UiO : Det juridiske fakultet

EU-domstolens avgjørelse C-362/14 «Schrems»

En analyse og vurdering av avgjørelsens betydning for reglene om overføring av personopplysninger til land utenfor EU og EØS

Kandidatnummer: 703

Leveringsfrist: 25.04.16

Antall ord: 17 857

Innholdsfortegnelse

1 Innledning

1.1 Tema og bakgrunn

Temaet for avhandlingen er betydningen av EU-domstolens avgjørelse av 6. oktober 2015, «Schrems-avgjørelsen»[1], for tolkningen av reglene om overføringer av personopplysninger til utlandet i EUs personverndirektiv.[2] Overføring av personopplysninger på tvers av landegrensene har lenge vært et sentralt aspekt ved personvernretten. For eksempel var harmonisering av de nasjonale reglene om overføringer av personopplysninger til andre land hovedårsaken til at Organisasjonen for økonomisk samarbeid og utvikling («OECD») begynte arbeidet med et internasjonalt regelverk for personvern på 70-tallet.[3]

Siden den gang har det skjedd en betydelig utvikling i kompleksiteten og omfanget av overføringer av personopplysninger mellom land.[4] Vi har opplevd en internasjonalisering av økonomi og kommunikasjon, store teknologiske fremskritt og større flyt av informasjon mellom myndigheter, selskaper og privatpersoner. Internett har forenklet global kommunikasjon og handel, og personopplysninger er blitt en viktig valuta for betaling av nettjenester.[5] Regler om overføring av personopplysninger over landegrensene kan påvirke en rekke aktiviteter i den globale hverdagen, som utkontraktering av arbeidsoppgaver og bruk av sosiale medier og skytjenester.

Det har kommet få avgjørelser om tolkningen av personverndirektivets regler om overføring av personopplysninger til utlandet siden direktivet ble vedtatt i 1995. I 2015 avsa imidlertid EU-domstolen Schrems-avgjørelsen. Avgjørelsen har særlig fått oppmerksomhet fordi EU-domstolen erklærte «Safe Harbor-beslutningen»[6] ugyldig. Mange amerikanske selskaper brukte beslutningen som grunnlag for å motta personopplysninger fra EU. I tillegg er avgjørelsen viktig fordi EU-domstolen kommer med generelle uttalelser om tolkningen av direktivets regler om overføring av personopplysninger.

1.2 Problemstilling, presiseringer og avgrensninger

Formålet med avhandlingen er å analysere og drøfte *hvilke krav Schrems-avgjørelsen stiller til overføringer av personopplysninger utenfor EU og EØS*. Den overordnede tesen er at i

---

1 C-362/14 Maximillian Schrems v Data Protection Commissioner

2 Direktiv 95/46/EC, heretter «personverndirektivet» eller «direktivet»

3 Bing (2014) s. 127

4 Kuner (2013) s. 1

5 Kuner (2013) s. 2

6 Decision 2000/520/EC

Schrems-avgjørelsen stiller EU-domstolen strenge og omfattende krav til overføringer av personopplysninger. Kravene følger av at domstolen legger avgjørende vekt på den grunnleggende retten til personvern fremfor realpolitiske hensyn som tilsier en mindre omfattende regulering av overføringer av personopplysninger.

For å forklare hvorfor EU-domstolen tillegger retten til personvern så stor vekt, tar avhandlingen utgangspunkt i ett rettslig og ett faktisk forhold. For det første ble EU-charteret, som gjør personvern til en grunnleggende rett, rettslig bindende og opphøyd på linje med EU-traktatene i 2009.[7] For det andre lekket Edward Snowden i 2013 store mengder dokumenter som blant annet tydet på at amerikanske myndigheter masseovervåket internasjonal tele- og datatrafikk i og utenfor USA.[8]

Hoveddelen av oppgaven er følgelig en rettsdogmatisk analyse av de materielle sidene ved Schrems-avgjørelsen. Avhandlingen drøfter både Schrems-avgjørelsens forhold til gjeldende rett i EUs personverndirektiv og hvordan avgjørelsen videreutvikler rettstilstanden. I tillegg vurderer avhandlingen Schrems-avgjørelsens resultat fra et rettspolitisk perspektiv. Avhandlingen drøfter særlig om Schrems-avgjørelsens strenge krav til personvern gjør det unødvendig vanskelig å overføre personopplysninger til utlandet og om EUs regler om overføring av personopplysninger er for inngripende i andre lands regulering av personvern.

Ettersom oppgavens tema er en avgjørelse fra EU-domstolen, tar jeg utgangspunkt i rettstilstanden etter EU-retten og anvender EU-rettens metode og rettskilder. Av hensyn til ordgrensen behandler jeg ikke andre rettsområder enn personvern og i mindre grad norsk personvernrett. Vurderingene av EU-retten kan likevel være relevante for norsk rett. Selv om Norge ikke er medlem av EU og dermed ikke folkerettslig bundet av EU-retten, er Norge forpliktet til å implementere EU-rett som er gjort til en del av EØS-avtalen, jf. EØS-loven § 1. Personverndirektivet ble innlemmet i EØS-avtalen i 1999.[9]

Schrems-avgjørelsen gjaldt reglene om overføringer av personopplysninger til tredjeland i personverndirektivet. Jeg behandler derfor ikke andre regelverk enn personverndirektivet og den kommende personvernforordningen som skal erstatte direktivet. Avhandlingen følger rettsutviklingen frem til 13. april 2016.

---

7 Europakommisjonen (2016)a

8 Restad (2015)

9 EØS-komiteen (1999), jf. St.prp. nr. 34 (1999-2000). Direktivet er transformert til norsk rett gjennom Lov 14.4.2000 nr. 31 om behandling av personopplysninger (Personopplysningsloven), se særlig §§ 29,30. EØS-landene har et visst spillerom ved implementeringen av direktivet, og personopplysningsloven skiller seg derfor på visse områder fra direktivet, se Schartum (2011) s. 86

1.3 Metode og rettskildebildet

1.3.1 EU-rettslig metode

EU-rettslig metode innebærer at tolkningen av rettsakten skal skje uavhengig av det enkelte medlemslandet nasjonale rettssystem; ellers ville man risikere forskjellige rettstilstander i EU-landene.[10] Man tar utgangspunkt i en alminnelig forståelse av ordlyden i rettsakten, med mindre det finnes legaldefinisjoner.[11] Imidlertid må man ta hensyn til at EU har 24 offisielle språk og potensielt tilsvarende mange autentiske språkversjoner.[12] Derfor er kontekstuell og formålsorientert tolkning viktig.[13] Avhandlingen tar utgangspunkt i den engelske versjonen av rettskildene fordi språket i Schrems-avgjørelsen var engelsk.[14] Ved tolkning av sentrale uttrykk benyttes også andre språkversjoner for å få frem nyanser i tolkningen.

Videre kan man bruke rettsaktens fortale for å utlede dens formål.[15] Derimot er rettsaktens forarbeider generelt sett en mindre viktig rettskilde.[16] EU-rettens avgjørelser er en tungtveiende rettskilde i EU, men avgjørelsene anses ikke som prejudikater verken for nasjonale domstoler eller for EU-domstolen selv.[17] Det er forbud mot offentlige dissenser i EU-domstolens avgjørelser, og premissene kan derfor synes knappe og vage, og man kan ikke alltid trekke et tydelig skille mellom avgjørelsenes *ratio decidendi* og *obiter dicta*.[18]

1.3.2 Rettskilder

Reglene om overføring av personopplysninger til utlandet er inntatt EUs personverndirektiv artikkel 25 og 26. Siden Schrems-avgjørelsen gjaldt tolkningen av førstnevnte bestemmelse, fokuserer avhandlingen mest på den. Direktivets formålsbestemmelse i artikkel 1 og fortalen gir også veiledning for tolkningen. Videre drøfter avhandlingen reglene om overføring av personopplysninger til utlandet i den kommende personvernforordningen. Jeg tar utgangspunkt i forordningsforslaget av 6. april 2016.

---

10 Fredriksen (2014) s. 218

11 Fredriksen (2014) s. 219

12 Fredriksen (2014) s. 219-220, Arnesen (2015) s. 31-33

13 Arnesen (2015) s. 29

14 Schrems-avgjørelsen merknad *

15 Fredriksen (2014) s. 228

16 Arnesen (2015) s. 29

17 Fredriksen (2014) s. 238. Avgjørelsene er heller ikke prejudikater for EØS-landene utenfor EU, men i praksis tillegges avgjørelse ofte vekt ved tolkningen av EØS-rett av hensyn til homogenitetsprinsippet, se Arnesen (2015) s. 26, Fredriksen (2014) s. 259

18 Fredriksen (2014) s. 240

I Schrems-avgjørelsen tolker EU-domstolen personverndirektivet i lys av Den europeiske unions Charter om grunnleggende rettigheter («EU-charteret» eller «charteret»). Charteret ble vedtatt i 2000 og ble rettslig bindende for EUs institusjoner og EU-landenes myndigheter i 2009.[19] Domstolen tolker også personverndirektivet i lys av bestemmelser i Traktaten om Den europeiske unions virkeområde («TEUV»). TEUV artikkel 267 gir dessuten EU-landenes nasjonale domstoler rett til å be EU-domstolen om en forhåndsavgjørelse om tolkningen av EU-rettslige spørsmål. Schrems-avgjørelsen er en slik forhåndsavgjørelse.

