UiO : Det juridiske fakultet

Bruk av skytjenester i EØS som er underlagt tredjelands lovgivning

Når er det en «overføring», skal et forbehold om utlevering anses som «instrukser» og hvilken tilnærming skal man bruke for å vurdere krav til supplerende beskyttelsestiltak der det i utgangspunktet ikke skjer en overføring til tredjeland?

Kandidatnummer: 522

Leveringsfrist: 25. april 2023

Antall ord: 15 284

Innholdsfortegnelse

1 Innledning

1.1 Tema og problemstilling

Temaet for oppgaven er bruk av skytjenester i EØS som er underlagt tredjelands lovgivning. Nærmere bestemt skal oppgaven ta for seg noen problemstillinger som har til felles at de gjelder dels uavklarte og vanskelige spørsmål og vurderinger som behandlingsansvarlige må gjøre ved valg av skytjenesteleverandører og ved opprettelse av skytjenesteavtaler, i grenseflaten mellom kapittel IV og V i General Data Protection Regulation (heretter kalt «GDPR» eller «forordningen».

Bruk av skytjenester har doblet seg for bedrifter i hele EU mellom 2016 og 2021.[1] Særlig i offentlig sektor har COVID-19 pandemien intensivert en digital transformasjon av organisasjoner som i større grad benytter seg av skytjenester. Imidlertid kan mange organisasjoner møte vanskeligheter med å anskaffe IT-produkter og tjenester som overholder EUs regler for databeskyttelse. På grunn av arten av dataene som behandles og den (potensielt) store mengden data som lagres i sky, er det av stor betydning at den grunnleggende retten til beskyttelse av personopplysninger er garantert.[2]

Når personopplysninger behandles i EØS er de beskyttet av reglene i GDPR og andre regler på EU- og medlemsstatsnivå. Derimot når personopplysninger overføres utenfor EØS er nivået for beskyttelse av individers rettigheter og friheter muligens lavere enn det som tilbys av det juridiske rammeverket i Unionen.[3]

Overføring av personopplysninger mellom stater er likevel nødvendig for å kunne utvide internasjonal handel og internasjonalt samarbeid, men dette skaper nye utfordringer og bekymringer med tanke på vern av personopplysninger jf. forordningens fortalepunkt 101. Hovedformålet med reglene om overføring av personopplysninger i GDPR kap. V er å hindre at det felles europeiske beskyttelsesnivået undergraves i en tid preget av utfordringer i form av løpende teknologisk utvikling og økt globalisering.[4]

Å bruke en skytjeneste med servere i EØS er i utgangspunktet ikke en overføring av personopplysninger til tredjeland i henhold til forordningens kap. V, men personopplysninger kan likevel ende opp i ikke-adekvate tredjeland dersom skyleverandøren er underlagt tredjelands

[1] Eurostat (2021).

[2] 2022 Coordinated Enforcement Action, s. 5.

[3] Guidelines 05/2021 (2.0), avsnitt 2.

[4] Skullerud mfl. (2018), s. 367.

lovgivning. Det blir dermed nødvendig for den behandlingsansvarlige å gjøre ytterligere vurderinger for å sørge for at beskyttelsesnivået ikke undergraves.[5]

For den behandlingsansvarlige er det viktig å vite hva som eventuelt utgjør en «overføring» i henhold til GDPR kap. V ettersom dette er en forutsetning for at kapitlet kommer til anvendelse, jf. GDPR art. 44. Det er også viktig å vite hvem som er behandlingsansvarlig(e) for den mulige overføringen, jf. bl.a. GDPR art. 5 nr. 2 Deretter må man finne ut av hva slags tiltak man kan iverksette og hva som er tilstrekkelige tiltak i denne konteksten, jf. bl.a. GDPR art. 32.

Oppgavens første problemstilling tar for seg hvordan «overføring» etter GDPR kapittel V skal forstås, herunder hvorvidt overføringsbegrepet omfatter «tilgjengeliggjøring» (pkt. 2).

Oppgavens andre problemstilling undersøker hvorvidt et forbehold om utlevering anses som «instrukser» fra den behandlingsansvarlige, og subsidiært: forutsatt at det er en instruks, hvorvidt behandlingsansvarlig har lov til å gi en slik instruks (pkt. 3).

Oppgavens tredje problemstilling undersøker hvilke vurderinger behandlingsansvarlig må gjøre når en skytjenesteleverandør potensielt kan overføre personopplysninger til tredjeland, herunder hvilken tilnærming man skal bruke for å vurdere krav til supplerende beskyttelsestiltak (pkt. 4).

1.2 Bakgrunn og aktualitet

Bakgrunnen for temaet er blant annet sak C-311/18 (Schrems II) fra juli 2020 som oppstiller skjerpede krav til overføring av personopplysninger ut av EU/EØS. Dommen oppstod som følge av en klage fra Maximillian Schrems, der han i korte trekk ba om at Facebook Ireland skulle forbys å overføre hans personopplysninger til USA, på bakgrunn av at loven og praksisen i landet ikke sikrer tilstrekkelig beskyttelse av personopplysninger mot overvåkningsaktiviteter som offentlige myndigheter er engasjert i.[6] I dommen ble Privacy Shield-avtalen mellom EU og USA underkjent fordi den ikke ga godt nok vern mot amerikansk masseovervåkning og etterretning.[7]

Et av spørsmålene som ble behandlet var hvilken beskyttelsesgrad som kreves av GDPR art. 46 nr. 1 og 46 nr. 2 bokstav c, ved overføring av personopplysninger til en tredjestat basert på standardkontrakter (Standard Contractual Clauses – SCC) vedtatt av Europakommisjonen, jf.

[5] Datatilsynet (2023c).

[6] C-311/18 Schrems II, avsnitt 52.

[7] Ibid, avsnitt 201.

GDPR art. 46 nr. 2 bokstav c.[8] Domstolen bemerket i Schrems II at selv om artikkel 46 ikke angir hva som kreves av «tilstrekkelige sikkerhetstiltak», «håndhevbare rettigheter» og «effektive rettsmidler», står den likevel plassert i kapittel V i forordningen, og må derfor leses i lys av artikkel 44, med tittelen «Generelt prinsipp for overføring», som fastslår at alle bestemmelser i kapitlet skal få anvendelse for å sikre at det nivået for vern av fysiske personer som garanteres i denne forordning, ikke undergraves. Dette beskyttelsesnivået må derfor sikres uavhengig av hvilken bestemmelse i kapittelet overføringen av personopplysninger til en tredjestat er basert på.[9] Imidlertid kreves det ikke at sikkerhetsnivået er identisk med det som er garantert EUs rettsorden, men begrepet «tilstrekkelig beskyttelsesnivå» skal forstås slik at det krever et beskyttelsesnivå som er «essentially equivalent» - vesentlig det samme.[10]

Standardkontrakter er kontraktuelle i natur og er ikke bindende for tredjestaters offentlige myndigheter. I denne forbindelse uttaler domstolen at det kan være nødvendig for den behandlingsansvarlige å supplere med ytterligere beskyttelsestiltak.[11] Hvorvidt lovgivningen i en tredjestat gir tilstrekkelig beskyttelse må vurderes fra sak til sak.[12] Dommen sier derimot ikke noe konkret om hva de supplerende beskyttelsestiltakene skal gå ut på, eller hvordan vurderingen skal foretas.

Ettersom Privacy Shield er underkjent må virksomheter ty til andre behandlingsgrunnlag. Det mest brukte overføringsgrunnlaget er Standardkontrakter, jf. GDPR art. 46 nr. 2 bokstav c. Frem til nyere tid har standardkontraktene vært basert på gammelt regelverk. I etterkant av Schrems II har EU-kommisjonen vedtatt nye som er basert på GDPR og som tar høyde for Schrems II-dommen ved at den inneholder bestemmelser som reflekterer tilleggspliktene som dommen gir.[13]

Dette løser imidlertid ikke alt. Problemet for potensielle dataeksportører er i første rekke at det er usikkerhet rundt definisjonen av «overføring». Deretter er det utfordrende å vurdere tredjelands lovgivning og hvorvidt tredjelands etterretningslovgivning ikke er til hinder for etterlevelse av standardkontraktens innhold. Til slutt er det vanskelig å identifisere passende tilleggstiltak ettersom Schrems II er taus om dette.

I etterkant av dommen har dermed EDPB sett seg nødt til å veilede behandlingsansvarlige og databehandlere rundt denne problematikken.

---

[8] Ibid, avsnitt 90.

[9] Ibid, avsnitt 92.

[10] Ibid, avsnitt 94.

[11] Ibid, avsnitt 132 og 133.

[12] Ibid, avsnitt 134.

[13] Datatilsynet (2021).

Blant annet har EDPB kommet med en veileder om «measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data» (Andre versjon vedtatt 18. Juni 2021). Formålet med denne veilederen er å hjelpe behandlingsansvarlige og databehandlere som overfører personopplysninger til tredjeland med den komplekse oppgaven å vurdere tredjeland og identifisere passende tilleggstiltak der det er nødvendig.

EDPB har også kommet med en veileder om «the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V og the GDPR» (Første versjon vedtatt 18 november 2021. Andre versjon vedtatt februar 2023). Denne forsøker å bistå behandlingsansvarlige og databehandlere i EU med å identifisere om en behandling utgjør en overføring til et tredjeland/internasjonal organisasjon, og følgelig hvorvidt de må overholde bestemmelsene i GDPR kap. V.

Det norske datatilsynet (heretter kalt Datatilsynet) og Digitaliseringsdirektoratet m/DFØ på oppdrag fra SKATE (heretter kalt SKATEs veileder) har kommet med hver sin veileder om overføring til tredjeland. Datatilsynet sin veileder følger i stor grad EDPB sin, mens SKATE sin skiller seg ut på noen vurderingstemaer. Intensjonen var å lette arbeidet med de krevende vurderingene, men avstanden mellom myndighetene har i stedet bidratt til økt forvirring.[14]

Med dette som bakgrunn inviterte advokatfirmaet Simonsen Vogt Wiig Datatilsynet og Digdir til paneldebatt om bruk av skytjenester etter Schrems II 30. november 2022. Her ble det blant annet diskutert hva som menes med «overføring» i praksis, hvorvidt forbehold utgjør instruks og hvilke vurderingstemaer EU-domstolen legger opp til når det gjelder overvåking. Representanten fra Datatilsynet hevdet blant annet at SKATEs veileder er for de som ønsker å utfordre rettssystemet og at de er mer opptatt av å definere seg ut av ansvar. Representanten fra Digdir hevdet på sin side at skytjenester må vurderes riktig og at man må ha et realistisk bilde av risiko.[15]

I etterkant av paneldebatten har begge veilederne blitt endret til å samsvare mer og Datatilsynet og Digdir/DFØ er ikke like uenig som først antatt, men det gjenstår fortsatt noen spørsmål som denne oppgaven forsøker å svare på. På den ene siden gir alle veilederne en viss avklaring rundt en del spørsmål, men skaper samtidig mye usikkerhet når de avviker fra hverandre.

[14] Olsen og Tønseth (2022).

[15] Opptak av paneldebatten kan finnes her: https://svw.no/artikler/full-forvirring-om-skytjenester

1.3 Avgrensninger

Oppgaven avgrenses til vurderinger som må gjøres ved bruk av skytjenesteleverandører geografisk lokalisert i EØS, men som er underlagt tredjelands lovgivning.

Den tenkte situasjonen og forutsetningen for problemstillingene er denne:[16] Et norsk selskap X er behandlingsansvarlig og engasjerer en skytjenesteleverandør Y geografisk lokalisert i EØS som databehandler. Selskapet Y er et datterselskap av et tredjelandsbasert morselskap Z. Selskapet Y behandler dataene til selskapet X utelukkende i EØS. Ingen land utenfor EØS, og heller ikke morselskapet Z har tilgang til dataene. Videre følger det av databehandleravtalen mellom X og Y at selskapet Y kun skal behandle personopplysninger på dokumenterte instrukser fra selskapet X. Selskapet Y er imidlertid underlagt tredjelandslovgivning med ekstraterritoriell virkning, noe som i dette tilfellet betyr at selskapet Y kan motta tilgangsanmodninger fra tredjelandsmyndigheter. Siden selskapet Y ikke er i et tredjeland (men et EU-selskap underlagt artikkel 3 nr. 1 GDPR), utgjør ikke utlevering av data fra den behandlingsansvarlige X til databehandleren Y en overføring, og kapittel V GDPR gjelder ikke. Som nevnt er det imidlertid en mulighet for at selskapet Y mottar tilgangsanmodninger fra tredjelandsmyndigheter, og dersom selskapet Y etterkommer en slik anmodning, ville en slik utlevering av data bli ansett som en overføring i henhold til GDPR kapittel V.

Dette er utgangspunktet for alle de tre problemstillingene, med noen modifikasjoner. I pkt. 2 om «overføring» tenkes at det i tillegg er en underdatabehandler i et tredjeland som får fjerntilgang til dataene som lagres i EØS for supportformål. I pkt. 3 om «instrukser» tenkes det at databehandleravtalen inneholder et forbehold om utlevering av personopplysninger til tredjeland.

Hver problemstilling berører temaer som det kan skrives mer utdypende om, men oppgaven avgrenses mest mulig til det som er mer særegent for situasjonen beskrevet ovenfor – bruk av skytjenester i EØS som er underlagt tredjelands lovgivning.

