegrepet er mer sentral for personvernforordningen. Selv om EU-domstolen fant at publisering på internett var å gjøre personopplysningene tilgjengelige, var ikke operasjonen omfattet av overføringsbegrepet. Publisering på internett skiller seg fra ordinære overføringstilfeller ved at personopplysningene blir gjort tilgjengelige for alle og enhver. Problemstillingen er derfor hva som gjør en tilgjengeliggjøring tilstrekkelig lukket til å omfattes av overføringsbegrepet.

Det foreligger ingen autoritative rettskilder som har drøftet problemstillingen. I Lindqvist-dommen ble det lagt vekt på den tekniske karakteren av operasjonene som forutsatte at personer i tredjestater aktivt måtte oppsøke nettsidene.[136] Flere former for tilgjengeliggjøring forutsetter imidlertid aktivitet fra den andre parten, og det er forfatterens syn at dette ikke var det avgjørende momentet for at EU-domstolen kom til at publisering av personopplysninger på internett ikke er omfattet av overføringsbegrepet. EU-domstolen la imidlertid også vekt på at

[134] Se kapittel 2.1.
[135] Ibid.
[136] Se kapittel 3.2.2.

overføringsreglenes ville innebære at all publisering av personopplysninger på internett ville være ulovlig dersom begrepet omfattet publisering på internett. Dommen kan forstås slik at overføringsreglene ikke var egnet for å regulere publisering av personopplysninger på internett.

I EDPB sine retningslinjer nevnes det noen eksempler på tilgjengeliggjøringer som er å opprette konto, gi tilgangsrettigheter til eksisterende konto, «bekrefte»/«godta» en effektiv forespørsel om ekstern tilgang, bygge inn en harddisk eller sende inn et passord til en fil.[137] Disse formene for tilgjengeliggjøring har til felles at det gjøres til en lukket enhet.

Det er nærliggende å konkludere med at tilgjengeliggjøring må gjøres til en mer lukket enhet, enn det publisering av personopplysninger på internett vil være. Spørsmålet er imidlertid hvor grensen skal trekkes. Dersom personopplysninger publiseres på en nettside et begrenset antall brukere må ha passord og tillatelse for å få tilgang til, kan det tenkes at tilgjengeliggjøringen er underlagt reglene i kapittel V. Dersom hver bruker befinner seg i hver sin tredjestat, vil imidlertid publiseringen ikke kunne utføres i samsvar med GDPR. Det er følgelig ikke antall brukere, men brukernes geografiske lokasjon som avgjør hvorvidt reglene er egnet til å regulere operasjonen.

En betraktning er å benytte en motsatt forståelse av tilgjengeliggjøringsbegrepet i opphavsretten, der det stilles krav om at verket må gjøres tilgjengelig for *allmenheten*. Å forstå tilgjengeliggjøringsbegrepet i personvernretten til å omfatte alle former for tilgjengeliggjøringer med unntak av tilgjengeliggjøringer til allmenheten, kan begrunnes i at øvrige regler i GDPR vil legge store begrensinger på slike behandlinger.[138] Jo flere personopplysninger gjøres tilgjengelige for, jo færre personopplysninger vil lovlig kunne tilgjengeliggjøres etter reglene i GDPR.

Svaret på hvilke operasjoner av tilgjengeliggjøringer som omfattes av kapittel V er ikke gitt. Et alternativ er at begrepet omfatter alle former for tilgjengeliggjøring med unntak av publisering på internett. Et annet alternativ er at begrepet omfatter de former for tilgjengeliggjøring som reglene i kapittel V er egnet til å regulere. Et tredje alternativ er å benytte en motsatt forståelse av tilgjengeliggjøringsbegrepet i opphavsretten, og omfatte alle former for tilgjengeliggjøring med unntak av tilgjengeliggjøring til allmenheten. I mangel på autoritative kilder er det mest

[137] EDPB Guidelines 05/2021 s. 8.

[138] Se kapittel 3.2.2.

nærliggende å konkludere med at begrepet omfatter alle former for tilgjengeliggjøringer med unntak av publisering på internett. Ettersom det foreligger et behov for å trekke en klar grense, er det sannsynlig at fremtidige rettsavgjørelser vil avklare spørsmålet.

Et spørsmål som kan tas opp i den sammenheng er om tolkningsresultatet vil åpne for omgåelse av regelverket ved at behandlingsansvarlige eller databehandleres publiserer personopplysninger på internett med eneste hensikt å overføre opplysningene til en tredjestat. Datatilsynet er klare på at en slik omgåelse vil være brudd på GDPR artikkel 6 og kapittel V.[139] Etter forfatterens syn vil videre de grunnleggende prinsippene i GDPR artikkel 5 nr. 1 innebære at slike publiseringer er ulovlige. Det siktes særlig til at personopplysningene skal behandles lovlig, rettferdig og åpent, samt sikre integritet og konfidensialitet, jf. artikkel 5 nr. 1 bokstav a og f.

3.3.3 Risiko for mulige overføringer

Siste typetilfelle som vil problematiseres omtales som «risiko for mulige overføringer». Med risiko for mulige overføringer menes tilfeller der det verken skjer en faktisk overføring eller tilgjengeliggjøring av personopplysninger til en tredjestat, men en risiko for at overføring vil skje. Særlig i to tilfeller gjør risikoen seg gjeldende: i) når behandlingsansvarlige eller databehandlere overfører personopplysninger til selskaper i EU/EØS som har morselskap i en tredjestat, og ii) når behandlingsansvarlige eller databehandlere tar i bruk skytjenesteleverandører med serverparker i EU/EØS, men hovedvirksomhet i en tredjestat. Bakgrunnen for at det foreligger en risiko, er at tredjestatsmyndigheter kan gi pålegg om å utlevere personopplysninger som følge av mor-datterselskap struktur eller hovedvirksomhet i en tredjestat. Blir pålegg fulgt, vil personopplysninger overføres til en tredjestat. I det videre vil det ikke skilles mellom de to typetilfellene da de ofte glir over i hverandre og samme betraktninger vil gjøres gjeldende.

Etter en ren ordlydsforståelse av artikkel 44 vil ikke en risiko for mulige overføringer omfattes av reglene i kapittel V. Reglene gjelder overføringer til «tredjestater». Overføring til et selskap som befinner seg i EU/EØS vil ikke innebære en overføring til en tredjestat.[140] Artikkel 44 benytter videre begrepet «overføringer», ikke «risiko for mulige overføringer».

---

[139] «*Omgåelse av regelverket ved å publisere personopplysninger med eneste hensikt om å overføre dem til et tredjeland, vil i alle tilfeller kunne være brudd på både artikkel 6 og kapittel V i personvernforordningen.*» Sitat hentet fra Datatilsynet (2023).

[140] Se kapittel 3.2.1.

Systembetraktninger taler for det samme, da samtlige overføringsgrunnlag i kapittel V forutsetter en vilje eller kunnskap om overføringen for å tas i bruk. I Schrems II uttalte EU-domstolen at ved bruk av standard personvernbestemmelser som overføringsgrunnlag må dataeksportører vurdere hvorvidt beskyttelsesnivået er tilstrekkelig i praksis.[141] Å foreta slike vurderinger er utfordrende uten en vilje eller kunnskap om en overføring.[142]

Formålsbetraktninger taler i begge retninger. Når personopplysninger overføres til et selskap i EU/EØS med et morselskap i en tredjestat, vil risikoen for at de registrertes personvern undergraves være reell. Dette fordi morselskapet er underlagt tredjestaters lovgivning, og kan motta pålegg om utlevering av personopplysninger fra tredjestatsmyndigheter. På grunn av konsernrelasjoner og selskapsstrukturer, kan det omfatte personopplysninger som kun er overført til datterselskapet i EU/EØS. Det taler for at tilfellet bør omfattes av overføringsreglene. Risikoen for at personvernet undergraves vil videre være større dersom datterselskapet har tatt forbehold om utlevering av personopplysninger i tilfelle pålegg fra tredjestatsmyndigheter.