Det er lite rettspraksis fra EU-domstolen om personverndirektivets regler om overføring av personopplysninger til utlandet[20]. Domstolen har derimot avsagt avgjørelser som ikke direkte gjelder direktivet artikkel 25 eller 26, men som likevel gir veiledning for hvordan bestemmelsene skal tolkes.[21] EUs generaladvokat Bot gav en innstilling i Schrems-avgjørelsen. Slike innstillinger er ikke en del av EU-domstolens avgjørelse, men dersom domstolen bygger på innstillingen, kan en grundigere redegjørelse i innstillingen supplere en knapp begrunnelse fra domstolen.[22]

Både Europakommisjonen (heretter også «kommisjonen») og Artikkel 29-arbeidsgruppen (heretter også «arbeidsgruppen») har kommet med uttalelser om tolkningen av Safe Harbor-beslutningen, Schrems-avgjørelsen og regelverket som skal erstatte Safe Harbor-beslutningen. kommisjonens meddelelser regnes imidlertid som etterfølgende retningslinjer, og de har begrenset selvstendig rettskildeverdi.[23] Artikkel 29-arbeidsgruppens rådgivende uttalelser om tolkningen av personverndirektivet er dessuten ikke rettslig bindende, jf. personverndirektivet art. 29(1). Imidlertid er arbeidsgruppen sammensatt av blant annet eksperter fra de nasjonale datatilsynene i EU-landene, jf. personverndirektivet art. 29(2). Arbeidsgruppen har derfor i praksis stor innflytelse.[24]

Jeg anvender også ulike internasjonale avtaler for å tolke Schrems-avgjørelsen og reglene i personverndirektivet: OECDs personvernretningslinjer fra 1980, Europarådets personvernkonvensjon fra 1981 og Den europeiske menneskerettskonvensjon («EMK») artikkel 8 med

---

19 Europakommisjonen (2016)a

20 Case C-101/01 Lindqvist, Schrems-avgjørelsen

21 Eksempelvis case C-293/12 Digital Rights Ireland, som gjaldt gyldigheten av datalagringsdirektivet (direktiv 2006/24/EC)

22 Fredriksen (2014) s. 245-246

23 Fredriksen (2014) s. 230

24 Büllesbach (2010) s. 139

tilhørende rettspraksis fra Den europeiske menneskerettsdomstol («EMD»). Jeg bruker dessuten juridisk teori for å belyse rettstilstanden og tolkningsproblemer.

1.4 Begrepsavklaringer

Formålet med dette delkapitlet er å presisere hvordan avhandlingen bruker utvalgte sentrale begreper. Fordi avhandlingen tolker EU-rett, legges det EU-rettslige meningsinnholdet til grunn selv om avhandlingen bruker norske begreper.

1.4.1 Personvern

Personvern er ikke et universalt definert rettslig begrep. I avhandlingen reflekterer «personvern» begrepene «*data protection*» og «*privacy*», som er vanlige i EU-retten. Begrepene anvendes ofte om hverandre, selv om de har noe ulikt meningsinnhold, se også avsnitt 4.5.2.3[25]

1.4.2 Personopplysninger og behandling av personopplysninger

Personverndirektivet omhandler behandling av personopplysninger («*processing of personal data*»), jf. direktivet art. 1(1). Personopplysninger defineres som «*any information relating to an identified or identifiable natural person ('data subject')*», jf. art. 2(a). Det individet som personopplysningene kan knyttes til, «*data subject*», betegnes heretter som den registrerte. Etter ordlyden er ikke direktivet begrenset til å gjelde opplysninger med et bestemt innhold. Det er for eksempel uten betydning om opplysningene gjelder private eller arbeidsrelaterte forhold.[26]

Det sentrale kriteriet er at opplysningene gjelder et bestemt individ som direktive eller indirekte er identifisert eller kan identifiseres, jf. direktivet art. 2(a). Det er tilstrekkelig at individet kan identifiseres ved hjelp av metoder som en hvilken som helst person med rimelighet kan forventes å ta i bruk.[27] Personopplysninger er følgelig et vidt begrep, og reglene om overføring av personopplysninger til utlandet kan derfor potensielt komme til anvendelse på et bredt spekter av informasjon.

Behandling («*processing*») av personopplysninger er definert som «*any operation or set of operations which is performed upon personal data, whether or not by automatic means […]*»,

---

[25] Bygrave (2014) s. 26, Kuner (2013) s. 19-20

[26] Case C-101/01 Lindqvist (24)

[27] Direktiv 95/46/EC fortalen (26)

jf. personverndirektivet art. 2(b). Selv om overføringer av opplysninger til andre land ikke er uttrykkelig nevnt i ordlyden, er det klart at direktivet omfatter slike overføringer.[28]

1.4.3 Behandlingsansvarlig og databehandler

En behandlingsansvarlig («*controller*») er en «*natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data*», jf. direktivet art. 2(d). De fleste av forpliktelsene etter personverndirektivet er lagt til den behandlingsansvarlige.[29]

En databehandler («*processor*») er en «*natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller*», jf. direktivet art. 2(e). Ved utkontraktering som involverer overføring av personopplysninger til utlandet, vil gjerne behandlingsansvarlig forbli behandlingsansvarlig, mens den som utfører oppdaget, vil være databehandler.[30] Databehandleren må imidlertid forplikte seg til å følge den behandlingsansvarliges instruksjoner og sørge for informasjonssikkerhet ved behandlingen, jf. direktivet art. 17(2) og (3).

1.4.4 Overføringer til tredjeland

Det er ikke åpenbart hva som regnes som en overføring («*transfer*») av personopplysninger til utlandet etter personverndirektivet artikkel 25 og 26. Begrepet er ikke legaldefinert verken i personverndirektivet eller i forslaget til personvernforordningen. Artikkel 29-arbeidsgruppen har heller ikke gitt uttalelser om overføringsbegrepet. Skjer det eksempelvis en overføring når en europeer laster opp personlig informasjon til en nettside som har en server i USA? Internettets struktur gjør det vanskelig både for sender og mottaker å vite og kontrollere hvilke land informasjonen sendes gjennom, og EU-domstolen har ikke gitt entydig uttrykk for om opplastninger til internett er overføringer.[31] Avhandlingen går ikke nærmere inn på grensedragningen, men det kan poengteres at det ville vært en fordel med en avklaring av hva som ligger i «*transfer*».

Begrepet tredjeland («*third country*») i personverndirektivet artikkel 25(1) er heller ikke legaldefinert. Ut fra sammenhengen må det likevel antas at «tredjeland» sikter til land som ikke

---

28 Schrems-avgjørelsen (45)

29 Bullesbach (2010) s. 37

30 Se også Ot.prp.nr.92 (1998-1999) s. 103

31 Kuner (2013) s. 12-13 med henvisning til case C-101/01 Lindqvist

er adressert i personverndirektivet, altså land som ikke er medlem av EU.[32] Siden Norge ikke er med i EU, er Norge i utgangspunktet et tredjeland. EØS-komiteen har imidlertid innlemmet personverndirektivet i EØS-avtalen, og derfor likestilles Norge med EU-landene.[33] Når det i den videre fremstillingen vises til EU-landene, kan dette derfor leses som EØS-landene. Avhandlingen bruker «dataeksportør» om senderen av personopplysningene i EU-landet og «dataimportør» om mottakeren av personopplysningene i tredjelandet.

1.4.5 Tilsynsmyndighet

Personverndirektivet pålegger hvert EU-land å opprette en uavhengig tilsynsmyndighet («*supervisory authority*», heretter også «datatilsyn» eller «tilsyn») som skal kontrollere implementeringen av direktivet, jf. direktivet art. 28.[34] De nasjonale datatilsynene har ulike kompetanser og oppgaver, blant annet ved overføringer av personopplysninger til tredjeland.

1.5 Videre fremstilling

Oppgavens videre fremstilling er tredelt. Først belyses rettstilstanden før Schrems-avgjørelsen. I kapittel 2 redegjør jeg for det rettslige bakteppet for Schrems-avgjørelsen: Personverndirektivets regler om overføring av personopplysninger til tredjeland. For å forstå hvorfor EU-domstolen erklærte Safe Harbor-beslutningen ugyldig i Schrems-avgjørelsen, ser jeg nærmere på bakgrunnen for at beslutningen ble truffet, hva den gikk ut på og hva den ble kritisert for i kapittel 3.

Oppgavens hoveddeler, kapittel 4 og 5, inneholder analyser og vurderinger av Schrems-avgjørelsen. Jeg fokuserer på hvilke rettssetninger som kan utledes av avgjørelsen og reflekterer rundt disse. Dessuten drøfter jeg avgjørelsens rekkevidde både for overføringer etter direktivet artikkel 25 og artikkel 26 og for den kommende personvernforordningen.

Til slutt drøfter jeg rettstilstanden etter Schrems-avgjørelsen. I kapittel 6 gjør jeg noen rettspolitiske vurderinger av Schrems-avgjørelsens resultat. Videre gir jeg en kort presentasjon og analyse av det nye regelverket som tilsikter å erstatte Safe Harbor-ordningen. Kapittel 7 inneholder en oppsummering av avhandlingens vurderinger og konklusjoner.