1.4 Rettskilder og metode

1.4.1 Gjennomføring av Personvernforordningen i norsk rett

Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven) angir at forordning (EU) 2016/679 (GDPR), gjelder som norsk lov, jf. § 1. Regulering av personvern i forordning i stedet for direktiv får visse konsekvenser. Ved bruk av et direktiv har hvert land muligheten til å bestemme hvordan direktivet skal innføres i nasjonal lovgivning, noe som gir

[16] Sml. med Guidelines 05/2021 (2.0), s. 13. Eksempel 12.

rom for nasjonale variasjoner og særpreg. Dette resulterer i at bestemmelsene i hvert land blir likeartede, men ikke identiske. I motsetning til direktiver, gjelder forordninger direkte i alle EU-medlemsland, samt i Norge når forordningen er inkludert i EØS-avtalen. Dette innebærer at de samme bestemmelsene gjelder "ord for ord" i alle disse landene og skal i utgangspunktet tolkes og praktiseres likt i alle land.[17]

1.4.2 EU-rett som norsk rettskilde

Når norske rettsanvendere skal forholde seg til EU-rett, må de først ta stilling til innholdet i den aktuelle EU-regelen. Dette tolkningsspørsmålet må avgjøres basert på rettskildeprinsippene som gjelder i EU-retten I norsk litteratur er det vanlig å behandle de ulike avtalene med EU separat. Dette resulterer i at EØS-avtalen ofte får mest oppmerksomhet, og at det EØS-rettslige homogenitetsprinsippet fremstilles på en måte som kan gi inntrykk av at dette er et unikt tolkningsprinsipp som kun gjelder innenfor EØS-rettens område. I realiteten er homogenitetsprinsippet bare et navn på formålet om ensartet («homogen») fortolkning av EØS-avtalen og de underliggende delene av EU-retten som er tatt inn i avtalen. Tilsvarende målsettinger ligger også til grunn for de andre avtalene som knytter Norge til EU-retten.[18]

En helhetlig tilnærming til EU-rett som rettskilde i norsk rett er en naturlig tilnærming ettersom alle Norges avtaler med EU gjelder (forskjellige deler av) det som fra EU-domstolens ståsted utgjør ett helhetlig, overnasjonalt rettssystem. EU-domstolens metodiske tilnærming er grunnleggende sett den samme uavhengig av hvilke deler av EU-retten som står til prøve i en sak.[19]

Sondringen mellom primærrett og sekundærrett er grunnleggende i EU-retten. Primærretten består av traktatene – først og fremst traktaten om Den europeiske union (TEU) og traktaten om Den europeiske unions virkemåte (TEUV) – supplert med EUs pakt om grunnleggende rettigheter og de generelle EU-rettslige prinsippene som EU-domstolen har utviklet. Sekundærretten består av alle de rettsakter (forordninger, direktiver og beslutninger) som EU-institusjonene har vedtatt med utgangspunkt i de kompetansegrunnlagene som traktatene etablerer. Primærretten er lex superior, og sekundærretten må følgelig tolkes i overensstemmelse med primærretten.[20]

EU-retten kjennetegnes også av grunnprinsippene om myndighetstildeling, nærhet og forholdsmessighet. I henhold til EU-traktaten artikkel 5 har EU bare den myndighet som

[17] Schartum (2020), s. 17.
[18] Fredriksen og Mathisen (2019), s. 387.
[19] Ibid, s. 388.
[20] Ibid, s. 396.

medlemsstatene har tillagt Unionen gjennom traktatene, og denne myndigheten kan bare utøves dersom og så langt formålet ikke kan ivaretas av medlemsstatene Til dette kommer den særegne institusjonelle balansen som ligger under utformingen av de ulike hjemmelsgrunnlagene i traktatene. Forordninger, direktiver og beslutninger må derfor ikke bare fortolkes i overensstemmelse med materielle rettsregler i primærretten, men også på et vis som ikke går ut over det aktuelle hjemmelsgrunnlagets rekkevidde.[21] I kontekst av GDPR er det artikkel 8 nr. 1 i Charteret (Charter of Fundamental Rights of the European Union) og artikkel 16 nr. 1 i TEUV som er aktuelle hjemmelsgrunnlag.

Ettersom denne oppgaven skal tolke flere begrep i GDPR er det relevant å gå nærmere inn på sentrale trekk ved EU-domstolens tolkningsmetode.

EU-rettslige bestemmelser skal som utgangspunkt og hovedregel gis en autonom og ensartet fortolkning. Det vil si at de skal tolkes på samme måte uavhengig av nasjonal begrepsbruk, nasjonal juridisk metode og nasjonal rettskultur. Selvstendig og ensartet fortolkning bidrar til å gi EU-retten likt innhold i hele EU, og dermed til å sikre at rettigheter og plikter etter EU-retten gjelder likt for alle.[22] Der et ord eller et uttrykk ikke er nærmere definert, skal fortolkningen ta utgangspunkt i den «sædvanlige betydning i almindelig sprogbrug».[23] Dette kan by på problemer der ulike språkversjoner har sprikende ordlyd, men for denne oppgavens vedkommende byr ikke dette på særlige problemer. Når det nedenfor gjøres tolkninger av den norske oversettelsen er dette fordi jeg anser tolkningsalternativene som gjeldende for både den norske oversettelsen og den engelske språkversjonen.

EU-domstolen opererer videre med et skille mellom kontekstuell og formålsorientert fortolkning. Kontekstuell tolkning innebærer at EU-rettslige bestemmelser tolkes i lys av den sammenhengen som de inngår i. Dette dekker alt fra fortolkning i lys av den umiddelbare sammenhengen som et ord eller uttrykk inngår i, til fortolkning i lys av grunnleggende rettigheter. EU-rettslige bestemmelser skal så langt som mulig tolkes i overensstemmelse med EU-retten som et hele. Av betydning er også sammenhenger og systematikk, slik som oppbygning, kapittelinndeling og nærmere plassering av bestemmelser, forholdet til andre regelsett osv.[24]

Formålsorientert fortolkning innebærer at EU-rettslige bestemmelser fortolkes slik at formålet fremmes, eller i det minste slik at måloppnåelsen ikke hindres.[25] Prinsipper og regler for å

[21] Ibid, s. 396 og 397.
[22] Ibid, s. 403.
[23] C-201/13 Deckmyn, avsnitt 19.
[24] Fredriksen og Mathisen (2019), s. 405.
[25] Ibid, s. 410.

beskytte individer i forbindelse med behandling av deres personopplysninger bør ivareta deres grunnleggende rettigheter og friheter, spesielt retten til vern av personopplysninger. Målet med GDPR er å fremme et område for frihet, sikkerhet og rettferdighet, samt en økonomisk union, og bidra til økonomisk og sosial utvikling. Dette inkluderer å styrke økonomiene i det indre markedet, samt å forbedre individets velferd, jf. fortalepunkt nr. 2.

Rettspraksis fra EU-domstolen anses ikke som bindende prejudikater, men de har med årene fått karakter av tungtveiende rettskilder som det kreves gode grunner for å fravike. Selve tolkningen av EU-domstolens avgjørelser er ikke vesensforskjellig fra tolkning av norsk høyesterettspraksis, men et særtrekk ved EU-domstolens avgjørelser er at de er knappe i stil med lite drøftende premisser og uten offentlige dissenser.[26] Dette gjør at man må lese de litt «gjennom linjene», som kan betraktes som argumentasjon med konstruert ratio decidendi. Med andre ord er rettspraksis fra EU-domstolen tungtveiende rettskilder, men man bør være litt varsom med hvilke slutninger man utleder fra premissene.

Mye rettspraksis knytter seg til avgjørelser og tolkningsresultater som er knyttet til det nå opphevede personverndirektivet (95/46/EF). Resonnementet bak at rettsanvendere kan bruke dette er at personvernforordningen er en videreføring av personverndirektivet og har derfor rettskildemessig relevans og vekt. Derimot der ordlyden i forordningen er en annen vil det være vanskelig å benytte eldre rettspraksis uten å gjøre mye analyser for å begrunne at den gamle rettskilden bør tillegges vekt.[27]

1.4.3 Kildebruk

Det er allerede påpekt at primærrett, sekundærrett (forordningen med dens ordlyd) og rettspraksis fra EU-domstolen er tungtveiende rettskilder. I kontekst av GDPR er det imidlertid en rekke soft law som også bør nevnes.

Denne oppgaven viser til en rekke veiledninger fra ulike entiteter. Det vises til blant annet veiledninger og anbefalinger fra Personvernrådet (EDPB), nasjonale Datatilsyn og DFØ/Digdir.

EDPB har som formål å sikre ensartet anvendelse av GDPR, og skal blant annet «granske alle spørsmål som gjelder anvendelse av denne forordning, og utstede retningslinjer, anbefalinger og best praksis for å fremme en ensartet anvendelse av denne forordning», jf. GDPR art. 70 nr. 1 bokstav e. Tidligere var det den såkalte Artikkel 29-gruppen som ga retningslinjer om hvordan de mente GDPR skulle tolkes. Senere har Personvernrådet gitt sin tilslutning til flere slike

[26] Ibid, s. 412 og 413.

[27] Schartum (2020), s. 25.

uttalelser og gjort dem tilgjengelige på sine hjemmesider.[28] Alle uttalelser og veiledninger som EDPB har gitt sin tilslutning til kommer til å bli referert som EDPB/Personvernrådet sin oppfatning. Selv om EDPB sine retningslinjer er soft-law (ikke bindende) representerer de generelt sett anerkjente synspunkter om hvordan GDPR skal tolkes de lege lata og tillegges vekt av datatilsyn og rettslige organer.

Samtidig er det særlig to refleksjoner som begrunner at det er vanskelig alltid å legge EDPB sine retningslinjer til grunn for anvendelsen av forordningen. For det første er EDPB en personvernmyndighet, som består av representanter for nasjonale tilsynsmyndigheter, jf. GDPR art 68 nr. 3. Oppnevning og sammensetning kan gjøre rettsanvendelsen og skjønnsutøvelsen mer «personvernvennlig» enn standpunktene en domstol vil innta. For det andre er retningslinjene svært detaljerte og har ofte preg av utfyllende regler snarere tolkninger. EDPB er ikke lovgiver.[29] Dermed betraktes ikke retningslinjene som noen «fasit».

Datatilsynet på sin side er til en viss grad nødt til å følge EDPB sine tolkninger med hensyn til en ensartet anvendelse av forordningen i hele Unionen. Hvis Datatilsynet fraviker EDPB sine tilnærminger står Datatilsynet i fare for å miste innflytelse i personvernrådet, og det kan være et brudd på EØS avtalen hvis loven tolkes annerledes. Datatilsynet skriver på deres nettside at de vil tolke loven likt som EDPB i en eventuell tilsynssak.[30] Dermed vil det også være av interesse for behandlingsansvarlige å tolke loven likt som disse.

Veiledninger og oppfatninger fra Datatilsynet og andre nasjonale tilsynsmyndigheter er viktige og bør tas i betraktning. Hvor stor vekt de har avhenger imidlertid av den konkrete veiledningen. Mange dokumenter er laget for å formidle komplekst innhold til ulike aktører som behandlingsansvarlige, databehandlere, registrerte og andre. Dette kan føre til at nyanser og mulige diskusjoner forsvinner for å gjøre innholdet mer forståelig og unngå unødvendig kompleksitet. Det kan ikke forutsettes at alle tilsynsmyndigheter har samme syn på ethvert juridisk spørsmål, og det er urealistisk for denne oppgaven å utforske hva alle slike myndigheter mener om et bestemt spørsmål. Språkbarrierer og arbeidsmengde legger derfor visse begrensninger på hvor mye vekt som kan tillegges nasjonale myndigheters oppfatninger.[31]

SKATEs veileder kan ikke tillegges mye rettskildemessig vekt, men har i likhet med juridisk teori en viss relevans som følge av argumentenes innholdsverdi. Grunnen til at den gis mye plass i oppgaven er at den brukes til å strukturere argumenter fordi den belyser oppgavens

[28] Ibid, s. 24.

[29] Ibid, s. 25.

[30] Datatilsynet (2023a), nederst på siden.

[31] Schartum (2020), s. 24.

problemstillinger på interessante måter. Dessuten gir den nyttig informasjon særlig når det gjelder den mer tekniske delen av risikovurderinger.

Det samme gjelder litteraturen det vises til. Disse har heller ikke nevneverdig vekt, men bidrar til økt forståelse.

Til slutt kan det nevnes at det ikke eksisterer noen forarbeider til GDPR som forklarer bestemmelsene, men forordningen inneholder fortalepunkter som kan gi en viss veiledning i forståelsen av bestemmelsene. Disse gir imidlertid ofte begrenset avklaring. Fortalens hovedformål er å presisere og begrunne viktige bestemmelser i forordningen, og den uttrykker ikke selvstendige rettsregler. Dermed har fortalen en begrenset betydning for å redusere usikkerheten rundt tolkningen av bestemmelsene.[32]

1.5 Fremstillingen videre

Hver problemstilling vil behandles i kronologisk rekkefølge. En behandlingsansvarlig må først klargjøre hvorvidt det foreligger en overføring (pkt. 2), og deretter finne ut hvem som eventuelt er behandlingsansvarlig der instrukser herunder forbehold kan være avgjørende for dette (pkt. 3). Deretter må det undersøkes om tiltak og garantier er på plass, og i forlengelsen av dette vurdere hvilke tilleggstiltak som må gjøres (pkt. 4).

Til slutt vies det plass til noen betraktninger av rettspolitisk og rettsfilosofisk art (pkt. 5). I pkt. 5.1 undersøkes det hvorfor det er såpass mye forvirring og usikkerhet knyttet til oppgavens problemstillinger fra et rettsfilosofisk perspektiv, og avslutningsvis i pkt. 5.2 foreslås løsninger for dette.

2 Når er det en overføring, og omfatter overføringsbegrepet «tilgjengeliggjøring» av personopplysninger?

Kapittel V i GDPR gjelder «overføring» av personopplysninger til tredjeland eller internasjonale organisasjoner. Begrepet er ikke definert i forordningen artikkel 4 («Definisjoner») eller andre steder i forordningen.

En naturlig språklig forståelse av «overføring» tilsier at det må finne sted en faktisk overføring av noe fra ett sted til et annet. I konteksten av kapittel V dreier det seg om overføring av «personopplysninger» som er definert som «enhver opplysning om en identifisert eller identifiserbar

[32] Ibid, s. 23.

fysisk person», jf. GDPR art. 4 nr. 1. Et sentralt kjennetegn ved overføringer generelt er at mottakeren får «objektet» i sin besittelse. I dette tilfellet – bruk av skytjenester – er objektet personopplysninger i form av elektronisk informasjon.

Formålet med kapittel V, som er angitt i artikkel 44, er å sikre beskyttelse av personopplysninger *etter* at de er overført («Enhver overføring av personopplysninger som behandles eller skal behandles etter overføring til en tredjestat»). Denne formuleringen tyder på at en overføring ikke finner sted før personopplysningene (som behandles eller skal behandles) er i besittelse av en importør utenfor EU/EØS.

I Lindqvist-saken (C-101/01)[33] vurderer EU-domstolen blant annet om publisering av personopplysninger på en nettside skal anses som en overføring. I avsnitt 69 uttaler domstolen at hvis artikkel 25 i direktiv 95/46 ble tolket slik at det skjer en «overføring til et tredjeland av personopplysninger» hver gang personopplysninger publiseres på en internettside, ville denne overføringen nødvendigvis være en overføring til alle tredjeland der de nødvendige tekniske mulighetene for å få tilgang til internett finnes. Dermed konkluderer domstolen i avsnitt 71 at det ikke nødvendigvis er en overføring til et tredjeland når man legger ut personopplysninger på en internettside som er tilgjengelig for alle på internett. Begrunnelsen er delvis at en internettbruker ikke bare måtte koble seg til internett, men også personlig utføre nødvendige handlinger for å få tak i informasjonen på nettsidene. Med andre ord inneholdt nettsidene ikke tekniske midler til å sende informasjon automatisk til personer som ikke med vilje søkte tilgang til sidene, jf. avsnitt 60.

Dommen antyder at en overføring av data bør være en aktiv handling som innebærer å sende data, og ikke bare gjøre dem passivt tilgjengelig. Lindqvist-dommen lest sammen med ordlyden av artikkel 44 antyder dermed at overføringsbegrepet har to vilkår eller momenter: det bør være en importør som ved aktiv handling sender personopplysninger til en eksportør som ved få/enkle handlinger kan få besittelse over opplysningene.

Rettstekniske hensyn støtter en slik tolkning. Dersom overføring tolkes utvidende til også å omfatte tilgjengeliggjøring, vil man få en rettsregel som er vanskeligere å anvende. Hvorvidt informasjon faktisk er overført er et ja/nei spørsmål, mens tilgjengeliggjøring eller grad av tilgang er et gradsspørsmål som åpner opp for vanskelige grensedragninger som «når en tilgang til personopplysninger på servere i EU/EØS er tilstrekkelig lukket til at det skal anses som en overføring».[34]

[33] C-101/01 *Lindqvist.*

[34] DFØ (2022a), pkt. 3.