På den andre siden kan formålsbetraktninger tale for at tilfellet ikke burde omfattes av overføringsreglene, da reglene vil innebære en begrensning av den frie flyten av personopplysninger innad i EU/EØS.[143] Overføring av personopplysninger til selskaper i EU/EØS med morselskap i tredjestater vil bli forbudt med mindre det foreligger et overføringsgrunnlag. Er risikoen for at de registrertes personvern vil undergraves liten, taler det klart for at tilfellet ikke omfattes. Det er særlig aktuelt dersom praksis viser at tredjestatsmyndigheter ikke pålegger morselskaper å utlevere personopplysninger overført til datterselskapet i EU/EØS, eller dersom datterselskapet ikke har tatt forbehold om utlevering av personopplysninger i tilfelle pålegg fra tredjestatsmyndigheter.

I 2021 ble mor- og datterselskapsstrukturen vurdert av den franske forvaltningsdomstol Conseil d'Etat.[144] Saken gjaldt behandling av personopplysninger knyttet til bruk av Doctolib for administrering av vaksinasjon mot Covid-19 i Frankrike. Klagende parter anførte at staten måtte suspendere avtalen med Doctolib fordi selskapet benyttet seg av det amerikanske selskapet Amazon Web Services (heretter «AWS») for lagring av personopplysninger. Conseil d'Etat fant

[141] C-311/18 avsnitt 131.
[142] Se kapittel 3.3.
[143] Se kapittel 3.2.3.
[144] CE – 450163.

imidlertid at Doctolib benyttet seg av AWS Luxembourg, et datterselskap av AWS med datasentre i Frankrike og Tyskland, for lagring av personopplysninger. Domstolen kom til at bruk av Doctolib ikke var i strid med GDPR, da tilstrekkelige tekniske og organisatoriske tiltak var på plass for å beskytte personopplysningene til de registrerte. Domstolen vurderte ikke konkret hvorvidt overføring av personopplysninger til datterselskapet var omfattet av overføringsbegrepet. Ettersom domstolen konkluderte med at avtalen med Doctolib kunne fortsette, er det imidlertid nærliggende å forstå avgjørelsen slik at overføring til datterselskapet ikke utgjorde en overføring til en tredjestat. Dersom domstolen hadde funnet at det var tilfellet, ville overføringen vært i strid med GDPR på grunn av manglende overføringsgrunnlag.

I en tysk avgjørelse avsagt av det offentlige anskaffelseskammeret i Baden-Württemberg i 2022 ble spørsmålet igjen vurdert.[145] Saken gjaldt lovligheten av en offentlig anskaffelsesprosess. Selskapet som vant anbudskonkurransen benyttet seg av tjenester fra et selskap i EU/EØS med morselskap i USA, og overførte i den anledning personopplysninger til datterselskapet. Datterselskapet i EU/EØS hadde tatt forbehold om utlevering i tilfelle pålegg fra tredjestatsmyndigheter. Det offentlige anskaffelseskammeret fant at overføringene til datterselskapet var ulovlige på grunn av morselskapet i USA. Domstolen la vekt på at uavhengig av hvor personopplysningene faktisk ble lagret, forelå den en risiko for at personopplysningene ville overføres til USA på grunn av amerikansk overvåkningslovgivning.

I en sak fra det danske datatilsynet ble spørsmålet igjen vurdert.[146] I vurderingen skilte datatilsynet mellom såkalte «tilsigtet» og «utilsigtet» overføringer. Dersom overføringen er «tilsigtet», er det danske datatilsynets oppfatning at overføringene er omfattet av reglene i kapittel V. I den sammenheng vurderte datatilsynet en overføring av personopplysninger til et selskap som hadde tatt forbehold om utlevering av personopplysninger om nødvendig for å overholde lovgivning eller bindende vedtak, som «tilsigtet» overføring. Etter det danske datatilsynets oppfatning er det tale om en overføring til en tredjestat dersom behandlingsansvarlige eller databehandlere overfører personopplysninger til et selskap i EU/EØS (med et morselskap i en tredjestat) som har tatt et slikt forbehold.

[145] 1 VK 23/22.

[146] Det danske Datatilsynet (2022).

Den 3. februar 2023 publiserte den tyske databeskyttelseskonferansen ("Datenschutzkonferenz", "DSK") en avgjørelse om mor- og datterselskapsproblematikken.[147] DSK kom, i motsetning til det offentlige anskaffelseskammeret i Baden-Württemberg, til at risiko for overføring ikke er omfattet av reglene i kapittel V. DSK fremhevet imidlertid at den behandlingsansvarlige må ta hensyn til denne risikoen i henhold til artikkel 28 i personvernforordningen.

Gjennomgangen av praksis fra nasjonale domstoler og tilsynsmyndigheter viser at mor- og datterselskapsproblematikken har blitt vurdert ulikt i EUs medlemsland, også innad i landene. Hvorvidt datterselskapet i EU/EØS har tatt forbehold om utlevering, er et moment som går igjen i vurderingene.

Systembetraktninger kan tale for at avgjørelsen avsagt av DSK har de beste grunner for seg. Reglene i GPDR skal beskytte personopplysninger, uavhengig av om de overføres til en tredjestat eller ikke. Kun reglene i GDPR kapittel V er rettet mot overføringer til tredjestater. Behandlingsansvarlige og dataeksportører må imidlertid ta hensyn til den risikoen som representeres av tredjestater innblanding etter øvrige bestemmelser i GPDR. Etter artikkel 28 plikter behandlingsansvarlige å vurdere selskapers infrastruktur som følge av kravene til valg av forsvarlig databehandler.[148] Det innebærer en vurdering av hvorvidt databehandleren har hovedkontor eller morselskap i tredjestater hvor det kan kreves utlevering. Videre plikter både den behandlingsansvarlige og databehandleren å treffe tiltak for å sikre et enhver fysisk person som har tilgang til personopplysningene, behandler opplysningene kun etter instruks fra den behandlingsansvarlige, jf. artikkel 32 nr. 4. Å overføre personopplysninger til et selskap som har tatt forbehold om utlevering av personopplysninger som følge av pålegg, vil følgelig kunne være i strid med øvrige regler i forordningen.

Nødvendighetshensyn taler derfor for at tilfellet ikke bør omfattes av overføringsreglene, da personvernet til de registrerte ivaretas av øvrige bestemmelser i personvernforordningen. Konsekvensbetraktninger taler i samme retning. Dersom behandlingsansvarlige og databehandlere må ha overføringsgrunnlag for å overføre personopplysninger til selskaper i EU/EØS, vil det stride mot det overordnede formålet bak GDPR om fri flyt av personopplysninger innad i EU/EØS.

---

[147] DSK beslutning av 31.01.2023.

[148] EDPB Guidelines 05/2021 avsnitt 24.

4 Hvordan kan personopplysninger lovlig overføres til tredjestater etter personvernforordningen?

4.1 Innledende bemerkninger

Overføring av personopplysninger til tredjestater er underlagt reglene i kapittel V i personvernforordningen. Det fremgår av artikkel 44 første punktum at overføring av personopplysninger til tredjestater «skal finne sted bare dersom den behandlingsansvarlige eller databehandleren [...] oppfyller vilkårene i dette kapittel». Bestemmelsen kan forstås som et forbud mot å overføre personopplysninger til tredjestater, med mindre vilkårene i kapittel V er oppfylt. Artikkel 45 til 49 i kapittel V angir som nevnt alternative overføringsgrunnlag. Det primære overføringsgrunnlaget er adekvansbeslutninger i henhold til artikkel 45. Dersom det ikke foreligger en adekvansbeslutning, kan overføring skje etter «nødvendige garantier» i form av standard personvernbestemmelser, jf. artikkel 46 nr. 2 bokstav c, jf. artikkel 46 nr. 1.