---

32 Büllesbach (2010) s. 113

33 EØS-komiteen (1999)

34 Tilsynsmyndigheten i Norge er Datatilsynet, se personopplysningsforskriften § 42

2 Reglene om overføring av personopplysninger til tredjeland

2.1 Overordnede hensyn for og mot overføringer av personopplysninger til utlandet

Det er ulike hensyn som taler henholdsvis for fri flyt av personopplysninger over landegrensene og for å begrense adgangen til å overføre personopplysninger til utlandet. Fri utveksling av opplysninger kan fremme global ytringsfrihet fordi man får mulighet til å dele informasjon og utveksle synspunkter på tvers av nasjonalitet og kultur.[35] Fri flyt av opplysninger kan også bidra til økonomisk, teknologisk og sosial vekst og vitenskapelig samarbeid.[36] Deling av informasjon kan dessuten være nyttig for offentlige myndigheter, eksempelvis for helsevesenet.[37] I tillegg åpner overføring av informasjon over landegrensene for at privatpersoner raskt og enkelt kan holde kontakt med familie og venner over hele verden og få tilgang til tjenester, særlig over internett, som ikke tilbys i deres land.[38]

Det er også potensielle farer ved å tillate overføringer av personopplysninger over landegrensene. Man risikerer at det skjer inngrep i individets grunnleggende rett til personvern, og personopplysninger kan misbrukes med eller uten den registrertes kjennskap til det. Ikke bare individer, men også selskaper, kan ha en interesse i å forhindre slike inngrep. Dersom selskaper ikke har kontroll på personopplysninger, kan selskapets kunder og samarbeidspartnere miste tilliten til dem.[39] Dessuten kan det gå utover individers rett til personvern dersom personopplysninger overføres til land der myndighetene mangler ressurser for å hindre inngrep i personvernet, eller der myndighetenes bruk av personopplysningene strider med grunnleggende rettigheter, eksempelvis ved masseovervåkning.[40]

Personverndirektivets regler om overføring av personopplysninger til utlandet er et utslag av avveininger mellom slike hensyn. Reglene skal «*protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data*», jf. direktivet art. 1(1). Reglenes formål er å hindre at den beskyttelsen personopplysninger får i ett land, uthules ved at opplysningene blir overført og behandlet i et annet land.[41] Derfor tar reglene sikte på å harmonisere beskyttelsesnivået for personopplysninger;

---

35 Kuner (2013) s. 102

36 Direktiv 95/46/EC fortalen (5) og (6)

37 Kuner (2013) s. 102

38 Kuner (2013) s. 102

39 Kuner (2013) s. 104

40 Tønseth (2016) s. 120, Kuner (2013) s. 103-104

41 Kuner (2013) s. 107

dersom beskyttelsesnivået er likt, innebærer ikke overføringer til andre land en omgåelse av EU-landets personvernregler.[42]

Samtidig skal direktivet fremme handel. Dersom et EU-land vedtar et forbud mot overføringer av personopplysninger til et annet EU-land som har et lavere beskyttelsesnivå, fungerer forbudet som en handelsrestriksjon på fri flyt av opplysninger som et kommersielt gode.[43] Personverndirektivet artikkel 1(2) fastslår derfor at medlemslandene verken skal «*restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1*».

2.2 Direktivets generelle krav til behandlingen av personopplysninger og geografiske og saklige virkeområde

Et vilkår for enhver behandling av personopplysninger, herunder overføringer til tredjeland, er at de generelle kravene til behandling av personopplysninger i direktivets kapittel II er oppfylt.[44] For det første stilles det krav til kvaliteten på behandlingen, jf. art. 6. Behandlingen skal være rettferdig, forsvarlig, relevant og i samsvar med spesifiserte, uttrykkelige og legitime formål. Personopplysningene skal videre være korrekte, oppdaterte og ikke lagres lengre enn nødvendig. For det andre må behandlingen begrunnes i minst ett av de spesifiserte grunnlagene i artikkel 7, eller i de strengere grunnlagene i artikkel 8 ved sensitive personopplysninger.

Personverndirektivets bestemmelser om saklig og geografisk virkeområdet begrenser dessuten rekkevidden av reglene for overføring av personopplysninger til tredjeland. Artikkel 4 bestemmer både direktivets geografiske rekkevidde og hvilket lands rett som kommer til anvendelse. Behandling av personopplysninger «*in the context of activities of an establishment of the controller*» i et EU-land, er underlagt det landets rett, jf. art. 4(1)(a). EU-landets lovgivning gjelder også dersom det følger av folkeretten, jf. (1)(b), eller dersom behandlingen forutsetter bruk av «*equipment, automated or otherwise*» som befinner seg i EU-landet, med mindre utstyret kun benyttes til forsendelse gjennom EU, jf. (1)(c). En aktør i et tredjeland som omfattes av et av disse alternativene, er en behandlingsansvarlig og ikke en dataimportør etter direktivets regler om overføringer av personopplysninger til tredjeland.[45] Avhandlingens tema omfatter dermed ikke disse situasjonene.

---

42 Kuner (2013) s. 108

43 Direktiv 95/46/EC fortalen (7), Büllesbach (2010) s. 31-32

44 Kuner (2013) s. 41

45 Dette fulgte også av Safe Harbor-beslutningen artikkel 2. Colonna (2014) drøfter grensedragningen

Direktivets saklige virkeområde dekker i utgangspunktet «*the processing of personal data wholly or partly by automatic means*» og visse former for manuell behandling, jf. personverndirektivet art. 3(1). Opplastning av informasjon på internett anses eksempelvis som automatisk behandling av personopplysninger.[46] Det gjelder unntak fra hovedregelen om direktivets saklige virkeområde blant annet for en aktivitet som «*falls outside the scope of Community law*» eller som er knyttet til *«public security, defence, State security […] and the activities of the State in areas of criminal law*», jf. direktivet art. 3(2) første strekpunkt. Medlemslandene kan også gjøre unntak fra bestemte regler i direktivet såfremt det er nødvendig av hensyn til for eksempel ytringsfrihet eller nasjonal sikkerhet, jf. art. 9 og 13.

2.3 Vilkår for overføring av personopplysninger til utlandet

2.3.1 Krav om tilstrekkelig beskyttelsesnivå

Utgangspunktet er at overføring av personopplysninger under behandling eller som skal behandles etter overføringen, kun er lovlig dersom landet opplysningene sendes til, «*ensures an adequate level of protection*», jf. personverndirektivet art. 25(1).[47] Videre i oppgaven omtales dette som tilstrekkelig beskyttelsesnivå eller forsvarlig behandling. Dersom kravet om tilstrekkelig beskyttelsesnivå ikke er oppfylt, er overføringer til tredjelandet i utgangspunktet forbudt.[48] Et spørsmål er derimot hva som er vurderingstemaet og terskelen for et tilstrekkelig beskyttelsesnivå.

«*[A]dequate level of protection*» er ikke legaldefinert. Det er uklart ut fra en alminnelig språklig forståelse av de ulike språkversjonene om beskyttelsesnivået må være fullgodt eller bare akseptabelt sammenlignet med EUs.[49] Dermed er det nærliggende å legge større vekt på reglens formål om å fremme personvern heller enn dens språklige utforming, se avsnitt 1.3.1. Büllesbach mener at minstekravet må være at tredjelandet har regler som ivaretar grunnkravene i personverndirektivet.[50] Det er imidlertid uklart hva som kreves utover dette. Direktivet artikkel 25(2) fastslår at vurderingen skal skje

> «*in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the*

---

46 Case C-101/01 Lindqvist (26), Büllesbach (2010) s. 42-43

47 Trolig må kravet til forsvarlig behandling av personopplysninger i personopplysningsloven § 29 (1) tolkes tilnærmet likt som direktivets standard, se Schartum (2011) s. 177

48 Direktiv 95/46/EC fortalen (57)

49 Se Generaladvokat Bot (2015) (142). Til sammenligning: Fransk: «assure un niveau de protection adéquat», tysk: «angemessenes Schutzniveau gewährleistet», dansk: «sikrer et tilstrækkeligt beskyttelsesniveau» og svensk: «säkerställer en adekvat skyddsnivå».

50 Büllesbach (2010) s. 114

data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country».

Ordlyden tyder på at det skal foretas en helhetsvurdering. Bestemmelsen inneholder ellers kun en ikke-uttømmende liste over retningslinjer for vurderingen.[51] Det er begrenset med andre rettskilder for hva vurderingstemaet og terskelen for tilstrekkelig beskyttelsesnivå er. Europakommisjonen og EU-landene tar gjerne utgangspunkt i kriteriene for forsvarlighetsvurderinger som Artikkel 29-gruppen har utarbeidet.[52] I Schrems-avgjørelsen presiserer imidlertid EU-domstolen vurderingstemaet og terskelen i forsvarlighetsvurderingen, se avsnitt 4.4.1.

2.3.2 Beslutninger om at et tredjeland sikrer et tilstrekkelig beskyttelsesnivå

EU-landene kan, for eksempel gjennom sine nasjonale datatilsyn, avgjøre om et tredjeland sikrer et tilstrekkelig beskyttelsesnivå for personopplysninger, jf. direktivet art. 25(1). Også Europakommisjonen kan treffe beslutninger om hvorvidt beskyttelsesnivået i et tredjeland er tilstrekkelig eller ikke, jf. henholdsvis direktivet art. 25(6) og 25(4). Hittil har Europakommisjonen besluttet at Andorra, Argentina, Canada, Færøyene, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Sveits og Uruguay – og frem til Schrems-avgjørelsen også visse selskaper i USA – sikrer et tilstrekkelig beskyttelsesnivå.[53]

Kommisjonen kan sette kriterier for beslutningen om tilstrekkelig beskyttelsesnivå, som at beslutningen kun gjelder for et bestemt tidsrom eller kun dersom tredjelandet gir individer rett til å klage til et selvstendig tilsyn.[54] Et spørsmål er imidlertid om Europakommisjonen har hjemmel til å beslutte at kun bestemte aktører i et tredjeland sikrer et tilstrekkelig beskyttelsesnivå, slik kommisjonen gjorde i Safe Harbor-beslutningen. Det virker å være en viss uenighet blant teoretikerne om direktivet åpner for slike løsninger. Schartum og Bygrave leser artikkel 25(6) som at kommisjonens beslutninger ikke må gjelde alle aktørene i et land.[55] Ifølge Blume kan derimot «*adequacy decisions […] only be made with respect to a country*».[56] Problemstillingen drøftes nærmere i avsnitt 4.5.3.