Jussprofessor Kuner ser stort sett vekk fra rettstekniske hensyn og hevder at Lindqvist dommen har begrenset relevans ettersom den hviler på en rekke spesifikke faktorer som: nødvendigheten av at en internettbruker personlig tar grep for å konsultere nettstedet, det faktum at informasjonen var på svensk og ikke var beregnet på å bli lest og brukt utenfor landet, og den tidlige utviklingen av Internett-teknologier på den tiden. Videre nevnes at Schrems går utover Lindqvist ved å relatere kravet om adekvat beskyttelsesnivå under personverndirektivet til det som kreves av Charteret, som ble hevet til status som primærrett flere år etter Lindqvist. Schrems-dommen viser at EU-domstolen ser på begrepet internasjonal dataoverføring i form av å kreve et høyt beskyttelsesnivå basert på EU standarder med hensyn til personopplysninger som sendes eller gjøres tilgjengelig («made accessible») på tvers av nasjonale grenser, i stedet for basert på en fast definisjon. Konklusjonen til Kuner er dermed at Lindqvist-dommen ikke ville fått samme utfall i dag i lys av Schrems og GDPR.[35] Her bør det imidlertid bemerkes at Kuner bruker ordene ”made accessible”, men ingen av Schrems-dommene knytter tilgjengeliggjøring opp mot overføringsbegrepet. Opinion 1/15 (avsnitt 214) som Kuner viser til bruker dessuten ordet «disclosure», ikke «made accessible». Førstnevnte er en langt mer aktiv handling enn sistnevnte.

European Data Protection Supervisor (EDPS) mener også Lindqvist har begrenset omfang med samme begrunnelse som Kuner om at dommen må tolkes kontekstuelt.[36] Selv om det ikke enda finnes noen formell definisjon av overføring, mener EDPS at behandlingsansvarlige bør anta at begrepet omfatter visse elementer som: kommunikasjon, avsløring eller på annen måte tilgjengeliggjøring av personopplysninger, utført med viten eller intensjon om at mottaker skal ha tilgang. Dette vil dermed medføre at «overføring» både dekker «bevisst overføring» og «tillat adgang» til data.[37]

Datatilsynet på sin side følger linjene til EDPB.[38] EDPB identifiserer tre kumulative vilkår for at en behandling regnes som overføring. Det første er at en behandlingsansvarlig eller databehandler er underlagt GDPR for den gitte behandlingen. Det andre er at denne behandlingsansvarlige eller databehandleren (dataeksportør) «discloses by transmission» eller på annen måte gjør personopplysninger tilgjengelig til en annen behandlingsansvarlig, felles behandlingsansvarlig eller databehandler (dataimportør). Det tredje er at dataimportøren er i et tredjeland eller er en internasjonal organisasjon.[39] Denne definisjonen omfatter dermed faktiske overføringer og tilgjengeliggjøring.

[35] Kuner (2020), s. 762-763.
[36] EDPS (2014), s. 6.
[37] Ibid, s. 7.
[38] Datatilsynet (2023b).
[39] Guidelines 05/2021 (2.0), s. 7 (avsnitt 9).

Som eksempel på tilgjengeliggjøring nevnes å opprette en konto, gi tilgangsrettigheter til en eksisterende konto, bekrefte eller godta en forespørsel om fjerntilgang, «embedding a hard drive» eller sende passordet til en fil.[40]

Imidlertid er det uklart hva den rettslige begrunnelsen for denne vide tolkningen er. Om de tre vilkårene for overføring skriver EDPB i veiledningens første versjon: «The EDPB has identified […] Having regard to relevant findings in […] Lindqvist, C-101/01» (fotnote 7).[41] Utover dette blir det ikke forklart hvorfor EDPB trekker de slutningene de gjør fra Lindqvist, og det utdypes ikke hvilke deler av avgjørelsen som gir grunnlag for deres definisjon av overføring. Det kan spekuleres i om dette er grunnen til at de har valgt å fjerne henvisningen til Lindqvist i den endelige versjonen av veiledningen.[42] At overføringsbegrepet også skal omfatte «otherwise make available» avviker fra den tradisjonelle ordlyden, og bør følgelig ha en rettslig begrunnelse.

Sett i sammenheng med Schrems og det EDPB skriver i introduksjonen kan man anta at deres vide definisjon kan forklares med formålet om å ha et tilstrekkelig beskyttelsesnivå for registrerte. Ikke bare beskyttelse etter reglene i GDPR, men også av andre regler, både på EU- og medlemsstatsnivå. Som de nevner i introduksjonen (avsnitt 2):

> *When personal data is processed in the EU, it is protected not only by the rules in the GDPR but also by other rules, both at EU and Member State level, that must be in line with the GDPR (including possible derogations therein) and ultimately with the EU Charter on Fundamental Rights and Freedoms. When personal data is transmitted or made available to entities outside the EU territory or to international organisations, the level of protection of individuals' rights and freedoms is likely not to be essentially equivalent to the one afforded by the overarching legal framework provided within the Union.*[43]

Logikken ser ut til å være at en anvendelse av kapittel V gir økt eller mer tilfredsstillende beskyttelse ved dataflyt til tredjeland, dermed vil man omfatte mer (potensiell) dataflyt i overføringsbegrepet. Den brede tolkningen sikrer at GDPRs databeskyttelsesstandarder gjelder for mer eller mindre «alle» situasjoner der personopplysninger behandles eller gjøres tilgjengelig utenfor EU/EØS, slik at rettigheter og friheter til registrerte personer er tilstrekkelig beskyttet.

---

[40] Ibid, s. 8 (avsnitt 16).

[41] Guidelines 05/2021 (1.0), s. 4 (avsnitt 7).

[42] Guidelines 05/2021 (2.0), s. 7 (avsnitt 9).

[43] Ibid, s. 5 (avsnitt 2).

Imidlertid i dokumentets avsnitt 31 skrives det om tilfeller der en viss dataflyt til tredjeland ikke kvalifiserer seg som en overføring til tredjeland i henhold til kapittel V GDPR. Det vises til eksempel 8 som handler om en ansatt av en behandlingsansvarlig fra EU som reiser på jobbtur til et tredjeland. Den ansatte kvalifiserer seg ikke som importør - derfor anvendes ikke kapittel V.

Eksempel 1 handler om en behandlingsansvarlig i et tredjeland som samler personopplysninger direkte fra en registrert i EU. Dette er også et tilfelle der kapittel V ikke anvendes på dataflyt til tredjeland. Grunnen er at den registrerte ikke kvalifiserer seg som eksportør.

Den behandlingen som skjer i eksempel 1 og 8 er fortsatt forbundet med de samme risikoene som følger ved overføring etter kapittel V, slik som risiko for utenlandsk etterretning, motstridende nasjonale lover, ineffektive rettsmidler etc., men siden det mangler en kvalifisert importør (eksempel 8) eller eksportør (eksempel 1), er det ikke en overføring etter kapittel V ettersom vilkår nr. 2 ikke er oppfylt. I denne sammenhengen anviser EDPB at det skal foretas risikovurderinger etter GDPR kapittel IV (bl.a. artikkel 24 «Den behandlingsansvarliges ansvar», artikkel 32 «Sikkerhet ved behandlingen og artikkel 35 «Vurdering av personvernkonsekvenser»). Det EDPB implisitt viser med dette er at en anvendelse av kapittel IV etter deres syn kan gi tilstrekkelig beskyttelse for de samme risikoene som gjør seg gjeldende ved overføringssituasjoner til tredjeland når vilkår 2 ikke er oppfylt.

Dersom man tolker «overføring» til bare å omfatte faktiske overføringer, vil dette resultere i at flere tilfeller ikke oppfyller vilkår nr. 2. I disse situasjonene må de(n) behandlingsansvarlige uansett gjøre risikovurderinger etter kapittel IV og andre relevante bestemmelser i GDPR som det kan påstås gir et tilstrekkelig beskyttelsesnivå i disse særtilfellene, slik som for eksempel 1 og 8 i veiledningen. Det kan dermed hende uenigheter om overføringsbegrepet har begrenset betydning i praksis for de registrertes friheter og rettigheter når det gjelder supporttjenester med fjerntilgangsmuligheter.

Det er fortsatt ønskelig med en avklaring fra rettspraksis, da det med det nåværende rettskildebildet er det vanskelig å konkludere. Sammenfatningsvis trekker domstolpraksis i form av Lindqvist-dommen, system- og ordlydstolkning i retning av at overføringsbegrepet bare dekker «faktisk overføring»[44], mens EDPB sin definisjon også omfatter tilgjengeliggjøring – som også kan gjelde situasjoner der potensielt ingen data flyter til tredjeland.

[44] DFØ (2022a).

3 Skal et forbehold om utlevering anses som instrukser fra den behandlingsansvarlige?

3.1 Tolkning av begrepet instruks

Spørsmålet er av interesse fordi en databehandler som går imot den behandlingsansvarliges instrukser vil kunne bli regnet som en annen behandlingsansvarlig. I så tilfelle vil det kunne være aktuelt med nye behandlingsgrunnlag, se pkt. 3.3.

Utgangspunktet er at den behandlingsansvarlige er den som bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes, jf. GDPR art. 4 nr. 7. Databehandleren skal behandle personopplysninger på «vegne av» den behandlingsansvarlige, jf. GDPR art. 4 nr. 8. Videre skal den behandlingsansvarlige bare bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i personvernforordningen, jf. GDPR art. 28 nr. 1. Databehandleren på sin side skal bare behandle personopplysninger etter instruks fra den behandlingsansvarlige, jf. GDPR art. 29.

Behandlingen skal være underlagt en avtale eller annet rettslig dokument der gjenstanden for og varigheten av behandlingen, behandlingens art og formål, typen personopplysninger og kategorier av registrerte samt den behandlingsansvarliges rettigheter og plikter er fastsatt, jf. GDPR art. 28 nr. 3. Artikkel 28 nr. 3 bokstav a gir en mulighet for databehandlere til å lovlig se bort fra den behandlingsnansvarliges instruksjoner for å overholde juridiske forpliktelser i henhold til EU/EØS-lover, men denne muligheten omfatter ikke overholdelse av tredjelands juridiske forpliktelser.

Likevel ser det ut til at tilgangsforespørsler fra tredjelandsmyndigheter er planlagt av flere skytjenesteleverandører. Noen databehandleravtaler inneholder klausuler som f.eks.:

> *"[CSP] will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body."*[45]

Spørsmålet er om et slikt forbehold er instrukser fra den behandlingsansvarlige.

[45] 2022 Coordinated Enforcement Action, s. 18.

Som nevnt står homogenitetsprinsippet sterkt ved tolkningen av EU/EØS-rettslige kilder. Ordlyden veier derfor tungt ved tolkningen av GDPR. En naturlig språklig forståelse tilsier at instrukser sier noe om hvorvidt en handling er påbudt eller forbudt. I GDPR-sammenheng er en nærliggende sirkeldefinisjon at instrukser sier noe om hvilke behandlinger som er innenfor eller utenfor instrukser.

Det norske akademis ordbok på sin side definerer «instruks» som en ordre om hvordan man skal handle eller opptre i et bestemt tilfelle.[46] Skullerud mfl. definerer instruks på en lignende måte i deres kommentarutgave til personvernforordningen: «Med en instruks menes gjerne en ordre, ofte skriftlig, som binder en annen virksomhet eller person til å handle på en bestemt måte.».[47]

SKATEs veileder påpeker at det i den daglige språkbruken er lite naturlig å omtale informasjon fra den ene parten – det eventuelle pliktsubjektet, som en instruks fra den annen part. Det konkluderes med at en instruks etter personvernforordningen må gi bestemmelser om hvordan den som instrueres skal behandle personopplysninger.[48] En lignende synsvinkel er at en instruks må være en ordre. En ordre, spesielt i juridisk sammenheng, innebærer etter sin ordlyd gjerne at en entitet med autoritet gir en bindende instruksjon som krever lydighet eller utførelse fra mottakeren.

Det kan imidlertid være utfordrende å skille mellom ordre og informasjon når begge disse fremstår som vilkår i en databehandleravtale. I dagligtalen oppfattes instruksjoner eller ordre som noe én part gir til den andre parten på eget initiativ og uten forhandling, men dette er ikke helt treffende for et avtaleforhold som er underlagt GDPR. Det er dermed nødvendig å se hen til avtalerettslige prinsipper og sammenhengen mellom rollefordelingen i personvernforordningen, for å avklare spørsmålet.

Skullerud mfl. hevder GDPR artikkel 29 etablerer et rådighetsforbud og at rådighetsforbudet for databehandlerforhold skal avtales mellom partene. Videre skrives: «Det oppstilles ikke nærmere krav med hensyn til instruksenes form, innhold eller presisjonsnivå. Formålet med instruksene må være å sikre at behandlingen skjer i samsvar med forordningens bestemmelser. De bør derfor tilpasses den aktuelle behandlingen, herunder den aktuelle risikoen for de registrertes rettigheter og friheter, og hva som ellers fremstår som naturlig mellom partene. Bestemmelsen krever heller ikke at instruksene er dokumenterte.».[49]

[46] Det Norske Akademis Ordbok.
[47] Skullerud mfl. (2018), s. 303.
[48] DFØ (2022c), pkt. 4.1.
[49] Skullerud mfl. (2018), s. 302 og 303.

Formålet med databehandleravtalen er blant annet å avklare partenes roller og ansvar etter forordningen, jf. fortalepunkt 79, men også å etablere instruksjonsmyndighet for den behandlingsansvarlige overfor databehandlere, jf. også art. 29, som pålegger databehandleren å behandle personopplysninger kun etter instruks fra den behandlingsansvarlige. Den behandlingsansvarlige er nærmest til å vurdere hvordan forordningens bestemmelser skal ivaretas ved den aktuelle behandlingen. Gjennom databehandleravtalen og nærmere instrukser skal den behandlingsansvarlige sørge for at disse bestemmelsene etterleves tilsvarende når behandlingen skjer i en annen virksomhet.[50]

Det følger videre av GDPR art. 28 nr. 10 at dersom en databehandler overtrer bestemmelsene i forordningen ved å fastsette formålene med og midlene for behandlingen, skal databehandleren anses for å være en behandlingsansvarlig med hensyn til den nevnte behandling. Dette gjelder f.eks. dersom en databehandler utleverer personopplysninger til en tredjepart uten at dette er forankret hos den behandlingsansvarlige. Med andre ord, hvis en databehandler ikke følger instruksene, står den i fare for å bli behandlingsansvarlig selv.

Artikkel 28 nr. 3 og 29 understreker betydningen av å vite hva en instruks er i databehandleravtaler for å sikre at behandlingen av personopplysninger skjer i samsvar med forordningen, samt for å avklare partenes roller og ansvar. Dette innebærer at instruksene i det minste må være tydelige. Hvis instruksene er utydelige, blir det vanskelig å vurdere om en databehandler ikke følger instruksene og dermed må anses som en behandlingsansvarlig.