I utgangspunktet taler reglene for at personopplysninger lovlig kan overføres til tredjestater basert på adekvansbeslutninger eller ved benyttelse av standard personvernbestemmelser. Dette utgangspunkt ble utfordret i Schrems I og Schrems II, og slått hardt ned på. I begge avgjørelser var forholdet til tredjestaters etterretningsmyndigheter et avgjørende moment for at overføringene ble funnet ulovlige. Forholdet til tredjestaters etterretningsmyndigheter er verken regulert i GDPR eller omtalt i forordningens fortale. I den videre fremstillingen skal det søkes å besvare hvordan dataeksportører lovlig kan overføre personopplysninger til tredjestater på grunnlag av adekvansbeslutninger og standard personvernbestemmelser, i lys av Schrems II og etterfølgende rettskilder fra EU Kommisjonen og Personvernrådet.

4.2 Adekvansbeslutninger

Personvernforordningens artikkel 45 hjemler overføring etter «adekvansbeslutninger». Etter artikkel 45 nr. 1 første punktum kan personopplysninger overføres til en tredjestat når «Kommisjonen har fastslått at tredjestaten, et territorium eller en eller flere angitte sektorer i nevnte tredjestat […] sikrer et tilstrekkelig beskyttelsesnivå». Slike overføringer «skal ikke kreve en særlig godkjenning», jf. annet punktum.

Et «tilstrekkelig» beskyttelsesnivå innebærer ikke at beskyttelsesnivået må være identisk med det som gjelder i EU, men at det er i det vesentlige det samme.[149] Et krav om identisk beskyttelsesnivå ville forhindre nesten enhver overføring av personopplysninger til tredjestater, ettersom personvernforordningen og omfanget av beskyttelsesnivået er unikt.[150]

Kommisjonen fastlegger adekvansbeslutninger etter artikkel 45 nr. 3 gjennom «gjennomføringsakter». Per 30. april 2023 foreligger det adekvansbeslutninger for Andorra, Argentina, Canada (kommersielle organisasjoner), Færøyene, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republikken Korea, Sveits, Storbritannia og Uruguay.[151] Før Kommisjonen treffer en adekvansbeslutning, skal det foretas en omfattende vurdering av den aktuelle tredjestaten, herunder dets rettsstat og relevant lovgivning, jf. artikkel 45 nr. 2. Videre skal Kommisjonen «fortløpende overvåke utvikling i tredjestater» og oppheve adekvansbeslutningen dersom en utvikling viser seg å føre til at tredjestaten ikke lenger sikrer et tilstrekkelig beskyttelsesnivå, jf. artikkel 45 nr. 3 og 5.

Har Kommisjonen besluttet at en tredjestat har regler som gir personvernet et tilstrekkelig beskyttelsesnivå, kan personopplysninger lovlig overføres til tredjestaten.[152] Personvernrådet har lagt tilsvarende til grunn i retningslinjer utarbeidet etter EU-domstolen avsa Schrems II. Det uttales at dersom personopplysninger utelukkende overføres til mottakere i tredjestater som er godkjent etter GDPR artikkel 45, behøver ikke dataeksportøren å foreta seg noe for å sikre personopplysningene under og etter overføringen.[153]

Utgangspunktet om at overføringer lovlig kan foretas til tredjestater som er tilkjent en adekvansbeslutning, må nyanseres. Adekvansbeslutninger kan overprøves av EU-domstolen og kjennes ugyldige.[154] Videre uttrykte EU-domstolen i Schrems II at uavhengig av overføringsgrunnlag må beskyttelsesnivået til personopplysningene garanteres.[155] En adekvansbeslutning skal i utgangspunktet kun treffes dersom beskyttelsesnivået i tredjestaten er tilstrekkelig. Men

[149] Sak C-362/14 avsnitt 73-74 og Sak C-311/18 avsnitt 94.
[150] Krzysztofek (2021) s. 255.
[151] EU Kommisjonen (u.å.) b.
[152] Forutsatt at øvrige bestemmelser i GDPR er overholdt.
[153] EDPB Recommendations 01/2020 s. 12, igjen under forutsetning at øvrige bestemmelser i GDPR er overholdt.
[154] Se eksempelvis sak C-311/18 avsnitt 199 der EU-domstolen setter til side Privacy Shield avtalen som ugyldig.
[155] Sak C-311/18 avsnitt 92.

selv om Kommisjonen plikter å undersøke og vurdere at beskyttelsesnivået faktisk er tilstrekkelig før de tilkjenner en adekvansbeslutning, viser tidligere praksis at dette ikke alltid er tilfellet.[156] Å ukritisk legge til grunn en adekvansbeslutning som overføringsgrunnlag kan føre til at virksomheten raskt må avvikle deres praksis dersom EU-domstolen skulle finne adekvansbeslutningen ugyldig. Dette var tilfellet i både Schrems I og Schrems II. Overføringer basert på Safe Harbour og Privacy Shield måtte avslutte øyeblikkelig, og dataeksportører fikk ikke tilkjent et slingringsrom for å omstille seg.

I praksis er det derfor ikke avgjørende hvorvidt det foreligger en adekvansbeslutning dersom tredjestaten i praksis ikke sikrer et tilstrekkelig beskyttelsesnivå. Kommisjonens plikter å endre eller oppheve en adekvansbeslutning når «tilgjengelig informasjon» viser at en tredjestat ikke lenger sikrer et tilstrekkelig beskyttelsesnivå, jf. artikkel 45. nr. 5. Relevant informasjon om tredjestaters myndighetspraksis er ikke nødvendigvis tilgjengelig for Kommisjonen. Maximilian Schrems anla sak for EU-domstolen i Schrems I på bakgrunn av de såkalte Snowden-avsløringene i 2013.[157] IT-tekniker og tidligere CIA-ansatt Edward Snowden publiserte gradert informasjon om hvordan amerikanske myndigheter overvåket nasjonale og utenlandske borgere gjennom etterretningsprogrammet PRISM.[158] Å vurdere hvorvidt en tredjestat sikrer et tilstrekkelig beskyttelsesnivå, kan følgelig være utfordrende på grunn av mangel på tilgjengelig informasjon. Videre må det foretas vurderinger av fremmedlovgivning. Uten grundig kompetanse innenfor et annet rettssystem er det en utfordrende oppgave.

Ettersom adekvansbeslutninger oppheves uten tid til dataeksportører å områ seg og finne nye overføringsgrunnlag, anbefales det å følge utviklinger i tredjestater. Dersom en adekvansbeslutning er blitt kritisert eller klaget inn for EU-domstolen, kan det være god grunn for dataeksportører å vurdere øvrige overføringsgrunnlag.

[156] Sak C-362/14 og sak C-311/18.

[157] Sak C-362/14 avsnitt 28.

[158] Restad, Notaker og Mæhlum (2023).

4.3 Standard personvernbestemmelser

4.3.1 Rettslig utgangspunkt

Etter artikkel 46 nr. 1 følger det at dersom en adekvansbeslutning ikke foreligger, kan personopplysninger bare overføres om dataeksportøren har gitt «nødvendige garantier» og under forutsetning av at de registrerte personene har «håndhevbare rettigheter og effektive rettsmidler». Bestemmelsen kan i likhet med artikkel 44 og 45 forstås som et forbud mot overføring med mindre vilkårene er oppfylt.[159] Vilkårene er kumulative. Dersom det foreligger nødvendige garantier, men de registrerte ikke har håndhevbare rettigheter eller effektive rettsmidler, vil ikke overføring kunne skje.

Med «nødvendige garantier» menes garantier som skal sikre at personopplysninger gis et tilstrekkelig vern, også etter at de er overført til en tredjestat.[160] Med «effektive rettsmidler» og «håndhevbare rettigheter» menes at de registrerte skal ha mulighet til å ivareta sine rettigheter etter at opplysningene er overført, ved hjelp av rettsmidler tilgjengelige i enten avsender- eller mottakerstaten.[161] Er man i realiteten avskåret fra å reise sak mot dataeksportøren eller dataimportøren i mottakerstaten ved brudd på de garantiene som er gitt, vil ikke vilkårene i artikkel 46 nr. 1 være oppfylt.