---

51 Büllesbach (2010) s. 114

52 Se A29WP (1998) s. 5-7. Arbeidsgruppens uttalelse har dermed i praksis fått stor innflytelse selv om den ikke er en bindende eller autoritativ kilde

53 Europakommisjonen (2016)b

54 Büllesbach (2010) s. 117

55 Schartum (2011) s. 180

56 Blume (2015) s. 35

EU-landene «*shall take the measures necessary*» for å følge kommisjonens beslutning, jf. direktivet art. 25(4) og (6).[57] Büllesbach tolker dette som at medlemslandene ikke kan forby overføringer til tredjeland som kommisjonen har besluttet at sikrer et tilstrekkelig beskyttelsesnivå.[58] Weber mener derimot formuleringen er for vag til å fastslå at bestemmelsen må forstås slik, og han poengterer at uklarheten svekker forutberegneligheten av å slutte seg til eksempelvis Safe Harbor-ordningen.[59] Spørsmålet drøftes videre i avsnitt 4.3.

2.3.3 Samtykke, lovhjemmel og nødvendighet

Selv om et tredjeland ikke sikrer en forsvarlig behandling av personopplysninger, kan opplysninger likevel overføres til tredjelandet i medhold av alternativene i personverndirektivet artikkel 26(1)(a) til (f). Disse unntakene er ikke et fokus for avhandlingen fordi de ikke var et tema i Schrems-avgjørelsen. Likevel er det hensiktsmessig å nevne dem for å fremheve at det finnes andre grunnlag for å overføre personopplysninger enn de som fremgår av Schrems-avgjørelsen. Unntakene i artikkel 26(1) bygger i hovedsak på tre typer grunnlag for å overføre personopplysninger: Samtykke fra den registrerte, lovhjemmel og nødvendighet.[60]

En fordel med å bruke et av disse unntakene ved overføringer til tredjeland er at overføringene kan skje til et hvilket som helst tredjeland.[61] Derimot må unntakene, særlig samtykke, tolkes strengt, og unntakene er ikke ment å brukes som eneste overføringsgrunnlag over lengre tid.[62] Formålet er å anvende unntakene dersom overføringen innebærer liten risiko for den registrerte eller dersom andre interesser veier tyngre enn den registrertes rett til personvern.[63]

2.3.4 Tilstrekkelige garantier: «Binding Corporate Rules» og «Standard Contractual Clauses»

Selv om et tredjeland ikke sikrer et tilstrekkelig beskyttelsesnivå, kan medlemslandene godkjenne en overføring såfremt den behandlingsansvarlige sørger for «*adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals*

---

57 Beslutningene gjelder i utgangspunktet også for Norge, jf. personopplysningsforskriften § 6-1(1)

58 Büllesbach (2010) s. 118

59 Weber (2013) s. 126-127

60 Schartum (2011) s. 180

61 Determann (2015) s. 49

62 A29WP (2005) s. 7,11

63 Büllesbach (2010) s. 120

and as regards the exercise of the corresponding rights», jf. direktivet art. 26(2). To overføringsmetoder sikrer vanligvis tilstrekkelige garantier.

Den ene er at den behandlingsansvarlige bruker EUs standardkontrakter («Standard Contractual Clauses», heretter «SCC»). SCC godkjennes av Europakommisjonen, jf. personverndirektivet art. 26(4).[64] Slike kontrakter kan i utgangspunktet gi grunnlag for overføringer til et hvilket som helst tredjeland.[65] Derimot må standardavtalen dekke hver eneste overføring av personopplysninger, ellers må det inngås en ny avtale, eller overføringen må ha et annet lovlig grunnlag.[66] I tillegg må den behandlingsansvarlige sørge for at også senere mottakere av personopplysningene forplikter seg til å følge avtalens krav.[67] For tiden finnes det tre typer SCC: Én for overføringer til databehandlere utenfor EU og to for overføringer til behandlingsansvarlige utenfor EU.[68]

Den andre overføringsmetoden er bindende konsernregler («Binding Corporate Rules» og «Binding Corporate Rules for Processors», heretter «BCR»). Personverndirektivet nevner ikke eksplisitt BCR, men det er innfortolket som en av flere mulige «*adequate safeguards*» etter artikkel 26(2).[69] BCR åpner for at selskaper i og utenfor EU kan overføre personopplysninger seg i mellom, såfremt de er med i samme konsern og hele konsernet følger samme regler for behandlingen av personopplysninger.[70] Det er ingen standardkrav til utformingen av BCR, men Artikkel 29-arbeidsgruppen har gitt rådgivende uttalelser om hva som vanligvis kreves.

---

64 Disse beslutningene er i utgangspunktet bindende også for Norge, jf. personopplysningsforskriften § 6-1(1)

65 Determann (2015) s. 59-60

66 Tønseth (2016) s. 127

67 Determann (2015) s. 53

68 Europakommisjonen (2015), Tønseth (2016) s. 127,129

69 Büllesbach (2010) s. 122

70 Tønseth (2016) s. 130

3 U.S.-EU Safe Harbor

I 2000 inngikk Europakommisjonen og *US Department of Commerce* («DoC») Safe Harbor-avtalen.[71] På bakgrunn av avtalen traff Europakommisjonen Safe Harbor-beslutningen.[72] Beslutningen gikk ut på at de amerikanske kommersielle selskapene som underla seg personvernkravene i avtalen, sikret et tilstrekkelig beskyttelsesnivå for personopplysninger etter personverndirektivet artikkel 25 (6). Beslutningen ble vedtatt også for resten av EØS-landene.[73]

3.1 Bakgrunn og forhandlingene

Under arbeidet med personverndirektivet ble det klart at USA ikke sikret et tilstrekkelig beskyttelsesnivå for personopplysninger etter direktivet artikkel 25. USA har en fragmentert og sektorspesifikk personvernlovgivning, mens personverndirektivet har en generell og helhetlig regulering av personopplysninger.[74] I tillegg har ikke USA et uavhengig personverntilsyn.[75] Det virket ikke realistisk for mange amerikanske aktører å basere seg utelukkende på alternative overføringsgrunnlag etter direktivet artikkel 26. Dersom EU stoppet overføringer av personopplysninger til USA, kunne imidlertid tapet for transatlantisk handel bli på opptil 120 milliarder dollar.[76]

Det kan spørres hvorfor USA ikke unngikk dilemmaet ved å endre lovgivningen sin for å imøtekomme EUs krav til personvern. USA og EU har imidlertid grunnleggende ulike tilnærminger til hvor mye staten griper inn gjennom lovregulering. Særlig ville amerikanske myndigheter regulere det voksende markedet knyttet til internett minst mulig, og det var liten politisk vilje i den amerikanske kongressen til å endre personvernlovgivningen.[77] Samtidig ble personverndirektivet oppfattet som ekstraterritoriell jurisdiksjon fra EUs side.[78] Det oppstod dermed en situasjon hvor verken EU eller USA kunne akseptere motpartens regulering av personvern, men hvor det var vesentlig for transatlantisk handel at de kom til enighet.

---

71 Safe Harbor (2000), Export.gov (2016)

72 Decision 2000/520/EC, se art. 1

73 EØS-komiteen (2000) art. 1

74 Heisenberg (2005) s. 32, Reidenberg (2001-2002) s. 725,739

75 Colonna (2014) s. 204

76 Heisenberg (2005) s. 84

77 Heisenberg (2005) s. 76,83

78 Shaffer (2000) s. 55

Eksisterende internasjonale regelverk kunne ikke løse konflikten. Personvern var unntatt fra WTO-regimet, og WTOs mekanismer for konfliktløsning var dermed ikke aktuelle.[79] Både EU og USA hadde sluttet seg til OECDs personvernretningslinjer fra 1980, men disse var ikke rettslig bindende.[80] Representanter for Europakommisjonen og DoC startet derfor forhandlinger om et bilateralt personvernrammeverk som skulle gi grunnlag for en forsvarlighetsvurdering fra kommisjonen.

Den amerikanske siden hadde imidlertid begrenset med forhandlingsrom. Formålet var ikke å gjennomføre personverndirektivet eller endre på den eksisterende personvernlovgivningen i USA, men kun å bli enige om en frivillig ordning med selvregulering for amerikanske selskaper.[81] Da unngikk man å involvere kongressen, og ordningen samsvarte med interessene til kommersielle aktører med innflytelse over DoC.[82]

En vesentlig grunn til at partene kom til enighet, var at de tolket artikkel 25 i personverndirektivet som at *selskaper*, og ikke bare tredjelandet som sådan, kunne sikre et tilstrekkelig beskyttelsesnivå for personopplysninger.[83] Amerikanerne foreslo derfor en ordning med selvregulering der amerikanske selskaper som fulgte et sett med personvernprinsipper, skulle anses å gi et tilstrekkelig beskyttelsesnivå – en trygg havn – for behandling av personopplysninger i USA.[84] I begynnelsen var europeerne skeptiske til at selvregulering ville være effektivt, og de fryktet at ordningen ville gi et lavere beskyttelsesnivå enn direktivet krevde, men over tid ble de overbevist.[85] Partene ble derfor enige om Safe Harbor-avtalen. På bakgrunn av avtalen traff kommisjonen Safe Harbor-beslutningen i juli 2000.