Ettersom databehandleravtaler er en del av et avtaleforhold kan det være aktuelt å se hen til avtalerettslige prinsipper for å vurdere hva som er en «tydelig» instruks. Det er tilsynelatende usikkert i hvor stor grad partenes oppfatninger skal vektes i vurderingen. SKATEs veileder hevder at et forbehold ikke skal anses som en instruks dersom ingen av avtalepartene oppfatter forbeholdet som en instruks,[51] men dette må nyanseres ytterligere.

I vanlige avtaleforhold er det to parter, mens det i personvernforordningen er flere aktører, blant annet de registrerte og tilsynsmyndigheter. På samme måte som at «behandlingsansvarlig» og «databehandler» anses som funksjonelle konsepter: de har som mål å fordele ansvar i henhold til partenes faktiske roller,[52] kan det argumenteres for at «instruks» også må anses som et funksjonelt konsept siden dette kan avgjøre hvorvidt en databehandler er selvstendig behandlingsansvarlig og dermed fordele ansvar i henhold til partenes faktiske roller. Dette innebærer at

[50] Skullerud mfl. (2018), s. 295.
[51] DFØ (2022c), pkt. 4.1.5.
[52] Guidelines 07/2020, s. 9 (avsnitt 12).

vurderingen av om en behandling er innenfor eller utenfor instruks bør være basert på en analyse av de faktiske elementene og omstendighetene i saken.

Det kan også føre til merkelige utfall dersom man skal hensynta partenes subjektive oppfatninger i de tilfellene der ordlyden er veldig klar. Hvis man ikke behandler personopplysninger utenfor instrukser er det en logisk implikasjon, og noe som følger av lovens system, jf. art. 28 nr. 3 bokstav a sammenholdt med art. 29, at man behandler personopplysninger innenfor instrukser. Enten er en behandling av personopplysninger i tråd med instrukser, eller så er den ikke det.

Dette betyr at to parter som mener et forbehold med klar ordlyd ikke er en instruks, må også mene at det er utenfor instruks når databehandleren overholder bindende ordre fra offentlig myndighet i tredjeland.

Oppsummeringsvis om tolkning av ordet «instruks» er det ikke slik at en instruks nødvendigvis må være en klar ordre. Det er heller ikke avgjørende hvorvidt partene anser noe som instruks. Enhver behandling av personopplysninger er enten i tråd med instrukser eller ikke, fordi instrukser positivt avgrenser hvordan og hvorfor en databehandler skal behandle personopplysninger. Et typisk forbehold gir normative føringer for når en databehandler kan sies å ha handlet utenfor eller innenfor instrukser. Dermed er det nærliggende å konkludere med at forbehold om utlevering som hovedregel skal anses som instrukser fra den behandlingsansvarlige

Det danske datatilsynet har en uttalelse som trekker i samme retning, men går ikke inn på hva som menes med «instrukser»:

Etter utgivelsen av det danske datatilsynets «vejledning om cloud» henvendte KOMBIT seg til datatilsynet med et spørsmål om forbehold.

Den aktuelle klausulen i databehandleravtalen hadde følgende ordlyd: «Once Customer has made its choice, AWS will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, *or as necessary to comply with the law or binding order of a governmental body*» (min utheving).[53]

Til dette svarer det danske datatilsynet at det etter deres oppfatning vil være snakk om en «tilsiktet overføring» av personopplysninger til tredjeland hvis, og i den grad, AWS etterkommer en forespørsel fra offentlig myndighet i tredjeland.[54]

[53] Det Danske Datatilsynet (2022).

[54] Ibid.

Spørsmålet her er naturligvis hva det danske datatilsynet mener med tilsiktet overføring, i motsetning til utilsiktet. I deres veiledning om skytjenester skriver de at det vil være en utilsiktet overføring dersom databehandleren velger å overføre personopplysninger til tredjeland i strid med databehandleravtalen.[55] Motsatt må dette bety at en tilsiktet overføring er en overføring av personopplysninger til tredjeland i tråd med databehandleravtalen. Med andre ord – tilsiktet overføring refererer til overføring i tråd med instrukser, mens utilsiktet refererer til overføring i strid med instrukser. Det danske datatilsynet anser forbeholdet som en instruks – dermed er en slik overføring en tilsiktet overføring.

Det norske Datatilsynet skriver at den danske veilederen kan være nyttig for norske virksomheter, men at de har litt ulike innfallsvinkler. De skriver blant annet: «Når det gjelder bruk av skytjenester i EØS underlagt tredjelands lovgivning, har det norske Datatilsynet og det danske Datatilsynet tilsynelatende litt ulike innfallsvinkler – men resultatet blir likevel i praksis mer eller mindre det samme. […] Det danske Datatilsynet skiller mellom såkalt «tilsigtet» og «utilsigtet» overføring (som også har blitt ytterligere forklart i den såkalte KOMBIT-saken)».[56]

Dette kan imidlertid se ut til å være en misforståelse fra Datatilsynet sin side. Basert på KOMBIT-svaret og det danske datatilsynets veiledning, synes det å være slik at det danske datatilsynet definerer «tilsiktet overføring» som en overføring som er i samsvar med databehandleravtalen og instruksjonene, mens «utilsiktet» refererer til en overføring i strid med databehandleravtalen og uten instruksjoner fra den behandlingsansvarlige. Videre skriver det norske Datatilsynet: «Vi mener at selv om en databehandleravtale ikke tar forbehold om overføring, kan det tenkes situasjoner der det likevel er holdepunkter for at potensielt ulovlige overføringer kan skje, med den konsekvens at tiltak må iverksettes for å forhindre brudd hvis leverandøren skal kunne velges. Slike omstendigheter kan for eksempel avdekkes under en risikovurdering av databehandleren etter artikkel 32. Det er mulig slike situasjoner ville blitt vurdert som utilsiktet overføring av danske kolleger, og i så fall har vi ulik tolkning.».[57] Både det danske og norske datatilsynet synes å mene at dette er en overføring som går utover instrukser, men forskjellen er at det danske datatilsynet betegner det som «utilsiktet». Så det kan argumenteres for at de ikke nødvendigvis har ulik tolkning, men snarere ulik terminologi.

Selv om det danske datatilsynet ikke skriver at et forbehold uttrykkelig er en instruks, mener de at det er tale om en tilsiktet overføring når databehandleren etterkommer en forespørsel fra

[55] Vejledning om cloud (2022), s. 29.
[56] Datatilsynet (2023c).
[57] Ibid.

tredjelands myndighet, der tilsiktet overføring betyr i tråd med databehandleravtalen. Dermed kan det påstås at også det danske datatilsynet mener forbehold er instrukser.

3.2 Forutsatt at forbeholdet ikke er en instruks, er det tale om felles behandlingsansvar?

Et annet spørsmål er om et forbehold i en avtale kan tolkes dithen at det ikke er en instruks, men at partene i fellesskap fastsetter formålene og midlene for behandlingen og dermed må anses som felles behandlingsansvarlige når skytjenesteleverandøren utleverer personopplysninger til tredjeland, jf. GDPR art. 26 nr. 1.

Felles behandlingsansvar endrer ikke hvilke vurderinger som må gjøres for å overholde GDPR, men det vil hovedsakelig ha betydning når det gjelder fordeling av forpliktelser for overholdelse av personvernregler og spesielt med hensyn til enkeltpersoners rettigheter.[58]

Mer spesifikt er skillet mellom felles behandlingsansvar og selvstendig behandlingsansvar aktuelt å ta stilling til fordi felles behandlingsansvar medfører en plikt til å framlegge informasjon som nevnt i artikkel 13 og 14, ved hjelp av en «ordning» seg imellom, jf. GDPR art. 26 nr. 1 hvorav det vesentligste innholdet i ordningen skal gjøres tilgjengelig for den registrerte, jf. art. 26 nr. 2. Det oppstilles ikke krav om en skriftlig avtale slik det er for databehandlerforhold, jf. art. 28. Det må kunne antas at ulikheten i ordlyden er tilsiktet for å understreke at andre ordninger kan aksepteres.

Videre kan den registrerte utøve sine rettigheter i henhold til GDPR med hensyn til og overfor hver av de behandlingsansvarlige, uavhengig av vilkårene for ordningen nevnt i nr. 1, jf. art. 26 nr. 3. Med andre ord kan de registrerte i så tilfelle forholde seg til hvilken som helst av partene, uavhengig av den interne ansvarsfordelingen. Dermed fører felles behandlingsansvar til et eksternt solidaransvar. Begrunnelsen for regler om felles behandlingsansvar er delvis de risikoene som følger av at flere virksomheter behandler personopplysninger samtidig. Dette kan medføre en økt risiko for manglende etterlevelse og kontroll, og manglende åpenhet for de registrerte. Derfor er det viktig å hindre ansvarspulverisering gjennom: å identifisere hva slags samarbeidsform som foreligger, å formalisere samarbeidet og å regulere hvilket ansvar den enkelte virksomhet har for å oppfylle forordningens bestemmelser, jf. fortalepunkt 79.[59]

Det følger av GDPR artikkel 26 nr. 1 at dersom to eller flere behandlingsansvarlige «i fellesskap» fastsetter formålene og midlene for behandlingen, skal de være felles

[58] Guidelines 07/2020, avsnitt 48.

[59] Skullerud mfl., s. 285.

behandlingsansvarlige. En naturlig språklig forståelse tilsier at to parter er felles behandlingsansvarlig når de samarbeider og er enige om hvordan og hvorfor personopplysninger skal behandles. Det er for eksempel ikke tale om felles behandlingsansvar dersom en skytjenesteleverandør overfører opplysninger til tredjeland i strid med instrukser. Da blir skytjenesteleverandøren en selvstendig behandlingsansvarlig i medhold av GDPR art. 28 nr. 10.

Noe av det mest utfordrende med felles behandlingsansvar kan være å i det hele tatt oppdage at man har et felles behandlingsansvar.[60] Både sak C-40/17 (Fashion ID) og sak C-210/16 (Wirtschaftsakademie) illustrerer dette.

Fashion ID-dommen handlet om en nettsideoperatør som hadde innebygd Facebooks «Like» knapp på sin nettside. Dette medførte at besøkendes personopplysninger ble overført til Facebook. Spørsmålet var om de av denne grunn var felles behandlingsansvarlig for innsamling og overføring av personopplysninger fra besøkende til Fashion IDs nettside.[61] Det ble konkludert med at Facebook sammen med Fashion ID bestemte «midlene» fordi Fashion ID ved å legge inn Like knappen på nettstedet utøvet avgjørende innflytelse over innsamling og overføring.[62] Om formålene uttalte domstolen at Fashion ID ved å legge inn Like knappen gjorde det mulig å optimalisere markedsføringen av produktene sine ved å gjøre dem mer synlige på Facebook når en besøkende på nettstedet klikker på Like knappen.[63] Siden både Fashion ID og Facebook hadde økonomiske interesser av dette ble konklusjonen at Fashion ID og Facebook sammen bestemte formålene for denne behandlingen.[64] At Fashion ID selv ikke hadde tilgang til personopplysningene som ble samlet inn var ikke avgjørende, fordi de sammen bestemte formålene og midlene.[65]

Wirtschaftsakademie-dommen handlet om hvorvidt en administrator av en fanklubb-side på Facebook kunne bli behandlingsansvarlig som følge av at fanklubben hadde valgt Facebook som plattform til å distribuere informasjon den tilbydde.[66] Domstolen uttaler at Facebook må anses som den som primært bestemmer formålet og midlene for behandling av personopplysninger til brukere av Facebook og dermed er behandlingsansvarlig.[67] I vurderingen av om administratoren av fanklubb-siden også er behandlingsansvarlig, pekes det på at behandlingen av personopplysninger er spesielt ment å gjøre det mulig for Facebook å forbedre sitt

[60] Schartum (2020), s. 70.
[61] C-40/17 *Fashion-ID*, avsnitt 64.
[62] Ibid, avsnitt 78 og 79.
[63] Ibid, avsnitt 80.
[64] Ibid, avsnitt 81.
[65] Ibid, avsnitt 82.
[66] C-210/16 *Wirtschaftsakademie*, avsnitt 25.
[67] Ibid, avsnitt 30.

annonseringssystem som overføres via nettverket, og å gjøre det mulig for fan-sidens administrator å for eksempel se profilen til besøkende som liker fan-siden, slik at de kan tilby besøkende mer relevant innhold og utvikle funksjoner som sannsynligvis vil være av større interesse for deres besøkende.[68] Det å bare bruke et sosialt nettverk som Facebook som vanlig bruker gjør deg ikke til behandlingsansvarlig,[69] men en administrator kan med hjelp av filtre som Facebook stiller til disposisjon, definere kriteriene i henhold til hvilke statistikker som skal utarbeides og utpeke hvilke kategorier av personer som skal få personopplysningene sine behandlet av Facebook.[70] Avhengig av målgruppen og formålene for å administrere og fremme sin aktivitet, er Wirtschaftsakademie delaktige i å bestemme formål og midler for behandling av personopplysninger til besøkende på fansiden.[71]

Som nevnt illustrerer disse to dommene at det kan være utfordrende å avgjøre hvem som er behandlingsansvarlig. Videre indikerer begge dommene at partenes interesse skal vektlegges i vurderingen av hvem som bestemmer formålene med behandlingen. En vanlig formulering er at den behandlingsansvarlige bestemmer «hva» og «hvorfor» en behandling skal foretas.[72]

EDPB viser til de to dommene ovenfor og uttaler at felles behandlingsansvar kan etableres når entitetene involvert forfølger formål som er nært knyttet eller komplementære, for eksempel når det er en gjensidig fordel som oppstår fra den samme behandlingsoperasjonen. Imidlertid er ikke hvorvidt det er en gjensidig fordel avgjørende, men det er bare en indikasjon på felles behandlingsansvar.[73]

I det en skytjenesteleverandør utleverer personopplysninger til myndigheter i tredjeland er gjerne formålet med dette å oppfylle en rettslig forpliktelse som påhviler skytjenesteleverandøren (merk at dette ikke må forveksles med behandlingsgrunnlaget i GDPR art. 6 nr. 1 bokstav c, som bare gjelder rettslige forpliktelser hjemlet i unionsretten eller en medlemsstats nasjonale rett, jf. art. 6 nr. 3). Den opprinnelige behandlingsansvarlige derimot har ingen forpliktelser overfor tredjelands myndigheter, og har neppe noe ønske om å overføre personopplysninger til tredjeland – men har på tross av dette godtatt forbeholdet.

Selv om skytjenesteleverandøren heller ikke har et ønske om å utlevere personopplysninger til tredjeland, har de likevel interesse av å unngå juridiske sanksjoner fra tredjelands lovgivning som de er underlagt. Fordelingen av interesse tilsier dermed, avhengig av den konkrete

[68] Ibid, avsnitt 31.

[69] Ibid, avsnitt 35.

[70] Ibid, avsnitt 36.

[71] Ibid, avsnitt 39.

[72] Guidelines 07/2020, avsnitt 35 og C-210/16 *(Opinion of Advocate General)*, avsnitt 46.