Artikkel 46 nr. 2 oppgir en rekke alternative former for nødvendige garantier. Det mest brukte overføringsgrunnlaget er «standard personvernbestemmelser» etter artikkel 46 nr. 2 bokstav c.[162] Det er fordi overføringsgrunnlaget er standardiserte og forhåndsgodkjente personvernbestemmelser vedtatt av Kommisjonen som ikke trenger videre godkjenning fra offentlige instanser.[163] På engelsk omtales disse som «Standard Contractual Clauses» («SCCs»). De standardiserte personvernbestemmelsene er juridisk bindende avtaler som gir forpliktelser for dataeksportører og dataimportører, og rettigheter til de registrerte.[164]

---

[159] Skullerud mfl. (2019) s. 377.
[160] Ibid.
[161] Ibid.
[162] Yakovleva (2020) s. 889.
[163] Skullerud mfl. (2019) s. 265.
[164] Datatilsynet (2020).

Til tross for at standard personvernbestemmelsene er utarbeidet og godkjent av Kommisjonen, har overføringsgrunnlaget vist seg problematisk av flere grunner. I likhet med adekvansbeslutninger, forplikter ikke standard personvernbestemmelsene myndigheter i tredjestater. Et ytterligere moment som gjør overføringsgrunnlaget mer problematisk enn adekvansbeslutninger, er at standard personvernbestemmelser kan benyttes som overføringsgrunnlag til en tredjestat som ikke sikker et tilstrekkelig beskyttelsesnivå. I forkant av Schrems II var derfor flere dataeksportører bekymret for at EU-domstolen skulle underkjenne bruken av standard personvernbestemmelser som overføringsgrunnlag.[165] EU-domstolen opprettholdt imidlertid overføringsgrunnlaget, og bekreftet at Kommisjonen ikke har en plikt til å vurdere nivået av personvern i områdene som personopplysningene overføres til.[166] EU-domstolen uttaler imidlertid i avgjørelsens avsnitt 131 at «in the absence of a Commission adequacy decision, it is for the controller or processor established in the European Union to provide, inter alia, appropriate safeguards».[167] Uttalelsen og avgjørelsen som helhet har blitt tolket til å oppstille nye plikter ved overføring av personopplysninger til tredjestater etter standard personvernbestemmelsene.[168] I det videre skal det søkes å redegjøres for disse, med utgangspunkt i Schrems II og etterfølgende rettskilder fra Personvernrådet og EU Kommisjonen.

4.3.2 Schrems II

I Schrems II vurderte EU-domstolen hvilket beskyttelsesnivå som kreves i henhold til overføring etter standard personvernbestemmelsene og hvilke momenter som må tas i betraktning for å vurdere beskyttelsesnivået.[169] Domstolen la til grunn at henvisningen i artikkel 46 nr. 1 til «nødvendige garantier» og «håndhevbare rettigheter og effektive rettsmidler" må forstås i lys av artikkel 44.[170] Artikkel 44 siste punktum fastsetter at alle bestemmelser i kapittel V i GDPR skal «sikre at det nivået for vern av fysiske personer som garanteres i denne forordning, ikke undergraves». Domstolen fant at beskyttelsesnivået må sikres uavhengig av hvilket overføringsgrunnlag som tas i bruk. Videre fant domstolen at kravet til tilstrekkelig beskyttelsesnivå må forstås i lys av EU pakten.[171] Domstolen vurderte derfor om standard

[165] Kuner (2020) b.
[166] Sak C-311/18 avsnitt 130.
[167] Ibid avsnitt 131.
[168] Datatilsynet (2023).
[169] Sak C-311/18 avsnitt 90.
[170] Ibid avsnitt 92.
[171] Ibid avsnitt 105.

personvernbestemmelser er et gyldig overføringsgrunnlag i lys av artikkel 7, 8 og 47 i Pakten.[172] Bestemmelsene gjelder retten til respekt for privatliv og familieliv, retten til beskyttelse av personopplysninger og adgangen til effektive rettsmidler og en upartisk domstol. Som utgangspunkt for denne vurderingen fremhevet domstolen at standard personvernbestemmelser kun er bindende for partene i avtalen.[173] Spørsmålet ble dermed om manglende evne til å gi beskyttelse mot myndighetene i den aktuelle tredjestaten, medfører at standard personvernbestemmelsene er ugyldige.[174] EU-domstolen besvarte dette spørsmålet benektende.[175]

EU-domstolen la imidlertid til grunn at i fraværet av en adekvansbeslutning, må det iverksettes tiltak for å kompensere for mangelen på tilstrekkelig beskyttelsesnivå i tredjestaten.[176] Domstolen støttet seg på uttalelser i forordningens fortale, som forutså bruk av «andre bestemmelser eller ytterligere garantier» ved overføring etter artikkel 46.[177] Standard personvernbestemmelsene var i utgangspunktet utarbeidet med det formål å sikre at personopplysningene har et tilstrekkelig beskyttelsesnivå etter at de blir overført ut av EU/EØS. EU-domstolen la imidlertid til grunn at man må vurdere hvorvidt beskyttelsesnivået vil opprettholdes i praksis, særlig i lys av tredjestaters lovgivning som ikke er bundet av overføringsgrunnlaget og som går lenger enn det som er nødvendig og proporsjonalt.[178] Av den grunn uttalte domstolen at standard personvernbestemmelser i noen tilfeller må suppleres av ytterligere tiltak. Dersom det er nødvendig med ytterligere tiltak og de ikke iverksettes, er overføringen ulovlig og må stanse.[179] EU-domstolen la til grunn at overføringene må vurderes «on a case-by-case-basis»[180] og at tilsynsmyndighetene skal vurdere overføringen «in light of all the circumstances of that transfer».[181]

Selv om standard personvernbestemmelser er forhåndsgodkjente avtaler kan de ikke benyttes som overføringsgrunnlag dersom beskyttelsesnivået ikke opprettholdes i praksis. Ved bruk av overføringsgrunnlaget, kan det utledes fra avgjørelsen at det foreligger en særlig risiko som

[172] Sak C-311/18 avsnitt 122.
[173] Ibid avsnitt 125.
[174] Ibid avsnitt 127.
[175] Ibid avsnitt 149.
[176] Ibid avsnitt 131.
[177] Ibid avsnitt 132.
[178] Ibid avsnitt 135.
[179] Ibid avsnitt 135.
[180] Ibid avsnitt 134.
[181] Ibid avsnitt 146.

følge av tredjestatsmyndigheter som må hensyntas. Utover dette, gir ikke EU-domstolen veiledning til hvilke momenter dataeksportører plikter å vurdere. Videre uttrykker ikke EU-domstolen seg uttrykkelig om hvilke tiltak dataeksportører plikter å iverksette dersom beskyttelsesnivået ikke er tilstrekkelig i praksis.

4.3.3 Etterfølgende rettskilder fra Personvernrådet og Kommisjonen

I kjølvannet av Schrems II har Personvernrådet utarbeidet retningslinjer om ytterligere tiltak for å bistå dataeksportører.[182] Personvernrådets retningslinjer er som nevnt ikke juridisk bindende, men for norske dataeksportører er det særlig av betydning at Datatilsynet har uttalt at de vil tolke loven likt som EDPB i en eventuell tilsynssak. [183] Videre har EU Kommisjonen som nevnt utarbeidet nye standard personvernbestemmelser. Under Direktiv 95/46/EF vedtok Kommisjonen tre sett med standard personvernbestemmelser.[184] Allerede før Schrems II-dommen falt hadde Kommisjonen startet utarbeidelsen av de nye standard personvernbestemmelser, som ble vedtatt 4. juni 2021.[185] Standard personvernbestemmelsene er ment å imøtegå de kravene som ble reist av EU-domstolen i Schrems II, og kan gi uttrykk for Kommisjonens forståelse av avgjørelsen.

De reviderte retningslinjene publisert av EDPB presenterer en sekstrinnsvurdering.[186] Sentralt i vår sammenheng er steg tre og fire i vurderingen. Steg tre innebærer at dataeksportører må vurdere hvorvidt overføringsgrunnlaget er effektivt i lys av alle omstendigheter knyttet til overføringen.[187] Det innebærer blant annet å vurdere tredjestaters lovgivning og praksis. Ikke all tredjestatslovgivning som hjemler inngrep i personvernet er problematisk, bare den som går lenger enn det som er nødvendig og proporsjonalt. I vurderingen av lovgivningen, kan det tas hensyn til dokumenterte praktiske erfaringer, herunder hvorvidt det foreligger tidligere utleveringsbegjæringer fra tredjestatsmyndigheter. Informasjonen vurderingene bygger på *bør* være

[182] EDPB Recommendations 01/2020.