3.2 Innholdet i Safe Harbor-beslutningen

Safe Harbor-beslutningen inneholdt en fortale, seks bestemmelser og syv vedlegg. Schrems-avgjørelsen gjaldt beslutningens artikkel 1 og 3 og de tilhørende vedleggene. Utgangspunktet var at Safe Harbor-prinsippene og en «FAQ» («Frequently Asked Questions») tolket i lys av beslutningens vedlegg III-VI sikret et tilstrekkelig beskyttelsesnivå for personopplysninger som overføres fra EU til amerikanske selskaper, jf. Safe Harbor-beslutningen art. 1(1). For å få motta slike personopplysninger, måtte amerikanske selskaper oppfylle to tilleggsvilkår. Det

79 Heisenberg (2005) s. 3

80 OECDs personvernretningslinjer Explanatory Memorandum (20)

81 Heisenberg (2005) s. 82-83

82 Heisenberg (2005) s. 81

83 Heisenberg (2005) s. 88

84 Heisenberg (2005) s. 88

85 Heisenberg (2005) s. 88

kan påpekes at det ble presumert at selskaper oppfylte de to vilkårene dersom de gav DoC en egenerklæring om at de fulgte Safe Harbor-regelverket, jf. art. 1(3).

For det første måtte selskapet som mottok personopplysninger, «*unambiguously and publicly disclose*» at det skulle følge Safe Harbor-prinsippene, jf. art. 1(2)(a). Det var frivillig å slutte seg til ordningen, men den var bindende for de selskapene som gjorde det. De syv personvernprinsippene ble utformet av DoC og stilte krav om varsling («notice»), bestemmelsesrett («choice»), videre overføringer («onward transfer»), sikkerhet («security»), opplysningskvalitet («data integrity»), tilgang (access») og håndheving («enforcement»), jf. Safe Harbor-beslutningen vedlegg I. Safe Harbor-beslutningens FAQ inneholdt spørsmål og svar knyttet til mer spesifikke deler av gjennomføringen, jf. Safe Harbor-beslutningen vedlegg II.

For det andre måtte selskapet være underlagt myndigheten til enten *Department of Transportation* («DoT») eller det amerikanske handelstilsynet, *Federal Trade Commission* («FTC»), jf. Safe Harbor-beslutningen art. 1(2)(b) jf. vedlegg VII. FTC hadde derimot ikke myndighet over en rekke aktører som behandler personopplysninger, som banker eller kollektive formidlere av telekommunikasjon, jf. Safe Harbor-beslutningen vedlegg VII. Dersom individer klaget på de amerikanske selskapenes etterlevelse, skulle klagen i utgangspunktet behandles ved alternative tvisteløsningsmekanismer.[86] Kun dersom tvisten ikke ble løst på denne måten, skulle FTC eller DoT involveres.[87] Myndighetene kunne ilegge selskapene bøter eller utestenge selskapet fra Safe Harbor-ordningen.[88] EUs nasjonale tilsynsmyndigheter kunne dessuten i bestemte situasjoner suspendere overføringer etter Safe Harbor-ordningen, jf. Safe Harbor-beslutningen artikkel 3.

3.3 Kritikk av Safe Harbor-beslutningen

Safe Harbor-ordningen ble ansett som en suksess av mange; den forente USA og EUs ulike tilnærminger til personvern og kunne i tillegg fungere som en mal for løsning av andre mulige transatlantiske konflikter.[89] Til tross for dette ble både Safe Harbor-avtalen og Safe Harbor-beslutningen utsatt for kritikk. Av hensyn til ordgrensen behandles kun den delen av kritikken som var mest sentral for Schrems-avgjørelsen: Hvorfor Safe Harbor-beslutningen ikke oppfylte kravene i personverndirektivet artikkel 25.

---

86 Heisenberg (2005) s. 74

87 Colonna (2014) s. 206

88 Heisenberg (2005) s. 74

89 Heisenberg (2005) s. 73

Flere teoretikere kritiserte innholdet i Safe Harbor-prinsippene. Schartum og Bygrave mente Safe Harbor-prinsippene var en innholdsmessig svakere utgave av grunnprinsippene i personverndirektivet.[90] Weber argumenterte for at prinsippene var så vage at de kunne omgås ved tolkning.[91] Artikkel 29-arbeidsgruppen stilte dessuten spørsmål ved lovligheten av unntakene fra personvernprinsippene i Safe Harbor-beslutningen, og arbeidsgruppen krevde at Safe Harbor-prinsippene «*should only be limited to the extent* ***necessary*** *to comply with conflicting obligations […]*» (min utheving).[92]

Videre kritiserte ulike aktører Safe Harbor-beslutningens håndhevingsmekanismer. Artikkel 29-arbeidsgruppen mente at håndhevingsmekanismene var svake, blant annet fordi den registrerte ikke kunne klage til et uavhengig kontrollorgan.[93] Europaparlamentet gav også uttrykk for at det var uklart om Safe Harbor-ordningen gav den registrerte mulighet til å kreve kompensasjon for brudd på Safe Harbor-prinsippene.[94] Reidenberg og Weber påpekte videre at FTC kun hadde hjemmel til å gripe inn dersom bruddet på Safe Harbor-prinsippene var «*unfair or deceptive acts or practices*».[95]

Europaparlamentet problematiserte dessuten om kommisjonen hadde kompetanse til å fremforhandle Safe Harbor-ordningen uten Parlamentets godkjennelse.[96] Reidenberg var også inne på Safe Harbor-beslutningens formelle gyldighet; «*in the context of Safe Harbor negotiations, the European Commission never made a formal finding [of adequate level of protection]*».[97]

Safe Harbor-ordningen ble ikke bare kritisert for hvordan den fremstod på papiret, men også for hvordan den ble praktisert. En ofte sitert undersøkelse gjort av Connolly i 2008 tydet på at det var mangler ved den praktiske gjennomføringen av Safe Harbor-ordningen. Blant annet var det bare et mindretall av selskapene som var tilsluttet ordningen, som møtte selv grunnleggende krav etter ordningen, og flere selskaper hevdet urettmessig på hjemmesidene sine at de var medlemmer av Safe Harbor-ordninger.[98]

---

90 Schartum (2011) s. 93

91 Weber (2013) s. 126-127

92 A29WP (2000) s. 4-5

93 A29WP (2000) s. 6-7

94 Resolution A5-0177/2000 s. 8

95 Reidenberg (2001-2002) s. 741, Weber (2013) s. 126-127

96 Resolution A5-0177/2000 s. 9

97 Reidenberg (2001-2002) s. 742

98 Connolly (2008) s. 4-5. Se også Schartum (2011) s. 93, Weber (2013) s. 127

Snowden-avsløringene ledet også til at Europakommisjonen kom med to uttalelser om gjennomføringen av Safe Harbor-ordningen i 2013.[99] Uttalelsene gjenspeiler Connollys funn; kommisjonen påpekte blant annet mangel på gjennomsiktighet i etterlevelsen av ordningen og at mange egensertifiserte selskaper ikke fulgte Safe Harbor-prinsippene, som medførte både konkurransefortrinn for disse selskapene og brudd på grunnleggende rettigheter.[100]

kommisjonen krevde at ordningen måtte praktiseres strengere, og at det måtte sørges for tilgjengelige og rimelige tvisteløsningsmekanismer og mer effektiv og systematisk etterlevelse av prinsippene.[101] Kommisjonen la for øvrig til grunn at det kunne gjøres unntaket fra personvernet av hensyn til nasjonal sikkerhet «*only to an extent that is **strictly necessary** and proportionate*» (min utheving).[102]

[99] COM(2013) 846, COM(2013) 847, se COM(2013) s. 3

[100] COM(2013) 846 s. 6

[101] COM(2013) 846 s. 7

[102] COM(2013) 846 s. 8

4 Schrems-avgjørelsen

4.1 Sakens bakgrunn og EU-domstolens konklusjoner

Østerrikske Maximillian Schrems opprettet en bruker i det sosiale nettverket Facebook i 2008.[103] For å opprette en slik bruker må innbyggere i EU inngå avtale med det irske datterselskapet *Facebook Ireland*, men alle eller et utvalg av opplysningene som samles inn av datterselskapet, overføres og behandles i USA av morselskapet *Facebook, inc*.[104] I lys av Snowden-avsløringene klaget Schrems til den irske datatilsynsmyndigheten («*Data Protection Commissioner*») og krevde at Facebook Ireland måtte forbys å anvende Safe Harbor-ordningen for å overføre personopplysningene hans til USA.[105]

Schrems mente Snowden-avsløringene viste at USA ikke sikret forsvarlig behandling av personopplysninger. Det irske tilsynet mente det ikke var forpliktet til å undersøke saken nærmere. Det var ikke bevis for at amerikanske etterretningstjenester hadde Schrems' opplysninger, og dessuten mente tilsynet at det ikke hadde kompetanse til å ta stilling til beskyttelsesnivået i USA når kommisjonen i Safe Harbor-beslutningen allerede hadde gjort det.[106] Schrems tok saken inn for den irske *High Court*. Den irske domstolen vurderte at saken hadde EU-rettslige implikasjoner og besluttet derfor å utsette saken og sendte følgende spørsmål til EU-domstolen for en forhåndsavgjørelse:[107]

> « *(1) Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in [Decision 2000/520] having regard to Article 7, Article 8 and Article 47 of [the Charter], the provisions of Article 25(6) of Directive [95/46] notwithstanding?*

[103] Schrems-avgjørelsen (26)

[104] Schrems-avgjørelsen (27)

[105] Schrems-avgjørelsen (28)

[106] Schrems-avgjørelsen (29)

[107] Schrems-avgjørelsen (35)

(2) Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission decision was first published?»[108]

EU-domstolen konkluderte at en beslutning fra kommisjonen om et tredjelands beskyttelsesnivå ikke fratar den nasjonale tilsynsmyndigheten dens kompetanse til å behandle klager om beskyttelsesnivået i tredjelandet.[109] Videre tok EU-domstolen stilling til hvorvidt Safe Harbor-beslutningen var gyldig eller ikke. Domstolen konkluderte at beslutningen i sin helhet var ugyldig.[110]

Formålet med de følgende delkapitlene er å analysere og reflektere rundt rettssetningene som ledet til disse konklusjonene. I tillegg drøfter jeg hvilke tolkningsspørsmål avgjørelsen ikke besvarer. Avhandlingen skiller ikke mellom domstolens *ratio decidendi* og *obiter dicta* av grunnene som fremgår av avsnitt 1.3.1.