[73] Guidelines 07/2020 avsnitt 60.

situasjonen, at skytjenesteleverandøren må anses som en selvstendig behandlingsansvarlig for denne overføringen. Dette stemmer overens med Datatilsynet sine uttalelser på deres nettside: «[…] dersom en overføring skjer for at en tjenesteleverandør skal oppfylle sine juridiske forpliktelser, er det sannsynligvis tjenesteleverandøren som er behandlingsansvarlig for overføringen».[74]

Disse siste betraktningene gjør seg gjeldende uavhengig av hvorvidt forbeholdet anses som instruks eller ikke.

3.3 Forutsatt at forbeholdet er en instruks, har den behandlingsansvarlige lov til å gi en slik instruks?

Det er i pkt. 3.1 konkludert med at de aller fleste forbehold utgjør en instruks og i pkt. 3.2 er det konkludert med at det ved utlevering av personopplysninger til tredjeland, uavhengig av hvorvidt et forbehold anses som instruks, ikke er tale om felles behandlingsansvar for denne behandlingen, men at skytjenesteleverandøren muligens er selvstendig behandlingsansvarlig idet overføringen skjer.

Et annet spørsmål er om den opprinnelige behandlingsansvarlige har lov til å gi en slik instruks.

Det klare utgangspunktet er at den behandlingsansvarlige ikke kan instruere en databehandler utover behandlingsgrunnlaget. Det følger av GDPR art. 5 nr. 1 bokstav b at personopplysninger skal samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse.

Dette må vurderes konkret i hvert enkelt tilfelle der det blant annet skal tas hensyn til enhver forbindelse mellom formålene som personopplysningene er samlet inn for, og formålene med den tiltenkte viderebehandlingen, jf. GDPR art. 6 nr. 4 bokstav a, i hvilken sammenheng personopplysningene er blitt samlet inn, jf. bokstav b, personopplysningenes art, jf. bokstav c, de mulige konsekvensene for de registrerte av den tiltenkte viderebehandlingen, jf. bokstav d og om det foreligger nødvendige garantier, som kan omfatte kryptering eller pseudonymisering, jf. bokstav e. Som følge av ordlyden «blant annet» er ikke denne listen uttømmende.

For offentlige myndigheter er behandlingsgrunnlaget i mange tilfeller GDPR art. 6 nr. 1 bokstav c: «behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige», eller bokstav e: «behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er

[74] Datatilsynet (2023c).

pålagt». I de fleste tilfeller vil det være lite sannsynlig at å utlevere personopplysninger til tredjelands etterretningsmyndigheter er i tråd med disse behandlingsgrunnlagene, eller formålene som fastsettes i et av de rettslige grunnlagene.

I tillegg må den behandlingsansvarlige for å gi instruks om overføring til tredjeland identifisere et passende overføringsgrunnlag. For de fleste behandlingsansvarlige er det mest aktuelt med standardkontrakt, jf. GDPR art. 46 nr. 2 bokstav c. Deretter må man i tråd med sekstrinnsvurderingen til EDPB og Schrems II vurdere om overføringsgrunnlaget vil være effektivt i lys av alle omstendighetene ved overføringen, ved å blant annet undersøke lover og praksis i tredjelandet.[75] I denne vurderingen vil man mest sannsynlig komme til, for amerikanske lover og praksis sin del, at disse fører til et lavere beskyttelsesnivå enn i EØS. Følgelig må man iverksette ytterligere tiltak som veier opp for dette i henhold til Schrems II. Se mer om dette i pkt. 1.1 og 4.3.

Konklusjonen er dermed at behandlingsansvarlige ikke har lov til å instruere/ha forbehold i skytjenesteavtalen om utlevering av personopplysninger til tredjeland, med mindre det er identifisert behandlingsgrunnlag, forenlige formål og overføringsgrunnlag etter GDPR kap. V supplert med ytterligere tilleggstiltak.

4 Hvilke vurderinger må den behandlingsansvarlige gjøre når skytjenesteleverandøren potensielt kan overføre personopplysninger?

4.1 Utgangspunkt

Utgangspunktet er som nevnt i pkt. 1 og 2 at bruk av skytjenesteleverandører i EØS ikke er en overføring til tredjeland og at man ikke trenger å forholde seg til reglene i GDPR kap. V om overføring av personopplysninger til tredjeland. Likevel for det tilfellet at skytjenesteleverandøren er underlagt tredjelands lovgivning kan det være nødvendig med ytterligere vurderinger. Det forutsettes i den videre drøftelsen at det ikke er noen instrukser/forbehold om utlevering av personopplysninger til tredjeland.

Det er på det rene at behandlingsansvarlige ved en faktisk overføring eller tilgjengeliggjøring, i henhold til Schrems II, må iverksette supplerende beskyttelsestiltak. Spørsmålet er hvordan man skal vurdere beskyttelsestiltak i situasjoner der man som utgangspunkt ikke overfører personopplysninger til tredjeland, men der skytjenesteleverandøren er underlagt tredjelands

[75] Datatilsynet (2023a).

lovgivning som medfører en mulighet for at utenlandsk etterretning innhenter data til etterretningsformål.

Ved valg av skyleverandører der overføring av personopplysninger til tredjestater kan skje, er det alltid relevant å se hen til bl.a. artikkel 32 og 35 i GDPR. Selv om overføring til tredjestater ikke nevnes eksplisitt i disse bestemmelsene, vil risikoen for fysiske personer rettigheter og friheter kunne være høy dersom artikkel 46 eller 49 kommer til anvendelse.

Dersom risikovurderingen viser at det er høy risiko for at utenlandsk etterretning får utlevert data må man sørge for at databehandleren gjennomfører egnede tiltak, jf. art. 28 og 32. Spørsmålet da er om hvordan man skal vurdere hvilke tiltak som må gjøres, herunder om man skal ta en risikobasert eller rettighetsbasert tilnærming.

Det følger av GDPR art. 28 nr. 1 at behandlingsansvarlige bare skal bruke databehandlere 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». Vurderingen må stå i forhold til risikoen behandlingen medfører, se fortalepunkt 81. GDPR art. 32 nr. 1 sier det blant annet skal tas hensyn til «risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter» når man gjennomfører «egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen». Målet med denne risikobaserte tilnærmingen er å redusere risikoen for at utenlandsk etterretning får utlevert personopplysninger.

Den andre tilnærmingen, som gjerne kalles rettighetsbasert i litteraturen[76], er den som blant annet følger av Schrems II som angir at det kan være nødvendig for den behandlingsansvarlige å supplere med ytterligere beskyttelsestiltak for å sikre et «tilsvarende beskyttelsesnivå», se gjennomgangen i pkt. 1.1 og pkt. 4.2

Denne tilnærmingen er i utgangspunktet forbeholdt overføringssituasjoner i henhold til GDPR kap. V, og det er da naturlig å stille spørsmål om dette også kan gjelde situasjoner der man i utgangspunktet ikke overfører personopplysninger til tredjeland, men skytjenesteleverandøren er underlagt tredjelands lovgivning.

Om denne situasjonen skriver Datatilsynet: «Når det gjelder hva slags tiltak man kan iverksette og hva som er tilstrekkelig, er det naturlig å se hen til tiltakene beskrevet i forrige delkapittel,

[76] For eksempel Gellert undersøker forholdet mellom den risikobaserte og den rettighetsbaserte tilnærmingen, og hvorvidt dette er to motsetninger eller en mulighet til å analysere koblingene mellom lov, regulering og risiko.

altså tiltak man kan iverksette for å sikre lovlig overføring av personopplysninger. Kryptering eller pseudonymisering med god nøkkelhåndtering kan være særlig praktisk.».[77]

EDPB skriver i deres Coordinated Enforcement Action (CEA) om bruk av skytjenester av offentlig sektor, at den behandlingsansvarlig må analysere om lovgivningen i et tredjeland vil gjelde for skytjenesteleverandøren og kunne føre til muligheten for å rette tilgangsforespørsler om tilgang til data lagret av skytjenesteleverandør – i den forbindelse vurdere om passende og forholdsmessige tekniske, organisatoriske og/eller juridiske sikkerhetstiltak i henhold til artikkel 28 er på plass eller kan settes i verk. I fotnoten til dette står det: "Similar safeguards as those provided by the EDPB in the recommendations concerning supplementary measures for transfers could be adduced."[78]

Det vises altså til de tilleggskravene som nevnt i EDPB sin veileder, men ikke eksplisitt hvordan de skal vurderes. Vurderingen er viktig for behandlingsansvarlige nettopp for å vite hva som er tilstrekkelige tiltak.

Denne delen av oppgaven skal altså forsøke å avklare hvordan man skal vurdere hvilke tilleggskrav som er nødvendige i en situasjon der man ikke overfører personopplysninger til tredjeland, men der skytjenesteleverandøren man bruker er underlagt tredjelands lovgivning.

Spørsmålet blir på sett og vis om det kreves en rettighetsbasert tilnærming for hvilke tiltak man må iverksette, selv om det ikke skjer noe overføring.

4.2 Proporsjonalitet i den rettighetsbaserte tilnærmingen (kap. V)

4.2.1 Innledning

Meningen med tilleggstiltakene som supplerer overføringsgrunnlag etter kap. V er å kompensere for manglende personvern i et tredjeland. Dermed vil det være nødvendig å vurdere beskyttelsesnivået i det aktuelle tredjelandet før man eventuelt vurderer hvilke supplerende tilleggstiltak som er nødvendig.

Datatilsynet skriver at lover og praksis kan utgjøre et inngrep i personvernet, uavhengig av om dataene er sensitive eller hvorvidt personene det gjelder faktisk har blitt negativt berørt av inngrepet – men ikke alle inngrep utgjør en krenkelse. «Det er først når lovene og praksisene går lenger enn nødvendig og proporsjonalt at de utgjør en krenkelse. Man trenger bare iverksette

[77] Datatilsynet (2023c).

[78] 2022 Coordinated Enforcement Action, s. 32.

ytterligere tiltak der det foreligger en krenkelse».[79] Videre skriver datatilsynet at man i vurderingen om lover og praksis utgjør en krenkelse av personvernet, blant annet kan se hen til momenter som: i) det EMD vektlegger i praksis knyttet til EMK art. 8 ii) det EU-domstolen trekker frem i Schrems II – dommen iii) det som fremgår av GDPR art. 45 nr. 2 og iv) det EDPB trekker frem i sine anbefalinger om europeiske essensielle garantier for overvåkingstiltak.[80]

Samlet sett tilsier disse at det skal foretas en proporsjonalitetsvurdering der inngrepet må ha hjemmel i lov, etterfølge legitime formål og være nødvendig i et demokratisk samfunn.

4.2.2 I samsvar med loven

Utgangspunktet er at behandlingen skal være basert på klare, presise og tilgjengelige regler. Enhver begrensning på utøvelsen av rettighetene og frihetene som er anerkjent av Charteret (og EMK) må være fastsatt ved lov. En forsvarlig «interference» må dermed være i samsvar med loven.[81] Lovgivningen må være juridisk bindende i henhold til nasjonal lovgivning. Vurderingen av tredjelandslovgivning bør fokusere på om den kan påberopes av enkeltpersoner for en domstol, jf. GDPR art. 45 nr. 2.[82] Videre må gjeldende lov angi under hvilke omstendigheter og under hvilke betingelser et tiltak som sørger for behandling av slike opplysninger kan vedtas. Kravet om at enhver begrensning på utøvelsen av grunnleggende rettigheter må være fastsatt ved lov innebærer at det rettslige grunnlaget som tillater inngrep i disse rettighetene må selv definere omfanget av begrensningen på rettighetens utøvelse.[83]

Imidlertid kan det være vanskelig å trekke den nedre grensen for inngrep mot tiltak som er så ubetydelige at det er ubetenkelig å tillate dem uten den rettssikkerhetsgarantien som ligger i lovkravet.[84] Normalt må det foreligge et konkret inngrep. Alle «rettslige inngrep» forutsetter lovhjemmel, mens for faktiske handlinger er stillingen mindre entydig. Noen faktiske handlinger kan være så ubetydelige at den kontrollgaranti som ligger i lovkravet, må anses unødvendig. Det er for eksempel neppe noe inngrep å samle inn åpent tilgjengelig informasjon om personer. Dette er handlinger som enhver – og da normalt også myndighetene – kan foreta.[85] Forskjellige inngrepsmåter i en og samme rettighet kan være eller mindre tyngende generelt og

[79] Datatilsynet (2023a).
[80] Ibid.
[81] Recommendations 02/2020, avsnitt 26.
[82] Ibid, avsnitt 27.
[83] Ibid, avsnitt 28.
[84] Aall (2018), s. 119.
[85] Ibid, s. 120.

man kan også sondre innenfor samme kategori inngrep i samme kategori rettighet etter hvor konkret følbart det er for den som rammes, individuelt.[86]

I sak No 58170/13 (Big Brother) ble det etter Snowden avsløringene levert tre klager knyttet til ulike overvåkningsregimer. 1) Bulk-innsamling av data 2) deling av personopplysninger til utenlandsk etterretning 3) innhenting av kommunikasjonsdata fra kommunikasjonstjenesteleverandører.

Retten kommer blant annet med noen generelle bemerkninger om hvordan man rettferdiggjør inngrep, og peker på vurderingen som EMK art. 8 legger til grunn. Om ordlyden av «i samsvar med loven» uttaler de at det kreves at det påklagede tiltaket har en viss hjemmel i nasjonal rett. Den må også være tilgjengelig for vedkommende og forutsigbar med hensyn til virkningene.[87]

Videre uttales at betydningen av «forutsigbarhet» i sammenheng med hemmelig overvåkning er ikke den samme som på mange andre felt. I den spesielle sammenhengen med hemmelige overvåkningstiltak, som for eksempel avlytting av kommunikasjon, kan ikke «forutsigbarhet» bety at enkeltpersoner skal kunne forutse når myndighetene sannsynligvis vil ty til slike tiltak, slik at de kan tilpasse sin oppførsel deretter. Imidlertid er risikoen for vilkårlighet åpenbar, spesielt der en makt tillagt den utøvende makt utøves i det skjulte. Det er derfor viktig med klare og detaljerte regler for hemmelige overvåkningstiltak, spesielt ettersom teknologien som er tilgjengelig for bruk stadig blir mer sofistikert. Den interne loven må være tilstrekkelig klar til å gi innbyggerne en tilstrekkelig indikasjon på omstendighetene og betingelsene for at offentlige myndigheter har fullmakt til å ty til slike tiltak.[88]

4.2.3 Etterfølge legitime formål

Formålsbetraktninger kan grupperes som spesielle og generelle. Generelle formål ligger som overordnede verdinormer innen rettssystemet. Typisk er hensyn som forutberegnelighet, andre rettssikkerhetshensyn og maktfordeling. Spesielle formål er spesifikke for den enkelte lov, og kommer gjerne til uttrykk i loven selv.[89] I EMK art. 8 er det tale om hensyn til den nasjonale sikkerhet, offentlig trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter. Disse hensynene eller formålene er nokså vide. Dermed blir kravet til forholdsmessighet særlig viktig. De samme hensynene vil gjøre seg gjeldende når det er tale om utenlandsk etterretning

[86] Ibid, s. 122.
[87] No 58170/13 *Big Brother*, avsnitt 332.
[88] Ibid, avsnitt 333.
[89] Aall (2018), s. 150.

som innhenter personopplysninger fra skytjenesteleverandører i EØS. Det er dermed først når etterretningen ikke er forholdsmessig at den blir problematisk.