[183] Datatilsynet (2023).

[184] To for overføring av personopplysninger fra behandlingsansvarlig i EØS til behandlingsansvarlig i en tredjestat (Decision 2001/497/EC og 2004/915/EC) og en for overføring av personopplysninger fra behandlingsansvarlig i EØS til databehandler i en tredjestat (Decision 2010/87/EU).

[185] Decision 2021/914/EU.

[186] EDPB Recommendations 01/2020 s. 6.

[187] Ibid s. 14.

relevant, objektiv, pålitelig, verifiserbar og tilgjengelig.[188] Etter retningslinjens vedlegg 3 innebærer det rapporter basert på praktisk erfaring med tidligere tilfeller av pålegg om utlevering fra offentlige myndigheter eller fravær av slike forespørsler.[189] Dersom vurderingen viser at overføringsgrunnlaget ikke sikrer et tilstrekkelig beskyttelsesnivå i praksis, må det iverksettes ytterligere tiltak.[190] Er det ikke mulig, kan overføringen ikke skje. Eksempler på tiltak som kan iverksettes er juridiske, organisatoriske og tekniske.[191] Juridiske og organisatoriske tiltak vil i seg selv ikke være tilstrekkelig uten at det iverksettes tekniske tiltak.[192]

Kommisjonens standard personvernbestemmelser oppstiller avtalevilkår for overføring av personopplysninger mellom behandlingsansvarlige og databehandlere.[193] Klausul 14 i standard personvernbestemmelsene retter seg direkte mot Schrems II. Etter klausul 14 bokstav a til d, plikter partene å garantere at de ikke har noen *grunn til å tro* at lovgivning og praksis i tredjestaten vil hindre partene i å oppfylle deres forpliktelser etter avtalen. Det skal i den forbindelse tas hensyn til konkrete omstendigheter ved overføringen, lovgivning og praksis i tredjestaten, og eventuelle juridiske, tekniske og organisatoriske tiltak. Dataimportører skal garantere at de har gjort sitt ytterste for å få tilgang til relevant informasjon. Partene forplikter seg å dokumentere vurderingene og gjøre dem tilgjengelige for tilsynsmyndigheter på forespørsel. Klausul 14 bokstav e til f gir plikter til dataimportør å varsle dataeksportør dersom den blir kjent med lovgivning og praksis som ikke er forenelig med dere forpliktelser etter standard personvernbestemmelsene. Alt skal dokumenters, lagres og gjøres tilgjengelig for tilsynsmyndighetene på forespørsel.

Det foreligger en diskusjon i det juridiske fagmiljø om reglene i kapittel V åpner for en risikobasert tilnærming, slik som øvrige bestemmelser i personvernforordningen gjør.[194] Personvernrådets første utkast til retningslinjer om ytterligere tiltak ble oppfattet å stenge for praktiske vurderinger av risiko i konkrete overføringstilfeller.[195] EU Kommisjonens utkast til standard personvernbestemmelser åpnet for konkrete risikovurderinger. I en «Joint Opinion» publisert

[188] EDPB Recommendations 01/2020 s. 18.
[189] Ibid. 47
[190] Ibid s. 21.
[191] Ibid s. 22.
[192] Ibid s. 22.
[193] Decision 2021/914/EU vedlegg.
[194] Se eksempelvis Yakovleva (2020) s. 917 og Datatilsynet (2022).
[195] Rode og Ramse (2021).

av Personvernrådet og European Data Protection Supervisor (heretter «EDPS») i januar 2021, sa nevnte aktører seg uenige med Kommisjonens oppfatning av reglene og forståelse av Schrems II.[196] EU Kommisjonen opprettholdt imidlertid sin tolkning av Schrems II ved den endelige utferdigelsen av standard personvernbestemmelsene. Da EDPB publiserte de reviderte retningslinjene 18. juni 2021, åpnet som illustrert disse også for en mer risikobasert tilnærming, ettersom vurderinger kan baseres på praktiske erfaringer med tilsynsmyndigheter i tredjestater.

Overføring etter de forhåndsgodkjente standard personvernbestemmelsene innebærer at dataeksportører må vurdere hvorvidt overføringsgrunnlaget vil sikre et tilstrekkelig beskyttelsesnivå i praksis og eventuelt vurdere hvilke tiltak som kan iverksettes for å sikre et tilstrekkelig beskyttelsesnivå. Å overføre personopplysninger etter de standardiserte personvernbestemmelsene kan følgelig ikke foretas uten en rekke juridiske og tekniske vurderinger, og forutsetter høy kompetanse blant dataeksportører i EU/EØS, både i å vurdere fremmedlovgiving og i å vurdere tekniske løsninger. Det er illustrerende at EU Kommisjonen selv brukte to år på å vurdere personvernet i Japan før de besluttet en adekvansbeslutning.[197] Datatilsynet uttaler på sine hjemmesider at det er viktig at dataeksportører foretar vurderinger samvittighetsfullt etter beste evne og dokumenterer dem godt.[198] I en eventuell tilsynssak vil Datatilsynet være særlig opptatt av at vurderingene er godt dokumentert.[199]

4.4 Overføring av personopplysninger til USA

Overføring av personopplysninger til USA i dag baserer seg i stor grad på standard personvernbestemmelser. Safe Harbour- og Privacy Shield-avtalene var en anerkjennelse av at transatlantiske overføringer er nødvendige for handelsforholdet mellom EU/EØS og USA. Til tross for denne nødvendigheten, ble overføringsgrunnlagene kjent ugyldige. Bruk av standard personvernbestemmelser som overføringsgrunnlag forplikter dataeksportører til å foreta vurderinger og om nødvendig iverksette egnede tiltak.[200] En adekvansbeslutning vil vesentlig forenkle overføringer, og kan følgelig ha stor betydning for den transatlantiske handelen.

[196] EDPB – EDPS Joint Opinion 2/2021 s. 19.
[197] Sandtrø (2020).
[198] Datatilsynet (2023).
[199] Ibid.
[200] Se kapittel 4.3.

På den bakgrunn publiserte Kommisjonen 13. desember 2022 et utkast til en ny adekvansbeslutning kalt EU-U.S. Data Privacy Framework.[201] Om og når en adekvansbeslutning vil komme i stand er fortsatt usikkert. Utkastet kommer som følge av at President Biden 7. oktober 2022 publiserte en såkalt «Executive Order»[202] (heretter «kjennelse» eller «E.O.») etter forhandlinger med Kommisjonen og med det mål å møte kravene i GDPR.[203] Kjennelsen skal imøtegå EU-domstolens konklusjon i Schrems II.[204] Hovedpunktene i Schrems II var at i) amerikansk lovgivning ikke var begrenset til det som er proporsjonalt og nødvendig i henhold til EU pakten artikkel 52 og ii) mangel på håndhevbare rettigheter for de registrerte i strid med EU pakten artikkel 47. I kjennelsen benyttes nå ordlyden «necessary» og «proportionate» tilsvarende EU paktens artikkel 52. Videre er det opprettet en «US Data Protection Review Court» som skal sikre at de registrerte har håndhevbare rettigheter og effektive rettsmidler i USA.

Det er imidlertid flere aktører som har uttalt seg negativt om utkastet til adekvansbeslutningen. Maximiliam Schrems og organisasjonen None of Your Buisness (heretter «NOYB»), argumenterer for at en slik avtale ikke vil stå seg etter personvernforordningen.[205] Det argumenteres for at kjennelsen ikke innebærer en materiell endring av amerikansk overvåkningslovgivning og at «US Data Protection Review Court» ikke tilfredsstiller kravene til en uavhengig domstol etter EU pakten artikkel 47.[206]

Committee on Civil Liberties, Justice and Home Affairs («Komiteen») har også uttalt seg negativt til utkastet.[207] Det fremheves at amerikansk personvernlovgivning ikke er en føderal lov, og at prinsippene om proporsjonalitet og nødvendighet etter amerikansk personvernrett ikke samsvarer med forståelsen av prinsippene i EU-retten. I tillegg peker Komiteen på at president Bidens E.O. ikke er «clear, precise or foreseeable in its application», fordi den på ethvert tidspunkt kan endres av USAs president. Komiteen er videre i likhet med NOYB av den oppfatning av domstolen ikke oppfyller de krav til en uavhengig og upartisk domstol som følger av EU paktens artikkel 47.