4.2 Utgangspunktet for vurderingene: Personvern som grunnleggende rettighet

Respekt for privat- og familieliv, hjem og korrespondanse og beskyttelse av personopplysninger er grunnleggende rettigheter i EU i medhold av henholdsvis EU-charteret artikkel 7 og 8.[111] I Schrems-avgjørelsen slo EU-domstolen fast at i den grad personverndirektivet gjennomfører EU-charteret art 7 og 8, må direktivet tolkes i lys av charteret.[112]

Hva innebærer det at direktivet må tolkes i lys av de grunnleggende rettighetene i charteret? Personvern har vært en grunnleggende rettighet siden direktivet ble vedtatt, så det var neppe det domstolen mente. Man kan derimot forstå domstolens uttalelse som at direktivets bestemmelser som gjennomfører charteret artikkel 7 og 8, må tolkes i tråd med rettspraksis om charteret og får samme rang som charteret. Direktivet er i utgangspunktet sekundærrett, mens charteret er sidestilt med EU-traktatene.[113]

---

108 Schrems-avgjørelsen (36)

109 Schrems-avgjørelsen (66)

110 Schrems-avgjørelsen (106)

111 Medlemslandene i EU er dessuten tilsluttet EMK, se Sejersted (2011) s. 58. EMK art. 8 sikrer også rett til respekt for privat- og familieliv, hjem og korrespondanse

112 Schrems-avgjørelsen (38)

113 Europakommisjonen (2016)a

Er det derimot gitt at reglene om overføring av personopplysninger til tredjeland gjennomfører charteret artikkel 7 og 8? EU-domstolen synes uten videre å forutsette at det er tilfellet. Derimot kan man argumentere at siden reglene om overføringer av personopplysninger er inntatt i direktivets kapittel IV, har de en subsidiær funksjon sammenlignet med grunnprinsippene i personverndirektivets kapittel II, og reglene er derfor ikke i kjernen av charteret artikkel 7 og 8.[114]

Argumentet kan kritiseres for å være formalistisk. Beskyttelsen grunnprinsippene gir, kan omgås dersom direktivet ikke også beskytter behandling av personopplysningene uavhengig av hvor opplysningene befinner seg. Personverndirektivets formål om å unngå omgåelse av personvernet blir dermed best ivaretatt om reglene i direktivet kapittel IV anses å gjennomføre charteret artikkel 7 og 8.

Videre kan man spørre om det har noen betydning at personverndirektivet, som ble vedtatt i 1995, og Safe Harbor-beslutningen, som ble truffet i 2000, er eldre enn EU-charteret. Charteret ble vedtatt i 2000 og ble bindende først i 2009. For å begrunne at direktivet skal tolkes i lys av charteret, viser EU-domstolen til tre avgjørelser. Alle tre avgjørelsene er nyere enn direktivet og Safe Harbor-beslutningen; *Rechnungshof*[115] er avsagt i 2003, mens *Google Spain*[116] og *Ryneš*[117] er avsagt i 2014.

På den ene siden er det neppe tvil om at det er gjeldende rett at direktivet må tolkes i lys av charteret, selv om charteret er nyere. På den andre siden innebærer det å tolke direktivet i lys av charteret en form for tilbakevirkning. Man kan argumentere rettspolitisk for at det fører til en ineffektiv praktisering av reglene fordi det kan skape usikkerhet for aktørene som forsøker å innrette seg etter Europakommisjonens beslutninger. Dersom direktivet skal gi en effektiv beskyttelse av personopplysninger, må imidlertid domstolen tolke direktivet dynamisk og i samsvar med rettsutviklingen.

EU-domstolen fastslo videre at direktivet har til formål ikke bare å sikre en *effektiv og fullstendig beskyttelse* av de grunnleggende personvernrettighetene, men også at de grunnleggende rettighetene gis et *høyt beskyttelsesnivå*.[118] Som drøftelsene nedenfor viser, er kravet til effektiv beskyttelse og høyt beskyttelsesnivå en rød tråd i dommens premisser, og kravet

---

114 Kuner (2013) s. 62-63 med henvisning til case C-101/01 Lindqvist

115 Case C-465/00

116 Case C-131/12

117 Case C-212/13

118 Schrems-avgjørelsen (39)

medfører en tolkning av reglene om overføring av personopplysninger der hensynet til retten til personvern tillegges stor vekt.

4.3 Avklaring av forholdet mellom kommisjonens og tilsynsmyndighetenes kompetanse

4.3.1 Tilsynsmyndighetene har så vid kompetanse som er nødvendig for å utføre deres oppgaver

Som diskutert i avsnitt 2.3.2 kan det problematiseres hvordan man skal harmonisere kommisjonens og de nasjonale tilsynenes kompetanser etter personverndirektivet. EU-domstolen uttalte at uavhengige, offentlige tilsyn er nødvendige for en effektiv og pålitelig håndheving av direktivet og følgelig også for en forsvarlig beskyttelse av personopplysninger.[119] For å sikre en effektiv håndheving må tilsynene ha kompetanse til å foreta ulike handlinger, som å gjøre undersøkelser og ta rettslige skritt.[120] En av tilsynenes oppgaver er å påse at overføringer til tredjeland er i samsvar med direktivet, og derfor måtte de ha kompetanse til å undersøke om overføring fra deres land til et tredjeland er i samsvar med direktivet.[121]

Domstolens uttalelser kan forstås som at tilsynsmyndighetenes kompetanse må tolkes så vidt at tilsynene kan oppfylle sine lovpålagte oppgaver, uten at man kan fastlegge én gang for alle hvilke kompetanser de har. Man kan argumentere rettspolitisk for at en slik dynamisk, formålsrettet tolkning leder til usikkerhet, både for tilsynene og de som er underlagt deres myndighet, om hva som til enhver tid er tilsynenes kompetanse. Når domstolen gir en så vag angivelse av tilsynenes myndighet, bidrar det derfor ikke nødvendigvis til en effektiv håndheving av reglene.

Man kan også spørre om datatilsynenes kontroll med overføringer til tredjeland innebærer at de utøver ekstraterritorial jurisdiksjon over tredjelandets aktører. EU-domstolen fastslo at tilsynene kun utøver myndighet over behandlingen som finner sted på europeisk territorium: Å overføre opplysninger er dekket av begrepet behandling av personopplysninger, og i og med at overføringen skjer fra et EU-land, finner behandlingen sted i EU-landet.[122]

Kuner mener domstolens resonnement illustrerer at det er meningsløst å skille mellom ekstraterritoriell og territoriell jurisdiksjon når det kommer til internasjonale overføringer av per-

---

[119] Schrems-avgjørelsen (40)-(42) med henvisning til personverndirektivet art. 28(1), EU-charteret art. 8(3) og TEUV art. 16(2)

[120] Schrems-avgjørelsen (43)

[121] Schrems-avgjørelsen (46)-(47)

[122] Schrems-avgjørelsen (44)-(45)

sonopplysninger.[123] På den ene siden kan man argumentere for at EU-domstolens resonnement stemmer formelt sett; personverndirektivet artikkel 25 regulerer overføringer fra en behandlingsansvarlig som enten er etablert i et EU-land eller som bruker utstyr i et EU-land, se avsnitt 2.2, og dermed skjer overføringen fra europeisk territorium. På den andre siden kan man kritisere domstolens tolkning for ikke å ta hensyn reglenes realpolitiske aspekter. En overføring av personopplysninger har både en avsender og en mottaker, og reelt sett vil en regulering av dataeksportøren også påvirke dataimportøren.

4.3.2 Forholdet mellom de nasjonale tilsynsmyndighetenes, kommisjonens og EU-domstolens oppgaver

Både kommisjonen og medlemslandene kan vurdere om tredjeland sikrer et tilstrekkelig beskyttelsesnivå, men Europakommisjonens beslutninger er bindende for alle medlemslandenes nasjonale organer, herunder datatilsynene, jf. direktivet art. 25(4) og (6) og TEUV art. 288(4).[124] Tilsynene skal kontrollere inngrep i individers grunnleggende rettigheter ved en behandling av personopplysninger, herunder ved overføringer til tredjeland.[125] Er tilsynene avskåret fra å kontrollere overføringer dersom kommisjonen har besluttet at et tredjeland sikrer et tilstrekkelig beskyttelsesnivå etter artikkel 25(6)?

Domstolen konkluderte at det ikke var tilfellet. Et individ som mener at et tredjeland ikke sikrer en forsvarlig beskyttelse av individets personopplysninger – selv om kommisjonen har besluttet at tredjelandet har et tilstrekkelig beskyttelsesnivå – kan henvende seg til sitt nasjonale tilsyn, som må undersøke klagen «*with all due diligence*».[126] Domstolen utdyper ikke hva kravet til «*due diligence*» innebærer. I lys av at personopplysninger skal gis en effektiv beskyttelse og et høyt beskyttelsesnivå, se avsnitt 4.2, kan man anta at tilsynene må behandle klagen grundig og forsvarlig.