4.2.4 Nødvendig i et demokratisk samfunn

Nødvendighetsvurderingen deles vanligvis inn i to kumulative undervilkår: For det første må det være et presserende samfunnsmessig behov for inngrepet (test 1) og dessuten må det stå i forhold til formålet, proporsjonalitet (test 2).[90]

I test 1 er målet å avgjøre om målet forfulgt av inngrepet er tilstrekkelig legitimt. Det involverer et element av veiing og balansering, siden det sosiale behovet som dekkes må være et «pressende» et.[91] WP29 uttaler at begrepet «presserende samfunnsbehov» innebærer et større nivå av alvor, hastverk eller umiddelbarhet knyttet til behovet tiltaket søker å adressere. Derfor vil definisjonen av presserende samfunnsbehov innebære å ta hensyn til en rekke faktorer som må vurderes konkret.[92] Det bør avgjøres om spørsmålet som står på spill kan føre til skade på eller ha en skadelig effekt på samfunnet (eller deler av det) hvis det ikke blir adressert. Tiltaket må kunne redusere denne skaden. Og man må spørre hva som er de bredere synspunktene (samfunnsmessige, historiske eller politiske osv.) i samfunnet om problemstillingen som diskuteres.[93]

Når legitimiteten til målet som forfølges er etablert (første balansetest), gjenstår det å se om «the interference» kan finne sted ved å bestemme om det står i forhold til et slikt forfulgt legitimt mål. Dette er andre balanseprøve, test 2. Testen krever at inngrepet ikke går lenger enn nødvendig for å møte det presserende sosiale behovet. Som det fremgår av arbeidsgruppen, er dette et spørsmål om balansering av skadene skapt av slik innblanding mot fordelene.[94]

Hvis det foreslåtte «tiltaket» (som for vår del er tredjelands lover og praksis som gir myndigheter myndighet til å foreta etterretning) oppfyller nødvendighetsdelen av vurderingen, må det også oppfylle testen om hvorvidt det fortsatt er en proporsjonal respons ved å veie opp det legitime målet som det foreslåtte tiltaket forfølger og det presserende samfunnsbehovet som er identifisert, over individets rett til personvern. Uansett hvordan denne vurderingen gjøres, bør den innebære en bevisstyrt forklaring på hvorfor de eksisterende tiltakene ikke lenger er tilstrekkelige for å møte dette behovet. Det må klart vises hvordan det foreslåtte tiltaket vil adressere det presserende samfunnsbehovet som er identifisert, støttet av bevis. Det bør på dette

[90] Ibid, s. 153.
[91] Gellert (2020), s. 13.
[92] Opinion 01/2014, pkt. 3.14.
[93] Ibid, pkt. 3.19.
[94] Gellert (2020), s. 14.

stadiet gis en forklaring på hvilke andre tiltak som ble vurdert og om disse ble funnet å være mer eller mindre inngripende i personvernet. I tillegg til denne avveiningen kan det også vurderes antall personer som berøres av tiltaket, mengden informasjon som samles inn, hvor lenge informasjonen vil bli lagret, tiltak som er iverksatt for å begrense omfanget av et tiltak, klagerett og hva slags type informasjon som samles inn [95]

4.3 Proporsjonalitet i den risikobaserte tilnærmingen (kap. IV)

Det er ikke bare vurderingen ovenfor om hvorvidt lover og praksis utgjør en krenkelse av personvernet som inneholder elementer av proporsjonalitet.

All behandling av personopplysninger skal etterfølge prinsippene satt i GDPR art. 5 nr. 1 og den behandlingsansvarlige er ansvarlig for og skal kunne påvise at art. 5 nr. 1 overholdes, jf. art. 5 nr. 2. Blant annet skal personopplysningene være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for, jf. art. 5 nr. 1 bokstav c, og behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak, jf. art. 5 nr. 1 bokstav f. Videre følger det av fortalepunkt 4 at: «Retten til vern av personopplysninger er ikke an absolutt rettighet; den må ses i sammenheng med den funksjon den har i samfunnet, og veies mot andre grunnleggende rettigheter i samsvar med forholdsmessighetsprinsippet».

Disse prinsippene kommer ytterligere til uttrykk i kapittel IV, nærmere bestemt artikkel. 24, 25, 28, 32 og 35.

For eksempel skal det i vurderingen av personvernkonsekvenser i GDPR art. 35 tas en vurdering av om behandlingsaktivitetene er «nødvendige og står i et rimelig forhold til formålene», jf. art. 35 nr. 7 bokstav b.

Også plikten i art. 32 nr. 1 om å gjennomføre egnede tekniske og organisatoriske tiltak kan anses som et utslag av forholdsmessighetsprinsippet, ettersom sikkerhetsnivået og tiltakene skal stå i et rimelig forhold til den aktuelle risikoen. Dette gjelder også for databehandlere, jf. art. 28 nr. 3 bokstav c. Dette reflekterer prinsippet om integritet og konfidensialitet i art. 5 nr. 1 bokstav f. Det kan også antas at opplysningenes tilgjengelighet og robusthet, jf. art. 32 nr. 1 bokstav b, er noe som skal bli sikret selv om det ikke eksplisitt nevnes. For eksempel i helsesektoren er det viktig at sensitive pasientopplysninger ikke kommer på avveie, men det er også viktig at de er tilgjengelige for å gi god helsehjelp.

[95] Opinion 01/2014, pkt. 3.26.

For å etterleve art. 32 nr. 1 må en behandlingsansvarlig eller databehandler foreta en rekke vurderinger. Den første er risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter. Den andre er hvilket sikkerhetsnivå som er egnet med hensyn til risikoen. Den tredje er hvilke tiltak som er egnede for å oppnå et slikt sikkerhetsnivå.

SKATEs veileder fokuserer på to risikotyper. Den første er bulkinnsamling in-transit, som innebærer systematisk innhenting av all grenseoverskridende internettrafikk for analyse, profilering og masseovervåkning, for eksempel for å avdekke kriminalitet, terrororganisasjoner, politiske endringer og sosial uro.[96] Den andre risikoen er lovpålagt utlevering av data om spesifikke personer eller virksomheter Dette innebærer at myndighetene krever at en aktør, f.eks. en skyttjenesteleverandør, utleverer data basert på lovgivningen. Denne typen innhenting er mer målrettet og skal underbygge en mistanke.[97]

For å få en viss oversikt over størrelsen på risikoen må man sammenholde konsekvens og sannsynlighet.[98]

Ved å vurdere konsekvens estimeres alvorlighetsgraden for den registrerte hvis etterretning samler inn opplysninger. Veilederen nevner offentlige tilgjengelige opplysninger som et eksempel der konsekvensen er lav hvis etterretningsmyndigheter får tilgang, siden lovgiver har veid konfidensialitet mot offentlighetshensyn.[99]

Særlig krevende er det å gjøre en vurdering av konsekvenser ved bulkinnsamling av in-transit data ettersom den utgjør et inngrep for flere mennesker samtidig. Konsekvensen avhenger av om det er metadata eller innholdsdata. Innholdsdata er ofte godt kryptert, mens metadata er lettere tilgjengelig, men vanskeligere å knytte til personer. Muligheten for å knytte IP-adresser til enkeltpersoner avhenger av flere faktorer, som dynamiske eller statiske IP-adresser, der dynamiske er vanskeligere å knytte til individer.[100]

Omfang og varighet er naturligvis også aktuelle momenter i konsekvensvurderingen. Lengre innsamlingsperiode tilsier at det samles inn mer data.[101]

[96] DFØ (2022b), pkt. 2.2.1.
[97] Ibid, pkt. 2.2.2.
[98] Ibid, pkt. 2.5.1.
[99] Ibid, pkt. 2.3.1.
[100] Ibid, pkt. 2.3.2.1.
[101] Ibid, pkt. 2.3.2.2.

Om sannsynlighet nevner SKATEs veileder at sannsynligheten påvirkes av faktorer som verdi, motivasjon, kapasitet og tilgjengelighet. Verdifulle data kan for eksempel motivere en aktør til å bruke flere ressurser på å få tak i dataen. Vanskeligheten med å få tak i opplysningene påvirker også sannsynligheten. Arbeidsgruppen mener det for eksempel er lite sannsynlig at etterretning går via kommersielle servere i EU/EØS for å hente offentlig tilgjengelige opplysninger.[102]

4.4 Proporsjonalitetsprinsippet som et bindeledd mellom rettighetsbasert og risikobasert tilnærming

Proporsjonalitet er en standard rettslig teknikk i konstitusjonell, administrative og menneskerettighets-/grunnleggende rettighetslov. Det er i hjertet av både EMK og Charteret. Selv om det ikke er et prinsipp eller en bestemmelse i seg selv i GDPR, så er sammenhengen mellom databeskyttelse og proporsjonalitet blitt understreket flere ganger i litteraturen,[103] og denne oppgavens pkt. 4.2 og 4.3.

Som vi har sett ovenfor i pkt. 4.3 er hele poenget med den risikobaserte tilnærmingen å bestemme om skal ta risikoene eller ikke, og dette tar form av en proporsjonalitetstest som involverer de ulike skadene og fordelene knyttet til risikoen.[104] Som nevnt, for å etterleve GDPR art. 32 nr. 1 må en behandlingsansvarlig eller databehandler foreta tre vurderinger: 1) Risikoen ved en behandling i form av sannsynlighet og konsekvens for inngrep i personers rettigheter og friheter, 2) hvilket sikkerhetsnivå som er egnet med hensyn til risikoen og 3) hvilke tiltak som er egnet for å oppnå et slikt sikkerhetsnivå. Med andre ord skal risikoen for innsyn reduseres til et tilfredsstillende nivå – noe som i praksis reduserer omfanget av inngrep i privatlivet, men det er ikke et absolutt krav om at det er null risiko for krenkelse.

Den rettighetsbaserte tilnærmingen tilsier derimot at det skal være null risiko for krenkelse. Beskyttelsestiltakene må fullt ut sikre at de registrertes rettigheter etter forordningen ikke krenkes, uansett hvor stor eller liten risikoen er.

Det kan hevdes at den rettighetsbaserte tilnærmingen er lite skalerbar ettersom en aktivitet enten er lovlig eller ulovlig. Imidlertid gjelder dette bare resultatet i seg selv. Selve vurderingen er mer skalerbar fordi den tar form av en proporsjonalitetstest der et inngrep som har hjemmel i lov, etterfølger legitime formål og er nødvendig i et demokratisk samfunn ikke utgjør en krenkelse.

[102] Ibid, pkt. 2.4.1.
[103] Gellert (2020), s. 9.
[104] Ibid, s. 9.

Skalerbarheten til den rettighetsbaserte tilnærmingen kan illustreres med et eksempel Datatilsynet bruker om myndigheters innhenting av offentlig tilgjengelige personopplysninger. De skriver at myndigheters innhenting av offentlig tilgjengelige personopplysninger lettere vil kunne utgjøre et proporsjonalt inngrep enn innhenting av opplysninger som ikke er tilgjengelig for allmenheten. [105] Datatilsynet begrunner ikke svaret, men tanken må være at inngrepet er proporsjonalt fordi ulempen med inngrepet er liten når opplysningene allerede er offentlig tilgjengelig.

Hvis den rettighetsbaserte tilnærmingen er basert på proporsjonalitetsprinsippet, og hvis den risikobaserte tilnærmingen også er basert på proporsjonalitetsprinsippet, undergraver dette den påståtte radikale motsetningen og forskjellen mellom dem. I kjernen handler både rettighetsbasert og risikobasert tilnærming til databeskyttelse om å vurdere proporsjonaliteten av en tenkt behandling.[106] Likheten mellom tilnærmingene viser seg særlig når det er tale om beskyttelsestiltak. Både tiltak etter GDPR art. 32 nr. 1 og tiltak som kreves av Schrems II og EDPB sin sekstrinnsvurdering har til felles at de må tas for å redusere omfanget av inngrep i en grunnleggende rett.

Forskjellen er derimot at tiltakene for den rettighetsbaserte tilnærmingen etter GDPR kap. V skal eliminere enhver risiko for at et inngrep utgjør en «krenkelse», mens tiltakene ved den risikobaserte tilnærmingen i 32 nr. 1 skal redusere risikoen (sannsynlighet og konsekvens) av inngrepet til et tilfredsstillende nivå.

Det er nærliggende å tenke at et inngrep først er på et tilfredsstillende nivå når det er forholdsmessig liten risiko for at det kan utgjøre en krenkelse. I så tilfelle er de to tilnærmingene stort sett sammenfallende og fører til samme konklusjoner om hvilke tiltak man må iverksette. Samtidig kan tilnærmingene ha forskjellige implikasjoner for hvilke tekniske tiltak som anses som tilstrekkelig effektive, nettopp fordi det alltid er en risiko for at utenlandsk etterretning innhenter data.

4.5 Tilnærmingenes betydning for vurdering av beskyttelsestiltak

Ettersom det ved den rettighetsbaserte tilnærmingen er et absolutt krav om null risiko for krenkelse, blir det langt viktigere med tekniske tiltak som kan fjerne all risiko. EDPB taler om å «preclude», altså utelukke potensielt krenkende tilgang.[107] EDPB nevner som eksempel kryptering ved lagring og transport, der de oppstiller nokså omfattende kriterier som må oppfylles

[105] Datatilsynet (2023a).

[106] Gellert (2020), s. 10.

[107] Guidelines 01/2020 (2.0), avsnitt 79.

for at krypteringen skal være et tilstrekkelig effektivt tiltak. Det er utenfor oppgavens rekkevidde å gå inn på de tekniske detaljene, men poenget er at det stilles langt større krav til effektive tekniske tiltak når risikoen skal ned på null, sammenlignet med å få risikoen ned på et «tilstrekkelig» nivå. Blant annet er det ifølge EDPB nødvendig at krypteringsnøklene administreres av en entitet som ikke er underlagt tredjelands lovgivning.[108] Kryptering av data under lagring hvor nøklene holdes unna skyleverandørens besittelse vil i stor grad begrense bruksområdene i skytjenestene.[109] Dermed vil det være mest aktuelt for de fleste skytjenesteleverandører å administrere krypteringsnøklene selv.

Det portugisiske datatilsynet pekte på dette som et moment da de bøtela det nasjonale instituttet for statistikk (Instituto Nacional de Estatística) for flere brudd på GDPR, blant annet problemer knyttet til bruken av Cloudflare Inc., en skytjenesteleverandør lokalisert i USA. Det nasjonale instituttet for statistikk hevdet de hadde gjort tilstrekkelige tiltak ved å sørge for pseudonymisering og kryptering av informasjon.[110] Angående kryptering svarte det portugisiske datatilsynet at kontrakten antydet at Cloudflare hadde krypteringsnøkkelen og dekrypterte datapakker.[111] Dermed var ikke de påståtte databeskyttelseshensynene ivaretatt.[112]

Det italienske datatilsynet har også gitt en uttalelse knyttet til deres utenriksdepartement og testing av elektronisk stemmegivning i valg for italienere i utlandet. Utenriksdepartementet ble pålagt å iverksette ytterligere tiltak dersom det ble overført personopplysninger til tredjeland for å sikre et beskyttelsesnivå som er i det vesentlig samme som i EU, inkludert kryptering gjort av den behandlingsansvarlig med krypteringsnøkler kun tilgjengelig for dem.[113]

Tilnærmingenes betydning for vurdering av beskyttelsestiltak vil dermed i praksis ha mest å si for hvorvidt skytjenesteleverandøren kan sitte på krypteringsnøkkel selv eller ikke. Så lenge en skytjenesteleverandør har tilgang til data i klartekst, eller mulighet til å gjøre om data til klartekst, kan tredjelands myndigheter få utlevert kundens data. Dersom proporsjonalitetstesten anviser at det er tale om et inngrep som teoretisk sett kan utgjøre en krenkelse, må det dermed iverksettes tekniske tiltak som gjør at skytjenesteleverandøren ikke har tilgang på data i klartekst, uansett risiko.