[201] Draft Decision (2022).
[202] Executive Order 14086.
[203] EU Kommisjonen (u.å.) c.
[204] The White House (2022).
[205] NOYB (2022) a.
[206] NOYB (2022) b.
[207] Committee (2023).

Personvernrådet på sin side er positive til endringene som følge av kjennelsen og opprettelsen av «US Data Protection Review Court».[208] De uttrykker imidlertid bekymring og ber om avklaring på flere punkter. Blant annet ber EDPB om mer utredning knyttet til rettigheter til de registrerte, videre overføringer, omfanget av unntak, midlertidig masseinnsamling av data og den praktiske funksjonen til «US Data Protection Review Court».

Uttalelsene fra nevnte aktører er ikke juridisk bindende og har av den grunn begrenset rettskildemessig vekt. Særlig gjelder dette uttalelsene fra NOYB. Deres uttalelser kan først og fremst tas til inntekt for at dersom det blir besluttet en adekvansbeslutning av Kommisjonen, vil gyldigheten av overføringsgrunnlaget med høy sannsynlighet tas til EU-domstolen. Hvorvidt avtalen faktisk vil stå seg er vanskelig å vurdere ettersom det er praksisen til amerikanske myndigheter og den ny opprettede domstolen som først og fremst vil være avgjørende for om beskyttelsesnivået er tilstrekkelig. De foreligger på nåværende tidspunkt ikke praksis tilgjengelig for å vurdere hvorvidt dette er tilfellet. Dette illustrerer utfordringer knyttet til å vurdere tredjestaters lovgivning, både for EU Kommisjonen og andre relevante aktører. Det kan imidlertid være grunn til å forvente at amerikanske myndigheter vil å gå langt for å imøtegå de krav reist av EU-domstolen og Kommisjonen, da den transatlantiske handelen er minst like viktig for amerikanske dataimportører.

Forhandlingene mellom Kommisjonen og President Biden, og endringene som følge av kjennelsen illustrerer det politiske aspektet knyttet til adekvansbeslutninger. Etter terrorangrepet den 11. September 2001 har bekjempelse av terrorisme vært en politisk kampsak i landet. Biden-administrasjonen har oppfordret den amerikanske kongressen til å fornye FISA 702.[209] Ifølge Wall Street Journal forventes Biden-administrasjonens oppfordring å være en vanskelig kampanje for å overtale lovgivere til å ikke begrense spionasjemakter.[210] Masseinnhenting av personopplysninger er nemlig ett ledd i bekjempelsen av terrorisme. Balanseringen mellom hensynet til personvernet og øvrige hensyn kan stille seg ulike i EU/EØS og tredjestater. Kravene som oppstilles av EU-domstolen og EU pakten, godtar imidlertid ikke slike uenigheter. Av den grunn er det utfordrende å få på plass adekvansbeslutninger med tredjestater med

[208] EDPB Opinion 5/2023.
[209] Bracy og Bryant (2023).
[210] Ibid.

lovgivning som ikke bygger på den samme forholdsmessige avveiningen av grunnleggende rettigheter i EU pakten. Det kan omtales som en konflikt mellom internasjonal personvernbeskyttelse og særskilte nasjonale regler og hensyn.

4.5 Overføring av personopplysninger til Israel

I 2011 besluttet Kommisjonen at Israel hadde et tilstrekkelig beskyttelsesnivå og tilkjente staten en adekvansbeslutning etter personverndirektivet.[211] Etter personvernforordningens artikkel 45 nr. 9 skal adekvansbeslutninger truffet av Kommisjonen på grunnlag av artikkel 25 nr. 6 i direktivet fortsette å gjelde etter forordningen erstattet direktivet. Politiske utviklinger i Israel kan imidlertid tale for at adekvansbeslutningen står i fare for å bli opphevet.

En forutsetning for at en tredjestat har et tilstrekkelig beskyttelsesnivå, er at de registrerte har håndhevbare rettigheter og effektive rettsmidler i tredjestaten. Det følger ikke uttrykkelig av ordlyden til GDPR artikkel 45, men er et moment i vurderingen av om det skal tilkjennes en adekvansbeslutning etter artikkel 45 nr. 2. I Schrems II ble som nevnt krav om håndhevbare rettigheter og effektive rettsmidler innfortolket i kravet om tilstrekkelig beskyttelsesnivå gjennom EU paktens artikkel 47. [212] EU-domstolen uttalte at:

> "*Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. (...) The very existence of judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law*". [213]

EU paktens artikkel 47 omhandler retten til effektiv klageadgang og rettferdig rettergang. Etter artikkel 47 andre ledd har enhver rett til en rettferdig og offentlig høring innen rimelig tid av en uavhengig og upartisk domstol. EU-domstolens avgjørelse i Schrems II indikerer at en

[211] Decision 2011/61/EU.
[212] Sak C-311/18 avsnitt 95.
[213] Ibid.

adekvansbeslutning tilkjent en tredjestat som ikke har uavhengige eller upartiske domstoler, ikke vil respektere essensen av artikkel 47 i EU pakten og være ugyldig.

Det er på den bakgrunn tatt til orde for at den politiske og rettslige utviklingen i Israel kan innebære at adekvansbeslutningen ikke lenger kan benyttes som et gyldig overføringsgrunnlag.[214] I januar i år la regjeringen frem et forslag om rettsreform. Reformen vil blant annet innebære at regjeringen får større innflytelse på valg av dommere til landets høyesterett, samt at det israelske parlamentet ved simpelt flertall kan overstyre avgjørelser avsagt av Høyesterett.[215] Dersom rettsreformen og nevnte endringer blir vedtatt, vil det innebære at domstolene mister sin uavhengighet og upartiskhet. Dataeksportører som benytter seg av adekvansbeslutningen tilkjent Israel som overføringsgrunnlag kan anbefales å føle den politiske utviklingen i landet og vurdere øvrige overføringsgrunnlag. Dersom rettsreformen går gjennom, er det sannsynlig at Kommisjonen vil oppheve adekvansbeslutningen eller at EU-domstolen vil finne den ugyldig i lys av EU paktens artikkel 47.

Den politiske utviklingen i Israel og følgene det kan få for landets adekvansbeslutning illustrerer igjen det politiske aspektet ved overføringsreglene. Etter EU paktens artikkel 2 følger det at Den europeiske union er «founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights [...].» Uavhengige og upartiske domstoler er en forutsetning for disse verdiene, særlig demokratiet. Ikke-demokratiske stater vil vanskelig oppfylle de krav som stilles av EU pakten, og derfor ikke tilkjennes adekvansbeslutninger. Ettersom bruk av adekvansbeslutninger forenkler overføringer, vil det trolig påvirke hvilke tredjestater som er attraktive handelsaktører for EU/EØS-statene.

[214] Spiro (2023).
[215] Judin (2023).

5 Konklusjon og avsluttende betraktninger

Funn i avhandlingen viser at det foreligger uavklarte spørsmål knyttet til overføring av personopplysninger til tredjestater og rekkevidden av overføringsbegrepet. Det er ikke uvanlig at det oppstår behov for rettslig avklaringer når nye forordninger blir etablert. Den rettslige tvilen knyttet til forordningens overføringsregler har imidlertid ført til at domstoler og tilsynsmyndigheter i EU/EØS-landene har tolket reglene ulikt. Resultatet er uønsket da forordningen ble etablert med formål å sikre rettslikhet innad i EU/EØS, og det er behov for rettslige avklaringer. Det er særlig tre forhold som bidrar til utfordringer ved tolkningen av bestemmelsene i kapittel V: i) uklar lovtekst, ii) tredjestaters lovgivning og praksis og iii) den raske teknologiske utviklingen.