Dersom tilsynet ikke tar klagen til følge, kan individet i medhold av EU-charteret artikkel 47 ta saken til sin nasjonale domstol, som kan be EU-domstolen om en forhåndsavgjørelse om gyldigheten av kommisjonens beslutning.[127] Dersom tilsynet tar klagen til følge, har tilsynet kompetanse etter direktivet artikkel 28(3) til å reise sak, og den nasjonale domstolen kan be om en forhåndsavgjørelse fra EU-domstolen.[128]

---

123 Kuner (2016) s. 10

124 Schrems-avgjørelsen (50)-(51)

125 Schrems-avgjørelsen (53)-(60)

126 Schrems-avgjørelsen (63)

127 Schrems-avgjørelsen (64)

128 Schrems-avgjørelsen (65)

Rettspolitisk kan man imidlertid kritisere rettssetningen om at tilsynene må behandle klager på beskyttelsesnivået i tredjeland for å lede til en ineffektiv praktisering av direktivet. Når Europakommisjonen tar stilling til beskyttelsesnivået i et tredjeland, har de interne retningslinjer for hvordan vurderingen skal foretas, de bruker gjerne lang tid og betydelige ressurser på å komme til en beslutning og de kan engasjere personverneksperter som uttaler seg om tredjelandets beskyttelsesnivå.[129] De nasjonale tilsynsmyndighetene har trolig mer begrensede ressurser, og de har ikke nødvendigvis kunnskaper til å analysere personvernreguleringen i andre land.[130]

Er det derfor realistisk å forvente at tilsynsmyndighetene skal kunne kontrollere kommisjonens forsvarlighetsvurderinger? Dersom tilsynene skal foreta en forsvarlig kontroll av kommisjonens beslutninger, kan det gå med mye tid og ressurser. Det kan i neste omgang gå utover tilsynenes andre oppgaver. I så fall kan Schrems-avgjørelsen i realiteten svekke tilsynsmyndighetenes kontroll. Alternativt kan tilsynet bruke mindre tid og ressurser, men da kan det kontrollen bli for overfladisk til å ha en reell hensikt.

En fordel med at kommisjonens forsvarlighetsvurderinger ikke blir overprøvd av de nasjonale tilsynene, er at det kan fremme harmonisering av rettstilstanden i EU. Det er ikke gitt at datatilsynene i de ulike EU-landene ville komme til samme konklusjoner om hvorvidt et tredjeland sikrer et tilstrekkelig beskyttelsesnivå eller ikke, og dette kan medføre en usikker rettstilstand.[131] EU-domstolen synes ikke å ha vurdert disse realpolitiske hensynene i Schrems-avgjørelsen.

4.4 Generell tolkning av personverndirektivet artikkel 25(6)

4.4.1 Tilstrekkelig beskyttelsesnivå: Vurderingstema og terskel

Før domstolen vurderte om Safe Harbor-beslutningen innebar at amerikanske selskaper sikret et tilstrekkelig beskyttelsesnivå etter personverndirektivet artikkel 25(6), tolket domstolen hva som ligger i kravet til tilstrekkelig beskyttelsesnivå. Domstolen tok først stilling til terskelen for at et tredjeland gir et tilstrekkelig beskyttelsesnivå for behandling av personopplysninger. EU-domstolen sluttet på bakgrunn av EU-charteret artikkel 8(1) at det måtte gjelde et sterkt personvern ved overføringer til utlandet.[132] Derfor er det naturlig å anta at terskelen for et

[129] Kuner (2016) s. 18

[130] Kuner (2016) s. 11

[131] Kuner (2016) s. 12

[132] Schrems-avgjørelsen (72)

tilstrekkelig beskyttelsesnivå er høy og at det ikke er godt nok at tredjelandet sikrer et akseptabelt beskyttelsesnivå, se avsnitt 2.3.1.

Man kan spørre om det innebærer at «*adequate [level of protection]»* er en like streng standard som «*equivalent protection*» i Europarådets personvernkonvensjon artikkel 12(3)(a). Bygrave tolker begrepet «*equivalent*» i personvernkonvensjonen som at det ikke kreves identisk beskyttelse i senderlandet og mottakerlandet, men at «*equivalent*» likevel er et strengere og mindre fleksibelt begrep enn «*adequate*».[133]

EU-domstolen kom med lignende betraktninger. Begrepet «*adequate*» innebærer ikke at tredjelandet må ha et identisk beskyttelsesnivå som EU, men beskyttelsesnivået må være «*essentially equivalent*».[134] EU-domstolen synes dermed å bekrefte at det er en sammenheng mellom begrepene «*adequate*» og «*equivalent*», og at førstnevnte er en noe lavere terskel enn sistnevnte. Imidlertid er det ikke dermed gitt at begrepet «*equivalent*» skal forstås på samme måte ved tolkningen av Europarådets personvernkonvensjon og personverndirektivet.

Videre gav EU-domstolen en viss veiledning for vurderingstemaet. Det sentrale er ikke hvilke virkemidler tredjelandet tar i bruk for å nå «*essentially equivalent*» beskyttelsesnivå, men at resultatet blir en effektiv beskyttelse på nivå med EUs.[135] Derimot er det fremdeles uklart hvor kvalitativt ulikt tredjelandets regulering av behandlingen av personopplysninger kan være fra EU-retten før tredjelandet ikke har et tilstrekkelig beskyttelsesnivå. Dessuten kan det påpekes at EU-retten endres, og beskyttelsesnivået i EU derfor ikke er konstant.

En annen problemstilling er hva som skal vurderes som å oppfylle et tilstrekkelig beskyttelsesnivå. Domstolen fastslo at det ikke var tilstrekkelig at tredjelandets rettslige system og landets internasjonale forpliktelser *på papiret* sikrer tilnærmet likt beskyttelsesnivå; personvernet måtte også være effektivt *i praksis*.[136] I tillegg påla domstolen kommisjonen å undersøke med jevne mellomrom eller ved behov om tredjelandet fremdeles faktisk og rettslig sikrer et tilstrekkelig beskyttelsesnivå.[137]

---

133 Bygrave (2002) s. 225 med videre henvisninger til flere teoretikere

134 Schrems-avgjørelsen (73). I den franske versjonen av avgjørelsen er uttrykket «substantiellement équivalent», i den tyske «tatsächlich […] gleichwertig», i den danske «i det væsentlige svarer til» og i den svenske «väsentligen likvärdig». Alle versjonene virker å tyde på at nivået må være nært opp mot tilsvarende EUs, uten at det er klart hvor stort spillerommet er

135 Schrems-avgjørelsen (74)

136 Schrems-avgjørelsen (74)

137 Schrems-avgjørelsen (76)

Rettssetningene reflekterer kravet til effektiv beskyttelse og høyt beskyttelsesnivå, se avsnitt 4.2. Samtidig kan uttalelsene ses på som en kritikk av Europakommisjonen: Snowden-avsløringene ledet til at Europakommisjonen vurderte Safe Harbor-ordningen i 2013, se avsnitt 3.3, men før det hadde ikke kommisjonen vurdert ordningen siden 2004.[138]

4.4.2 Domstolens grunnlag for prøvingen av kommisjonens beslutninger

Den irske domstolen spurte om det kunne tas hensyn til forhold som har skjedd etter at kommisjonen traff en forsvarlighetsbeslutning ved vurdereringen av beslutningens gyldighet. EU-domstolen fastslo at den – i alle fall – kunne ta hensyn til etterfølgende forhold ved vurdering av gyldigheten av forsvarlighetsvurderinger.[139] Domstolen bygget på generaladvokatens resonnement om at

> «*[o]therwise […] a number of years after an adequacy decision has been adopted, the assessment of validity that the Court must carry out cannot take into account events that have occurred subsequently, even though there is no limit on the period within which a reference for a preliminary ruling on validity may be made and it may be prompted specifically by subsequent facts that reveal the deficiencies of the act in question*».[140]

Generaladvokaten synes ikke å bygge sin vurdering på andre rettskilder enn reelle hensyn. Dette kan virke som et spinkelt rettskildegrunnlag. Derimot står formålsbetraktninger sterkt i EU-retten, og man kan argumentere for at denne tolkningen er nødvendig for at personverndirektivet artikkel 25(6) skal sikre en effektiv og sterk beskyttelse av personvern.

Hvor inngående prøver domstolen kommisjonens vurderinger av om et tredjeland sikrer et tilstrekkelig beskyttelsesnivå? EU-domstolen konstaterte at beskyttelse av personopplysninger er sentralt for personvern og at overføringer til et tredjeland uten tilstrekkelig beskyttelsesnivå kan krenke et høyt antall menneskers grunnleggende rettigheter, og derfor at

> «*the Commission's discretion as to the adequacy of the level of protection ensured by a third country is reduced, with the result that review of the requirements stemming from Article 25 of Directive 95/46, read in the light of the Charter, should be strict*».[141]

---

138 Loideain (2016) s. 10-11

139 Schrems-avgjørelsen (77)

140 Generaladvokat Bot (2015) (134)-(135)

141 Schrems-avgjørelsen (78)

Hva innebærer det for forsvarlighetsvurderingen at kommisjonens skjønn er begrenset? Domstolen bygget rettssetningen på en analogi til *Digital Rights Ireland*,[142] hvor grunnlaget for å begrense kommisjonens skjønn var at

> «*the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives*».[143]

Man kan tolke uttalelsen som at kommisjonen dermed har lite spillerom i forsvarlighetsvurderingen til å vektlegge for eksempel realpolitiske hensyn, som hvor viktig en forsvarlighetsvurdering er for handelen mellom EU og tredjelandet. Også her kommer det frem at reglene tolkes strengt til fordel for beskyttelse av personopplysninger fordi personvern er en grunnleggende rettighet.

4.5 Safe Harbor-beslutningen erklæres ugyldig

Den irske rettens spørsmål gjaldt ikke eksplisitt gyldigheten av Safe Harbor-beslutningen. Likevel drøftet EU-domstolen beslutningens gyldighet. Man kan problematisere om EU-domstolen dermed gikk utover spørsmålet fra den nasjonale domstolen. Slik den irske rettens spørsmål er formulert, kan det virke som retten ønsket en avklaring av tilsynsmyndighetens kompetanse etter personverndirektivet, og at spørsmålene derfor kunne løses uavhengig av det materielle innholdet i Safe Harbor-beslutningen.