---

[108] Ibid, avsnitt 84 pkt. 6 og avsnitt 90 pkt. 8.

[109] DFØ (2022b), pkt. 2.5.3.1.4.

[110] Engelsk maskinoversettelse kan finnes på https://gdprhub.eu/index.php?title=CNPD_(Portugal)_-_2022/1072, se avsnitt 228.

[111] Ibid, avsnitt 232.

[112] Ibid, avsnitt 233.

[113] 2022 Coordinated Enforcement Action, s. 24.

Med den risikobaserte tilnærmingen kan man etter en lignende proporsjonalitetstest angi at sannsynligheten og konsekvensen er såpass lav at det ikke er forholdsmessig å kreve at den behandlingsansvarlige selv administrerer krypteringsnøkkelen, sett opp mot ulempen dette medbringer.

Oppsummeringsvis må det kunne hevdes at tilnærmingene i praksis har liten betydning for de registrertes friheter og rettigheter ettersom tilnærmingene ved riktig anvendelse av loven alltid vil føre til et tilfredsstillende beskyttelsesnivå som følge av at begge vurderinger inneholder en form for proporsjonalitetsvurdering. Derimot kan tilnærmingene ha langt større betydning for behandlingsansvarlige og databehandlere, ettersom tilgang til personopplysninger i klartekst kan ha mye å si for bruksområdene i skytjenestene. Ettersom det ikke er tale om en overføring i vårt tilfelle er det imidlertid mest naturlig å foreta det som ligner mest på en risikobasert tilnærming som GDPR kap. IV anviser, men også se hen til momenter som nevnes i EDPB sin veiledning om ytterligere tiltak.

Et annet spørsmål er om dette er en god løsning, eller om det bør være slik at man skal ta en mer rettighetsbasert tilnærming til krav om supplerende beskyttelsestiltak i situasjoner der det i utgangspunktet ikke skjer en overføring.

Loven krever at man skal iverksette ytterligere tilleggstiltak (Schrems II) dersom overføring skjer, men det er ikke nødvendigvis slik at man må sørge for de samme tilleggstiltakene (i praksis tekniske tiltak som gir null risiko) for å hindre at slik overføring aldri skjer. Dette fremstår som noe paradoksalt. Dette betyr at loven krever null risiko for krenkelse av personopplysninger dersom vilkårene for overføring er oppfylt, mens den tillater en viss grad av risiko når det ikke er snakk om overføring.

Løsninger for denne inkonsekvensen foreslås avslutningsvis i pkt. 5.2.

5 Rettsfilosofiske- og politiske betraktninger

5.1 Uklarheter i språk og argumentasjon

5.1.1 Innledning

Grunnen til at det her vies plass til rettsfilosofiske betraktninger er at store deler av problemstillingene i oppgaven har vært gjenstand for forholdsvis mye debatt, særlig angående terminologi, som har skapt mye forvirring og usikkerhet blant bedrifter som forsøker å få klarhet og oversikt over hvilke vurderinger som må gjøres. I slike «debatter», for eksempel den som har pågått mellom DFØ/Digdir og Datatilsynet, er det viktig å ramme inn u/enighetene. I denne

sammenheng er det hensiktsmessig å se på juristers språk, og hva diskusjonsdeltakernes utsagn egentlig går ut på. Dersom man ikke har begreper om utsagnstyper eller man anvender dem på utsagn hvor de ikke hører hjemme, så blir debatten tilsynelatende en ordkrig med et misforstått resultat.[114]

Slike rettsfilosofiske betraktninger vil også, for denne oppgavens problemstillinger, kunne være førende for en diskusjon om hvordan loven bør være (de lege ferenda), og det er først og fremst derfor disse rettsfilosofiske betraktningene inkluderes.

5.1.2 «Overføring» som koblingsord, herunder hvordan språk skaper uklarhet om forholdet mellom definisjoner og karakteristikker

Jurister gir ofte sine drøftelser de lege lata i form av definisjonsdrøftelser, f.eks. «hva er en avtale?», «hva er en mangel?»,[115] «hva er en instruks?», «hva er en overføring?». Ofte blir definisjoner eller utsagn om hva noe er muliggjort av formidling gjennom såkalte «koblingsord». Med «koblingsord» sikter man til ord i en viss systematiserende rolle i juristers språk og argumentasjon. Nærmere bestemt ser man på koblingsord som formidlere mellom alternative rettsfakta og kumulative rettsfølger.[116]

Når det gjelder ordet «overføring» kan et rettsfaktum være at behandlingsansvarlig er underlagt GDPR for den gitte behandlingen og enten overfører eller tilgjengeliggjør personopplysninger for en dataimportør i et tredjeland eller dersom dataimportøren er en internasjonal organisasjon. Rettsfølgen(e) kan blant annet være plikt til å gi nødvendige garantier, jf. GDPR art. 46 med alt dette medfølger som å finne ut hvilket overføringsgrunnlag i art. 46 som er best egnet for deres overføring og hvilke ytterligere tiltak som er nødvendig. Med overføring som koblingsord blir regelen: Kapittel V GDPR kommer til anvendelse dersom det skjer en overføring av personopplysninger.

En side ved bruken av koblingsord er at det muliggjør at karakteristikker uttrykkes indirekte, via en definisjon eller via et utsagn om hva noe er.[117] En deskriptiv definisjon av ordet «overføring» er samtidig en indirekte måte å hevde f.eks. at tilsynsmyndigheter eller domstoler i saker om hvorvidt det har skjedd en overføring, erklærer at rettsfølgesiden skal inntre når og

[114] Eng (1998), s. 3.
[115] Ibid, s. 479.
[116] Ibid, s. 479 og 480.
[117] Ibid, s. 481.

bare når de anser kriterier for oppfylt som definisjonen trekker fram,[118] noe som kan skille seg fra hva som anses som «faktisk» overføring.

Tilsynelatende kan en debatt om ordet «overføring» synes å «henge i luften», men med et koblingsordperspektiv ser man argumentasjonens virkelighetstilknytning: debatten er indirekte et uttrykk for karakteristikker. Både deskriptive karakteristikker (utsagn om hvilke rettsregler som faktisk anvendes); normative karakteristikker (utsagn om hvilke rettsregler som bør anvendes); eller sammensmeltede deskriptive og normative karakteristikker (juristers karakteristikker de lege lata).[119]

En nøkkel til juristers språk og argumentasjon de lege lata er å se at disse frittsvevende definisjonsdrøftelsene av hva noe er, ofte er en språklig drakt for karakteristikker vedrørende rett og plikt, og vurderinger og valg.[120]

For eksempel setningen «Peder Ås overfører (i GDPR sin forstand) ikke personopplysninger» uttrykker utenfor jusen et frittsvevende utsagn om hva noe er, eventuelt en deskriptiv definisjon hvis man tar med innholdet i parentesen. Blant personvernjurister er imidlertid setningen en vanlig uttrykksmåte for en sammensmelting av det utsagn at GDPR kapittel V ikke kommer til anvendelse, eller at det ikke er nødvendig med ytterligere tilleggskrav som følger av Schrems II, men også det utsagn at andre personvernjurister antakelig vil mene det samme.[121]

I juristers språk og argumentasjon de lege lata møter man altså en tendens til dobbelt abstraksjon: Fra koblingsords rettsfølgeside (karakteristikksiden). Og fra vurderinger og valg (normativitet). Denne dobbelte abstraksjonen forklarer hvordan jurister kan formulere seg som om de abstrakt drøfter og beskriver hva noe er, mens de egentlig fordeler rett og plikt ut fra vurderinger og valg.[122]

Det kan tenkes at mye av forvirringen knyttet til bruk av skytjenester og overføring til tredjeland kommer av at man anlegger ordet «overføring» en koblingsordsynsvinkel, selv om det etter rettskildene ikke nødvendigvis er grunnlag for det (de lege lata), eventuelt om det ikke bør være slik (de lege ferenda).

[118] Sml. Ibid, s. 481.
[119] Ibid, s. 482.
[120] Ibid, s. 482.
[121] Sml. Ibid s. 482.
[122] Ibid, s. 482 og 483.

Man betrakter f.eks. «eiendomsrett» som en enhetlig størrelse i alle relasjoner, mens det etter rettskildene er slik at en person kan være eier i en relasjon, men ikke i en annen. Kredittkjøperen kan f.eks. være eier i forhold til selger, i den forstand at risikoen for varens ødeleggelse er gått over på ham, mens selgeren fremdeles er eier i forhold til kjøpers konkursbo, i den forstand at han kan stoppe gjenstanden hvis kjøper går konkurs før varen er gått inn på kjøpers lager. I hvilken grad et ord er et koblingsord er et rettsspørsmål, og må løses ved hjelp av alminnelig juridisk metode.[123]

På lignende måte kan man også stå i fare for å betrakte «overføring» som en enhetlig størrelse i alle relasjoner, når man egentlig overfører i større eller mindre grad.

SKATEs veileder ser ut til å generelt fokusere på de deskriptive karakteristikkene. En overføring er en faktisk flyt av informasjon[124] og instruks er en faktisk dokumentert instruks.[125] Definisjonene gjenspeiler virkelighetsoppfatningen. En slik oppfatning vil styrke et syn på retten som noe sikkert og forutberegnelig, men vil samtidig stå i et spenningsforhold til begrepenes operasjonaliserbarhet.

Med et begreps operasjonaliserbarhet sikter man til muligheten for angivelse av intersubjektivt kontrollerbare kriterier for hvorvidt noe faller inn under begrepet eller ikke. Ofte vil begrepets operasjonaliserbarhet være et gradsspørsmål; begrepets tilknytning til intersubjektivt kontrollerbare kriterier kan være mer eller mindre direkte, og mer eller mindre entydig.[126] Med andre ord: Hvis et begrep er operasjonaliserbart, betyr det at forskjellige personer kan bruke de samme kriteriene for å vurdere om noe tilhører kategorien som begrepet beskriver.

EDPB og de tilsynsmyndighetene som tolker loven likt som EDPB ser ut til å anse overføring i større grad som et operasjonaliserbart koblingsord der et viktig rettsfaktum er at tredjelands etterretningsmyndigheter kan få utlevert personopplysninger, og at overføring fungerer som et koblingsord som knytter dette rettsfaktumet til ønskede rettsfølger som er at GDPR kapittel V kommer til anvendelse for den behandlingsansvarlige, med et ansvar og/eller plikt for å sørge for at rettighetene til den registrerte ikke blir krenket. Samtidig angir EDPB tre kumulative kriterier for å vurdere om noe er en overføring – begrepet er dermed operasjonaliserbart.

Det kan imidlertid hevdes at en definisjon av «overføring» ikke trenger å hensynta begrepets operasjonaliserbarhet og at dens systematiserende funksjon er mindre viktig, ettersom

[123] Eng (2018), s. 107.
[124] DFØ (2022a).
[125] DFØ (2022c), pkt. 4.1.3.
[126] Eng (1998), s. 376 og 377.

rettsfølgende ved de vi kan kalle «overføringssituasjoner» uansett ivaretas ved eksisterende rettssikkerhetsmekanismer (GDPR kap. IV), jf. pkt. 4.4 som er tilstrekkelige for å sørge for at rettighetene til den registrerte ikke blir krenket, selv om det ikke nødvendigvis er tale om null risiko.

Til en viss grad er nok dette oppfatningen i dag, noe som vi allerede har vært inne på i pkt. 2. Begrepet «overføring» slik det tolkes i dag av EDPB virker ikke fullt ut systematiserende for å knytte enkelte rettsfaktum opp mot rettsfølger. Det rettsfaktum at tredjelands etterretningsmyndigheter kan få utlevert personopplysninger gjør seg gjeldende selv om man bruker amerikanske skytjenester som er geografisk lokalisert i EØS (ikke overføring). Dette fører til en følelse av inkonsekvens og dermed forvirring angående hvilken tilnærming man skal ha til supplerende beskyttelsestiltak i situasjonen som nevnt i pkt. 4. Det gir videre økt grad av forvirring når begge løsninger trolig gir gode resultater. Selv om det ikke er en overføring og kapittel V ikke anvendes, knyttes likevel rettsfaktumet til en passende rettsfølge – at behandlingsansvarlige plikter å sørge for at egnede tekniske og organisatoriske tiltak iverksettes.

Av samme grunn kan det argumenteres for at begrepet «overføring» ikke trenger å omfatte tilgjengeliggjøring, ettersom det eventuelle inngrepet i den registrertes rettigheter er av en slik art at eksisterende rettssikkerhetsmekanismer er tilstrekkelig til å sørge for at rettighetene til den registrerte ikke blir krenket.[127]

Også heuristiske hensyn, herunder estetiske hensyn, taler for en slik løsning. Med heuristiske hensyn siktes det til ønske om å gjøre en informasjonsmengde lettere å forstå, huske og anvende.[128] Det er lettere å anvende begrepet «overføring» når den viser til faktisk overføring, både materielt og tidsmessig. Den store forvirringen knyttet til overføringsbegrepet illustrerer relevansen av dette hensynet. Den definisjonen som fører til et overføringsbegrep som er lettest å anvende, men samtidig er nokså operasjonaliserbart, kan påstås å være en mellomløsning der EDPB med sine tre kumulative vilkår benyttes, men der vilkår 2 sløyfer «or otherwise makes personal data […] available». Konsekvensen blir i så tilfelle at å opprette en konto, gi tilgangsrettigheter til en eksisterende konto, akseptere en forespørsel om fjernadgang og sende inn et passord til en fil,[129] ikke alene fører til at GDPR kap. V kommer til anvendelse.

Målet med overføringsrestriksjoner er imidlertid å ikke undergrave beskyttelsesnivået som de registrerte sikres i Unionen, jf. fortalepunkt 101. Hvis personopplysninger er tilgjengelige i tredjeland kan dette føre til tilnærmet like mye undergraving av beskyttelse som en faktisk

[127] Se også argumentasjonen i DFØ (2022d), pkt. 6.

[128] Eng (1998), s. 395.

[129] Se Guidelines 05/2021 (2.0), avsnitt 16.

overføring, avhengig av typen personopplysninger som blir tilgjengelig. Dette tilsier i motsatt retning at overføringsbegrepet bør omfatte tilgjengeliggjøring slik EDPB anviser.