Mangel på en klar definisjon av begrepet «overføring» i personvernforordningen har medført inkonsekvent anvendelse av regelverket i EUs medlemsstater.[216] På den bakgrunn publiserte EDPB retningslinjer knyttet til begrepet.[217] Likevel er flere spørsmål fortsatt ikke avklart. Fra et normativt perspektiv er det ikke bærekraftig. Usikkerheter knyttet til begrepets rekkevidde kan medføre at behandlingsansvarlige og databehandlere foretar risikovurderinger fremfor å benytte seg av overføringsgrunnlag, noe som kan medføre at personvernet til de registrerte og tilliten til regelverket minsker. Hvorvidt en operasjon er underlagt reglene i kapittel V, bør være klart.

Det er videre et kompliserende moment at overføringsreglene er generelt utformet, og ikke tar høyde for forhold ved de konkrete overføringene.[218] Reglene i personvernforordningen kapittel V skal sikre at personvernet ikke undergraves når personopplysninger overføres til tredjestater.[219] Samtidig er formålet å sikre fri flyt av personopplysninger innad i EØS, samt fremme den økonomiske veksten og utviklingen i markedet.[220] Det må følgelig balanseres mellom vernet til personopplysninger og et system som kan fungere i det virkelige liv, for å unngå å bremse den økonomiske veksten ved å innføre et omfattende og komplisert regelverk. Balansegangen er utfordrende, og utviklingen så langt kan indikere at det fortsatt jobbes med å finne den. Den

[216] Se kapittel 3.3.3.
[217] Se kapittel 3.2.4.
[218] Se kapittel 3.2.2.
[219] Se kapittel 3.2.3.
[220] Ibid.

absolutte tilnærming til hvilken kategori av personopplysninger som overføres er ikke godt begrunnet.[221] Hvilke personopplysninger som overføres har betydning for risikoen for vernet til de registrerte, og bør følgelig hensyntas ved spørsmålet om reglene i kapittel V skal komme til anvendelse.

Avhandlingens kapittel 4 viser utfordringer knyttet til bruk av overføringsgrunnlag som i utgangspunktet var utferdiget for å sikre at de registrertes personvern ikke undergraves ved overføringer til tredjestater. Som følge av at EU-domstolen fant standard personvernbestemmelser i seg selv utilstrekkelige som overføringsgrunnlag er vurderinger som tidligere lå hos Kommisjonen lagt til den enkelte dataeksportør.[222] Bruk av standard personvernbestemmelser innebærer da at dataeksportører må foreta kompliserte vurderinger. Det er først og fremst ikke den teknologiske utviklingen som gjør vurderingene utfordrende, med tredjestaters lovgivning og praksiser. Dette er forhold som Kommisjonen kunne forutse og tatt hensyn til ved utformingen av standard personvernbestemmelsene. Lovgiver kunne også hensyntatt disse elementene ved utformingen av GDPR. Å flytte kompliserte og utfordrende vurderinger over på dataeksportørene kan medføre en vesentlig risiko for personvernet til de registrerte. Etterfølgende kontroll og ileggelse av overtredelsesgebyrer for gale vurderinger, vil ikke veie opp for den skade overføringen kan påføre den registrerte.

Adekvansbeslutninger vesentlig forenkler overføringer til tredjestater for dataeksportører. På grunn av nasjonale hensyn og regler vil adekvansbeslutninger ikke kunne tilkjennes enhver tredjestat.[223] Av den grunn vil dataeksportører måtte forholde seg til standard personvernbestemmelser og de utfordrende vurderingene fremover. Frykten for sanksjoner kan medføre at dataeksportører er tilbakeholdne, og i ytterste fall stanse overføringer til tredjestater. Det vil ha negative konsekvenser for næringslivet i EU/EØS og europeiske borgeres velferd. Omfattende vurderinger kan ha samme effekt. Dataflyt er viktig for økonomisk vekst.

Avslutningsvis kan det gis den betraktning at det er utfordrende å regulere et område som har et høyt teknologisk utviklingstempo. Et gap mellom juridiske konsepter og tekniske realiteter kan i ytterste fall medføre et svekket personvern og sikkerhet. Denne betraktningen gjør seg

[221] Se kapittel 3.2.2 og 3.2.3.
[222] Se kapittel 4.3.
[223] Se kapittel 4.4 og 4.5.

gjeldende på flere områder enn personvern. Lovgiver kan møte store utfordringer i fremtiden som følge av omfattende og langvarige lovgivningsprosesser. Slike utfordringer kan søkes å imøtegås gjennom bruk av tolkningsprinsipper, særlig tolkningsprinsippet i GDPR om teknologisk nøytralitet. Dette tolkningsprinsippet antas derfor å bli mer og mer sentralt i tiden fremover.

6 Litteraturliste

6.1 Lover

1992	Lov av 27. november 1992 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) (EØS-loven).
2018	Lov av 15. juni 2018 om behandling av personopplysninger (personopplysningsloven).

6.2 Traktater og konvensjoner

EU pakten	Charter of Fundamental Rights of the European Union (2012/C 326/02) (EUs pakt om grunnleggende rettigheter).
EØS-avtalen	Agreement on the European Economic Area (AVT-1992-05-02-1) (Avtale om det europeiske økonomiske samarbeidsområde).

6.3 Direktiver og forordninger

Alle kilder sitert fra lovdata.no eller eur-lex.eu.

Direktiv 95/46 EF	EUROPAPARLAMENTS- OG RÅDSDIREKTIV 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling

	av personopplysninger og om fri utveksling av slike opplysninger [Personverndirektivet].
Forordning 2016/679 EU	EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) [GDPR].
Direktiv 2001/29 EF	Europaparlaments- og rådsdirektiv 2001/29/EF av 22. mai 2001 om harmonisering av visse sider ved opphavsrett og beslektede rettigheter i informasjonssamfunnet. [Infosoc-direktivet – Opphavsrettsdirektivet].
Direktiv 2016/2102 EU	Europaparlaments- og rådsdirektiv (EU) 2016/2102 av 26. oktober 2016 om tilgjengeligheten av offentlige organers nettsteder og mobilapplikasjoner

6.4 Beslutninger fra EU Kommisjonen

Alle kilder sitert fra eur-lex-eu.

Decision 2000/520/EC	Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441).

Decision 2011/61/EU	Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data (notified under document C(2011) 332).
Decision 2016/1250/EU	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).
Decision 2021/914/EU	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) 2016/679 of the European Parliament and of the Council.

6.5 Internasjonal rettspraksis

6.5.1 Rettspraksis fra EU-domstolen

Sak C-101/01	Lindqvist v. Sverige [ECLI:EU:C:2003:596]
Sak C-311/18	Schrems II [ECLI:EU:C:2020:559]
Sak C-325/14	SBS Belgium [ECLI:EU:C:2015:764]
Sak C-362/14	Schrems I [ECLI:EU:C:2018:309]

Sak C-480/10	Kommisjonen v. Sverige [ECLI:EU:C:2013:263]
Sak C-582/14	Breyer v. Tyskland [ECLI:EU:C:2016:779]
Sak C-507/17	Google LLC, successor in law to Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL) [ECLI:EU:C:2019:772]

6.5.2 Rettspraksis fra Menneskerettighetsdomstolen

S. and Marper v. The United Kingdom	Case of S. and Marper v. The United Kingdom. Application nr. 30562/04 og 30566/04, 4. desember 2008.

6.6 Retningslinjer, veiledere mv.

A29WP Opinion 4/2007	Article 29 Data Protection Working Party, *Opinion 4/2007 on the concepts of personal data*, 01248/07/EN WP136 [Tilgjengelig på https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf].
Datatilsynet (2015)	Datatilsynet, Veiledning publisert av Datatilsynet https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/veiledere/anonymisering-veileder-041115.pdf.
Draft Decision (2022).	Draft Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate

	level of protection of personal data under the EU-US Data Privacy Framework.
EDPB – EDPS Joint Opinion 2/2021	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.
EDPB Guidelines 2/2018	European Data Protection Board, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, Adopted 25. May 2018.
EDPB 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 GDP, Adopted 14 February 2023. Version 2.0.
EDPB Recommendations 01/2020	Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Adopted 18 June 2021. Version 2.0.
EDPB Opinion 5/2023	Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, Adopted on 28 February 2023.