5.1.3 «Instruks» og ansvarsfraskrivelse, herunder årsaker til at språkformer brukes uten at uklarheter fjernes

Det finnes flere midler til ansvarsfraskrivelse. En av disse er å bruke flertydige eller ensidig deskriptive uttrykksmåter til ansvarsfraskrivelse på en mer direkte måte i tilfelle hvor den omtvistede handlingen er en fastsatt norm: En minister vil f.eks. fraskrive seg ansvar for instruks til et forvaltningsorgan, en som deltok i avtaleforhandlinger vil fraskrive seg ansvar for tilbud, aksept eller annen bindende partsdisposisjon, og derved ansvar for at avtale kom i stand,[130] eller en behandlingsansvarlig som deltok i avtaleforhandlinger om bruk av en skytjeneste vil fraskrive seg ansvar for at det skjer en utlevering av personopplysninger til tredjelands etterretning.

I disse tilfellene kan man oppnå ansvarsfraskrivelse ved å blande de grunnleggende utsagnstyper i handlingen selv: Man lar det være uavklart hvorvidt man har fastsatt en norm eller bare sagt noe om tro, forventninger, forhåpninger, e.l. Man fraskriver seg ansvaret ved å fraskrive seg handlingen selv.[131]

Det er allerede argumentert for at en «instruks» og dermed også forbehold i skytjenesteavtaler gir normative føringer for når en databehandler kan sies å ha handlet utenfor eller innenfor instrukser. Dersom man derimot anlegger en løsning som SKATEs veileder argumenterer for: at «instruks» forutsetter en viss retning og tydelighet og at databehandleren anser seg som instruert,[132] åpner man opp for større mulighet for uklarhet om hvorvidt instruks er gitt.

Den behandlingsansvarlige vil da i ettertid kunne vise tendens til å tolke forbeholdet som ikke-instrukser dersom utlevering mot formodning skjer. Databehandleren på sin side kan omvendt vise tendens til å tolke forbeholdet som instrukser dersom utlevering skjer. Begge parter har interesse i at forbeholdets status ikke avklares for at en databehandleravtale skal komme i stand, men dette er ikke en særlig tillitsskapende løsning og det fjerner heller ikke risikoen for at utlevering kan skje.[133] Dermed blir det viktig å utarbeide instruksene og eventuelle forbehold på en slik måte at partenes forventninger og forpliktelser er tydelige slik at det ikke blir mulig med noe ansvarsfraskrivelse.

[130] Eng (1998), s. 486.
[131] Ibid, s. 487.
[132] DFØ (2022c), pkt. 4.1.6.
[133] Sml. Eng (1998) s. 495.

Av hensyn til ansvarspulverisering, som også er nevnt i pkt. 3.2, jf. fortalepunkt 79 er det dermed hensiktsmessig at de fleste forbehold om utlevering til etterretningsmyndigheter anses som instrukser.

5.2 Avslutning

En mulig løsning for forvirring rundt risiko for innhenting av personopplysninger til etterretningsformål kan være å tydelig skille mellom tilsiktet og utilsiktet overføring, slik det danske datatilsynet taler om i deres veiledning om sky.[134] Det må kunne forutsettes at ingen parter ønsker å utlevere personopplysninger til utenlandsk etterretning og at slik utlevering alltid vil være utilsiktet.

Hvis en skytjenesteleverandør da overfører personopplysninger til tredjeland i strid med databehandleravtalen vil det være hensiktsmessig å kalle dette for en utilsiktet overføring, som betyr at GDPR kapittel V ikke kommer til anvendelse for den behandlingsansvarlige. Den behandlingsansvarlige må likevel gjøre risikovurderinger i henhold til GDPR kap. IV for å sikre nødvendig behandlingssikkerhet, herunder sørge for supplerende beskyttelsestiltak med en risikobasert tilnærming.

I databehandleravtalen bør skytjenesteleverandøren tydelig indikere om den er underlagt lovgivning i tredjeland, som på tross av instrukser fra den behandlingsansvarlige, vil kunne pålegge skytjenesteleverandøren å utlevere personopplysninger. I det en databehandler utleverer personopplysninger i strid med databehandleravtalen vil denne anses som selvstendig behandlingsansvarlig.

U/tilsiktet overføring som terminologi vil ikke føre til noen andre resultater enn det som er konklusjonene i pkt. 2-4 (de lege lata). Imidlertid kan det argumenteres for at dette ville ført til mindre forvirring, herunder redusert uklarhet i språk og argumentasjon angående risiko for utlevering til utenlandsk etterretning.

Dette gir imidlertid ikke tilfredsstillende svar på hvorfor behandlingsansvarlige må sørge for null risiko (tilstrekkelige tekniske tiltak) når databehandleravtalen inneholder et forbehold, mens det er nok med tilstrekkelig lav risiko dersom databehandleravtalen ikke inneholder et forbehold. Ansvaret allokeres riktignok til skytjenesteleverandøren som vil kunne bli behandlingsansvarlig, men beskyttelsesnivået til de registrerte vil fortsatt undergraves etter GDPR kapittel V sin standard.

[134] Se Vejledning om cloud (2022), s. 29 og 30.

Det kan påstås at dette i praksis likevel er en balansert løsning som oppfyller målsetninger som tilstrekkelig vern av friheter og rettigheter til de registrerte, samtidig som det tas hensyn til målsetning om økonomiske og effektive løsninger. Derimot gir dette en dårlig indre sammenheng med tanke på rettssystematiske hensyn.

Jeg anser det for å være to løsninger på denne inkonsekvensen.

Den første løsningen innebærer å akseptere en viss grad av risiko for at beskyttelsesnivået for de registrerte svekkes ved både tilsiktet og utilsiktet overføring. Dette alternativet bygger på forutsetningen om at risikoen ved behandling av personopplysninger ikke nødvendigvis må elimineres fullstendig, slik det fremkommer av den risikobaserte tilnærmingen i GDPR kap. IV. Denne løsningen tillater den behandlingsansvarlige å tilpasse sine plikter og ressurser på en proporsjonal og skalerbar måte.

Den andre mulige løsningen krever at tilsiktet og utilsiktet overføring behandles på lik linje ved å sikre null risiko for begge – det vil si å anvende en rettighetsbasert tilnærming også utenfor GDPR kapittel V sitt anvendelsesområde. Dette alternativet er mer restriktivt og kan begrense behandlingsansvarliges og databehandleres fleksibilitet, men vil eliminere all risiko.

Jeg anser den første løsningen med risikobasert tilnærming for å være mest hensiktsmessig. Denne tilnærmingen anerkjenner at det ikke alltid er forholdsmessig å eliminere all risiko og gir behandlingsansvarlige muligheten til å tilpasse sine plikter og ressurser på en proporsjonal og skalerbar måte. Dessuten synes risikovurderingsmekanismene i GDPR kap. IV å sikre et tilfredsstillende beskyttelsesnivå for de registrertes friheter og rettigheter, ettersom slike risikovurderinger er effektive for å vurdere proporsjonaliteten av en tenkt behandling.

6 Litteraturliste

6.1 Juridisk litteratur

6.1.1 Bøker

Aall (2018) — Aall, Jørgen «Rettsstat og menneskerettigheter», 5. Utg. Fagbokforlaget, 2018

Eng (1998) — Eng, Svein «U/Enighetsanalyse – med særlig sikte på jus og allmenn rettsteori», Universitetsforlaget, 1998

Eng (2018) — Eng, Svein «Rettsfilosofi», 4. Utg. Universitetsforlaget, 2018

Fredriksen og Mathisen (2019) — Fredriksen, Halvard Haukeland og Gjermund Mathisen «EU-rett som norsk rettskilde» i boka: *Juridisk Metode og Tenkemåte* Alf Petter Høgberg og Jørn Øyrehagen Sunde (red.) Universitetsforlaget, 2019

Gellert (2020) — Gellert, Raphael «The Risk-Based Approach to Data Protection», Oxford University Press, 2020

Kuner (2020) — Kuner, Chrisopher «Article 44. General principle for transfers» i boka: *The EU General Data Protection Regulation – A Commentary* Kuner, Christopher, Bygrave, Lee A., Docksey, Chrisopher (red.) 1. Utg. Oxford University Press, 2020

Schartum (2020) — Schartum, Dag Wiese «Personvernforordningen – En lærebok», 1. Utg. Fagbokforlaget, 2020

Skullerud mfl. (2018) — Skullerud, Åste Marie Bergseng, Cecilie Rønnevik, Jørgen Skorstad og Marius Engh Pellerud. «Personvernfordningen (GDPR) – Kommentarutgave», Universitetsforlaget, 2018

6.1.2 Artikler

Olsen og Tønseth (2022) — Olsen, Thomas og Malin Tønseth *Full forvirring om skytjenester* (07.12.2022). Tilgjengelig: https://svw.no/artikler/full-forvirring-om-skytjenester

6.2 Norske lover

Personopplysningsloven 2018 — Lov av 15. juni 2018 nr. 31 om behandling av personopplysninger (personopplysningsloven)

6.3 Traktater

EMK — Konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter, Roma 4. november 1950. [Offisiell norsk oversettelse].

Charteret — Convention for the Protection of Human Rights and Fundamental Freedoms, Rome 4 November 1950.

TEU — Traktaten om den Europæiske Union. Konsolideret udgave 2016 (EUT 2016/C 202/01).

TEUV — Traktaten om den Europæiske Unions funktionsmåde. Konsolideret udgave 2016 (EUT 2016/C 202/01).

6.4 EU-direktiver og forordninger

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 2016/579	Europaparlaments- og rådsforordning (EU) 2016/579 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* [Personvernforordningen]

6.5 Rettspraksis fra EU-domstoler

No 5029/71 *Klass and others v. Germany*	Dom av 06. september 1978, *Klass and others v. Germany,* ECLI:CE:ECHR:1978:0906JUD000502971
C-101/01 *Lindqvist*	Dom av 06. november 2003, *Lindqvist*, ECLI:EU:C:2003:596
C-201/13 *Deckmyn*	Dom av 03. september 2014, *Deckmyn*, ECLI:EU:C:2014:2132
C-362/14 *Schrems I*	Dom av 06. oktober 2015, *Schrems I*, ECLI:EU:C:2015:650
C-210/16 *Wirtschaftsakademie*	Dom av 05. juni 2018, *Wirtschaftsakademie*, ECLI:EU:C:2018:388
C-210/16 *(Opinion of Advocate General)*	Uttalelse av 24. oktober 2017, *Wirtschaftsakademie*, ECLI:EU:C:2017:796
C-40/17 *Fashion-ID*	Dom av 29. juli 2019, *Fashion-ID*, ECLI:EU:C:2019:629
C-311/18 Schrems II	Dom av 16. juli 2020, *Schrems II*, ECLI:EU:C:2020:559
No 58170/13 *Big Brother*	Dom av 25. mai 2021, *Big Brother Watch and others v. The United Kingdom,* ECLI:CE:ECHR:2021:0525JUD005817013

6.6 Veiledere, uttalelser m.m. fra EU-organer

EDPS (2014)	EDPS, Position Paper *The transfer of personal data to third countries and international organisations by EU institutions and bodies* (14. juli 2014)
Guidelines 01/2020 (2.0)	EDPB Guidelines 01/2020 *on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (vedtatt 18. juni 2021)
Guidelines 07/2020	EDPB Guidelines 07/2020 *on the concepts of controller and processor in the GDPR* (vedtatt 07. juli 2021)
Guidelines 05/2021 (1.0)	EDPB Guidelines 05/2021 *on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR* (vedtatt 18. november 2021)
Guidelines 05/2021 (2.0)	EDPB Guidelines 05/2021 *on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR* (vedtatt 14. februar 2023)
Joint Committee (2018)	Decision of the EEA Joint Committee No 154/2018 *amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022]* (6. juli 2018)
Opinion 01/15	Opinion 01/15 of the Court (Grand Chamber) (vedtatt 26. juli 2017)
Opinion 01/2014	WP29 Opinion 01/2014 *on the application of necessity and proportionality concepts and data*

	protection within the law enforcement sector (vedtatt 27. februar 2014)
Recommendations 02/2020	EDPB Recommendations 02/2020 *on the European Essential Guarantees for surveillance measures* (vedtatt 10. november 2020)
2022 Coordinated Enforcement Action	EDPB 2022 Coordinated Enforcement Action *Use of cloud-based services by the public sector* (vedtatt 17. januar 2023)

6.7 Øvrige kilder

Datatilsynet (2023a)	Datatilsynet 2023 *Overføring av personopplysninger ut av EØS – Tilleggskrav* (sist endret 16.03.2023). Tilgjengelig: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/tilleggskrav-til-overforingsgrunnlag-schrems-ii/
Datatilsynet (2023b)	Datatilsynet 2023 *Overføring av personopplysninger ut av EØS – Innledning* (sist endret 16.03.2023). Tilgjengelig: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/
Datatilsynet (2023c)	Datatilsynet 2023 *Overføring av personopplysninger ut av EØS – Opplysninger behandlet i EØS, inkludert skytjenester i EØS* (sist endret: 16.03.2023). Tilgjengelig: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/personopplysninger-utelukkende-behandlet-i-eos/

Datatilsynet (2021) Datatilsynet 2021 *Nye standardavtaler* (publisert 09.06.2021). Tilgjengelig: https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/nye-standardavtaler/

Det Danske Datatilsynet (2022) Det Danske Datatilsynet 2022 *Vedrørende tilsigtede eller utilsigtede overførsler til tredjelande* (publisert 29.03.2022). Tilgjengelig: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/mar/vedroerende-tilsigtede-eller-utilsigtede-overfoersler-til-tredjelande

Det Norske Akademis Ordbok Det Norske Akademis Ordbok *instruks* Tilgjengelig: https://naob.no/ordbok/instruks

DFØ (2022a) DFØ Veiledning for offentlig sektors bruk av skytjenester etter Schrems II, *Hva er en overføring? (Oppdatert: 14.09.2022)* Tilgjengelig: https://markedsplassen.anskaffelser.no/hva-er-en-overforing

DFØ (2022b) DFØ Veiledning for offentlig sektors bruk av skytjenester etter Schrems II, *Hjelp til å vurdere personvernrisikoen for innhenting til etterretningsformål* (Oppdatert 11.10.2022) Tilgjengelig: https://markedsplassen.anskaffelser.no/veiledning/veiledning-etter-schrems-ii/personvern-risiko-for-etterretning/96

DFØ (2022c) DFØ Veiledning for offentlig sektors bruk av skytjenester etter Schrems II, *Betyr skytjenesters forbehold i avtalen at jeg instruerer dem?* (Oppdatert 14.09.2022) Tilgjengelig: https://markedsplassen.anskaffelser.no/veiledning/veiledning-etter-schrems-ii/105

DFØ (2022d) DFØ Veiledning for offentlig sektors bruk av skytjenester etter Schrems II, *Overføring av personopplysninger ved supporttjenester* (Oppdatert

14. september 2022) Tilgjengelig: https://markedsplassen.anskaffelser.no/overforing-av-personopplysninger-ved-supporttjenester

Eurostat (2021) Eurostat *Cloud computing used by 42% of enterprises* Tilgjengelig: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20211209-2

Vejledning om cloud (2022) Det danske datatilsynet *Vejledning om cloud* (Mars 2022). Tilgjengelig: https://www.datatilsynet.dk/Media/637824109172292652/Vejledning%20om%20cloud.pdf