6.7 Rettskilder fra utenlandske domstoler og tilsynsorganer

CE – 450163 — Kilde lest via en datamaskinoversettelse hentet på GDPR Hub: CE - 450163 - GDPRhub hentet 28. april 2023.

1 VK 23/22 — Kilde lest via en datamaskinoversettelse hentet på GDPR Hub: VK Baden-Württemberg - 1 VK 23/22 - GDPRhub hentet 28. april 2023.

Det danske Datatilsynet (2022) — Det danske Datatilsynet. «Vedrørende tilsigtede eller utilsigtede overførsler til tredjelande.» (29.03.2022) Vedrørende tilsigtede eller utilsigtede overførsler til tredjelande (datatilsynet.dk) hentet 28. april 2023.

DSK beslutning av 31.01.2023 — Kilde lest via artikkel publisert på German DSK Publishes Decision on the Data Protection Assessment of Access Possibilities of Third Country Public Authorities to Personal Data | Inside Privacy hentet 28. april 2023.

6.8 Juridisk litteratur

6.8.1 Bøker

Arnesen (2015) — Arnesen, Finn og Are Stenvik. *Internasjonalisering og juridisk metode.* 2. utg., Oslo: Universitetsforl. 2015.

Krzysztofek (2021) — Krzysztofek, Mariusz. *GDPR: Personal Data Protection in the European Union*. Nederland: Kluwer Law International B.V., 2021.

Kuner (2020) a — Kuner, Christopher. *The EU General Data Protection Regulation (GDPR): A Commentary*. New York: Oxford Academic, 2020.

Naef (2023) — Naef, Tobias. "Concluding Remarks: Data Protection Without Protectionism." I *European Yearbook of International Economic Law*. Springer, Cham, 2022. Concluding Remarks: Data Protection Without Data Protectionism | SpringerLink.

Serjersted (2011) — Sejersted, Fredrik mfl. *EØS-RETT*. 3. utg., Oslo: Universitetsforl., 2011.

Skullerud mfl. — Åste Marie Bergseng Skullerud mfl., *Personopplysningsloven og personvernforordningen (GDPR). Kommentarutgave*. Oslo: Universitetsforl., 2019.

Yakovleva (2020) — Yakovleva, Svetlana. *Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities'*. I The Journal of World Investment & Trade 21, 6, 2020. Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities' in: The Journal of World Investment & Trade Volume 21 Issue 6 (2020) (brill.com).

6.8.2 Artikler

Hauglid (2022) — Mathias K. Hauglid og Karl Øyvind Mikalsen, «Tilgang til helseopplysninger i maskinlæringsprosjekter.» Lov og rett 2022/7, Juridika, 14. september 2022, Tilgang til helseopplysninger i maskinlæringsprosjekter» hentet 4. mai 2023.

Kuner (2020) b — Christopher Kuner. «The Schrems II judgment of the Court of Justice and the future of data transfer regulation.» European Law Blog, 17. juli 2020, The Schrems II judgment of the Court of Justice and the future of data transfer regulation – European Law Blog hentet 7. april 2023.

Ødegaard (2023) — Magnus Ødegaard. «Er Google Analytics Ulovlig å bruke i Norge nå?» Finansavisen, 4. mars 2023 Er Google Analytics ulovlig å bruke i Norge nå? | Finansavisen hentet 20. april 2023.

6.9 Andre kilder

6.9.1 Kommentarer til utkast

University of Lyon (2022) — Students of the LL.M Digital Law and Technology, Catholic University of Lyon, Comments on the EDPB Guidelines 05/2021, tilgjengelig på

Microsoft Word - Public Consultation LL.M Lyon.docx (europa.eu) hentet 30. april 2023.

Committee (2023) Committee on Civil Liberties, Justice and Home Affairs. Draft Motion for a Resolution. Tilgjengelig på RD_Statements (europa.eu).

6.9.2 Nettsider

Bracy og Bryant (2023) Bracy, Jedidiah og Jennifer Bryant. «EDPB welcomes 'improvements' to the EU-US adequacy decision, concerns remain.» 28. februar 2023 EDPB welcomes 'improvements' to EU-US adequacy decision, concerns remain (iapp.org) hentet 30. april 2023.

Datatilsynet (2019) Datatilsynet. «Behandlingsansvarlig og databehandler.» 17. juli 2019 Behandlingsansvarlig og databehandler | Datatilsynet hentet 30. april 2023.

Datatilsynet (2022) Datatilsynet. «Digir, DFØ og Datatilsynet følger opp veileder.» 28. september 2022 Digdir, DFØ og Datatilsynet følger opp veileder | Datatilsynet hentet 17. april 2023.

Datatilsynet (2023) Datatilsynet. «Overføring av personopplysninger ut av EØS.» 16. mars 2023 Overføring av personopplysninger ut av EØS | Datatilsynet hentet 17. april 2023.

EDPB (u.å) European Data Protection Board. «Endorsed WP29 Guidelines.» U.å. https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en hentet 17. april 2023.

EU Kommisjonen (u.å.) a EU Kommisjonen. «Annual reports on the application of the Charter.» U.å. Annual reports on the application of the Charter (europa.eu) hentet 17.04.2023.

EU Kommisjonen (u.å.) b EU Kommisjonen. «Adequacy decision.» U.å. Adequacy decisions (europa.eu) hentet 30. april 2023.

EU Kommisjonen (u.å.) c EU Kommisjonen. «Commercial sector: launch of the adoption procedure for a draft adequacy decision on the EU-U.S. Data Privacy Framework." U.å.https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en hentet 29. april 2023.

EU Kommisjonen (2023) EU Kommisjonen. «D2.4 Second Report on Facts and Figures.» Februar, 2023. Tilgjengelig på: Results of the new European Data Market study 2021-2023 | Shaping Europe's digital future (europa.eu) hentet 17. april 2023.

Judin (2023) Judin, Tobias. «Reisebrev fra Israel». 7. februar 2023 Reisebrev fra Israel - Personvernbloggen hentet 17. april 2023.

NOYB (2022) a — NOYB. «Statement on EU Comission adequacy decision on US.» 13. desember 2022 Statement on EU Comission adequacy decision on US (noyb.eu) hentet 17.04.2023.

NOYB (2022) b — NOYB. «Open Letter on the Future of EU-US Data Transfers.» 23. mai 2022 Open Letter on the Future of EU-US Data Transfers (noyb.eu) hentet 4. mai 2023.

Nätt (2022) — Nätt, Tom Heine. ”skytjeneste.” 21. desember 2022. https://snl.no/skytjeneste hentet 7. april 2023.

Restad, Notaker og Mæhlum (2023) — Restad, Hilde, Hallvard Notaker og Lars Mæhlum. «Edward Snowden.» 21. april 2023 https://snl.no/Edward_Snowden hentet 23. april.

Rode og Ramse (2021) — Rode, Ane og Jostein Ramse. «Endelig veileder om Schrems II fra Personvernrådet – større åpning for risikobasert tilnærming.» Endelig veileder om Schrems II fra Personvernrådet - større åpning for risikobasert tilnærming - Føyen (foyen.no) hentet 2 mai. 2023.

Spiro (2023) — Spiro, James. «EU would view Israel “in the same category as China” if judicial reforms go through.» 2. februar 2023 EU would view Israel “in the same category as China” if judicial reforms go through | Ctech (calcalistech.com) hentet 17. april 2023.

Sandtrø (2020) — Sandtrø, Jan. «Overføring av personopplysninger utenfor EØS-området – hva gjør vi etter Schrems

II?» 27. november 2020 Overføring av person-opplysninger utenfor EØS-området – hva gjør vi etter Schrems II? (linkedin.com) hentet 1. mai 2023.

The White House (2022) The White House. «FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework.» https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/ hentet 4. mai 2023.