EU-domstolen fastslo imidlertid at Safe Harbor-beslutningens gyldighet var et underliggende spørsmål for den irske domstolen.[144] Uavhengig av om EU-domstolen gikk utenfor spørsmålet fra den irske domstolen, kan man derfor argumentere rettspolitisk for at det er prosessparende at domstolen avgjorde den underliggende konflikten i saken med en gang.

EU-domstolen understreket for øvrig at kun den, og ikke nasjonale domstoler eller nasjonale tilsyn, hadde kompetanse til å erklære EU-rettsakter for ugyldige.[145] Slutningen har gode grunner for seg. Dersom de nasjonale domstolene kunne erklære EU-rettsaktene ugyldige,

---

142 Case C-293/12 (47)-(48), med videre henvisning til en avgjørelse fra EMD om EMK art. 8

143 Case C-293/12 (46), se også avsnitt 4.5.2

144 Schrems-avgjørelsen (67)

145 Schrems-avgjørelsen (61)

kunne en og samme EU-rettsakt vært gyldig i ett EU-land, men ugyldig i et annet. Hensynet til ensartet anvendelse av EU-retten underbygger derfor EU-domstolens konklusjon.

EU-domstolen vurderte for øvrig kun gyldigheten av Europakommisjonens Safe Harbor-beslutning. Domstolen tok ikke stilling til lovligheten av Safe Harbor-avtalen mellom kommisjonen og DoC eller innholdet i amerikansk personvernregelverk.[146] I de følgende avsnittene drøftes manglene domstolen finner ved Safe Harbor-beslutningen som førte til at den ble erklært ugyldig, og om disse manglene var de samme som beslutningen ble kritisert for før Schrems-avgjørelsen. Avhandlingen drøfter fire overordnede krav som domstolen vurderer beslutningen ut fra: Effektiv håndheving og prosessuelle rettigheter, vilkår for inngrep i personvernet, formell konstatering av tilstrekkelig beskyttelsesnivå og hjemmel for innskrenkninger av de nasjonale tilsynsmyndighetenes kompetanse.

4.5.1 Krav til effektiv håndheving og prosessuelle rettigheter

Som drøftet i avsnitt 4.4.1 innebærer kravet til tilstrekkelig beskyttelsesnivå i direktivet artikkel 25 at tredjelandets rettslige system og landets internasjonale forpliktelser i praksis må gi tilnærmet like god beskyttelse av personopplysninger som EU-retten. Domstolen vurderte derfor om Safe Harbor-ordningens system med egenerklæringer var effektivt i direktivets forstand.

Domstolen presiserte at kravet til tilstrekkelig beskyttelsesnivå ikke utelukker et system med egenerklæringer, men at systemet i så fall måtte suppleres med effektive kontrollmekanismer for å identifisere og sanksjonere brudd på personvernprinsippene.[147] Uttalelsen gjenspeiler det overordnede kravet til høyt beskyttelsesnivå og effektiv beskyttelse av personopplysninger; en materiell rettighet som ikke kan gjennomføres prosessuelt, kan fort bli illusorisk.

Hvilke prosessuelle rettigheter hadde de registrerte etter Safe Harbor-beslutningen? Domstolen fastslo at Safe Harbor-beslutningen ikke gav de registrerte mulighet til å bruke rettsmidler for å få adgang til, rettet eller slettet sine personopplysninger, og beslutningen oppfylte dermed ikke kravene til en effektiv rettslig domstolsprøving etter EU-charteret artikkel 47.[148] De registrerte hadde kun adgang til tvisteløsning ved FTC, og FTC har kun myndighet til å behandle kommersielle tvister, ikke tvister om lovligheten av myndigheters inngrep i personvernet.[149] Safe Harbor-ordningen sikret dermed ikke rett til effektiv administrativ og rettslig prø-

[146] Mer om dette i Bourgeois (2016)

[147] Schrems-avgjørelsen (81)

[148] Schrems-avgjørelsen (95)

[149] Schrems-avgjørelsen (89)

ving. Som nevnt i avsnitt 3.3 var dette et av hovedpunktene i kritikken av Safe Harbor-beslutningen.

Det kan problematiseres om domstolen er for teoretisk i sin analyse av effektiviteten av Safe Harbor-beslutningens kontrollmekanismer. Domstolen vurderte bare hvordan reglene i Safe Harbor-beslutningen var utformet, ikke hvordan de hadde fungert i praksis, til tross for at domstolen presiserte at direktivet artikkel 25 krever at personopplysninger gis en tilstrekkelig beskyttelse både på papiret og i praksis. EU-domstolen trakk riktignok frem kommisjonens uttalelser fra 2013, som la stor vekt på Safe Harbor-ordningens praktiske gjennomføring, men domstolen sluttet seg ikke direkte til uttalelsene.[150]

Videre kan man spørre om domstolens tilnærming var for ensidig i den forstand at den burde vurdert hvor effektivt de europeiske nasjonale tilsynene håndhevet Safe Harbor-beslutningen. Som nevnt i avsnitt 3.2 hadde de europeiske tilsynene en viss myndighet til å gripe inn i overføringer på bakgrunn av Safe Harbor-beslutningen. Imidlertid brukte ikke de europeiske datatilsynene denne kompetansen.[151] Et motargument er at det ikke var nødvendig for EU-domstolen å ta stilling til verken den amerikanske eller europeiske praktiseringen av Safe Harbor-beslutningen når beslutningen ikke engang på papiret oppfylte kravene i direktivet.

4.5.2 Vilkår for å gjøre inngrep i personvernet

4.5.2.1 Klare og presise regler og streng proporsjonalitetsvurdering

Åpnet Safe Harbor-beslutningen for større inngrep i personvernprinsippene enn det som var forsvarlig dersom beslutningen skulle sikre effektiv og fullstendig beskyttelse av retten til personvern? Før domstolen tok stilling til spørsmålet presiserte den at det kan foreligge et inngrep i personvernet uavhengig av om opplysningene er sensitive eller om inngrepet kan få negative konsekvenser for de berørte.[152] Terskelen er altså lav for at noe skal regnes som et inngrep. På den andre siden er det ikke gitt at ethvert inngrep er ulovlig.

Hvilke vilkår må være oppfylt for å gjøre lovlige inngrep i personvernet? For det første krever EU-domstolen at rettsakten som åpner for inngrepet, gir «*clear and precise rules governing the scope and application of a measure*» og at rettsakten pålegger «*minimum safeguards*» som effektivt reduserer risikoen for misbruk av og ulovlig tilgang til personopplysninger.[153] Dette sikrer de registrerte en viss mulighet til å forutse hvordan opplysningene deres kan bli brukt

[150] Schrems-avgjørelsen (90), Kuner (2016) s. 13

[151] Treacy (2014) s. 5-6, COM(2013) 847 s. 4

[152] Schrems-avgjørelsen (87) med henvisning til case C-293/12 Digital Rights Ireland (33)

[153] Schrems-avgjørelsen (91)

etter overføringen.[154] Kravene er særlig viktige ved automatisk behandling av opplysninger og ved betydelig risiko for at noen skaffer seg ulovlig adgang til opplysningene.[155] For det andre må unntak fra og begrensninger i den grunnleggende retten til beskyttelse av personopplysninger være strengt nødvendige («*strictly necessary*»).[156]

Man kan spørre hvor EU-domstolen henter de to vilkårene fra. Domstolen refererer til *Digital Rights Ireland*. I den saken viste domstolen til EU-charteret artikkel 52, som krever at inngrep i grunnleggende rettigheter må ha lovhjemmel, respektere kjernen i rettighetene og være i samsvar med proporsjonalitetsprinsippet.[157] Formuleringen «*clear and precise rules*» utleder domstolen i *Digital Rights Ireland* imidlertid fra analogi til EMDs praksis om tolkningen av EMK artikkel 8.[158]

Man kan dermed argumentere for at å tolke personverndirektivets regler i lys av charteret artikkel 7 og 8, se avsnitt 4.2, medfører at EU-domstolen også kan bygge på rettspraksis om andre EU-rettsakter om personvern – *Digital Rights Ireland* gjaldt datalagringsdirektivet – og fra domstoler utenfor EU-systemet, her EMD. Hvordan kan man metodisk begrunne at EU-domstolen viser til praksis fra EMD? Ett argument er at selv om EU som sådan ikke er tilsluttet EMK, er alle EUs medlemsland tilsluttet konvensjonen.[159]

4.5.2.2 Hvilke inngrep i personvernet åpnet Safe Harbor-beslutningen for?

Safe Harbor-beslutningen gav adgang til å gjøre generelle unntak fra plikten til å følge Safe Harbor-prinsippene

> «*(a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization*».[160]

---

154 A29WP (2016)a s. 1

155 Schrems-avgjørelsen (91)

156 Schrems-avgjørelsen (92)

157 Case C-293/12 (38)

158 Case C-293/12 (52),(54)-(55)

159 Sejersted (2011) s. 58

160 Decision 2000/520/EC tillegg I fjerde avsnitt

I tillegg var Safe Harbor-ordningen forbeholdt selskaper, og amerikanske myndigheter verken måtte eller kunne slutte seg til ordningen.[161] Samtidig fulgte det av Safe Harbor-beslutningen at de amerikanske selskapenes forpliktelser etter amerikansk rett ved motstrid hadde forrang over forpliktelser etter Safe Harbor-ordningen.[162]

Det innebærer at amerikanske selskaper som etter amerikansk rett pliktet å gi myndighetene personopplysninger som de har fått overført fra EU, måtte overgi opplysningene, selv om Safe Harbor-ordningen ikke gav noen garantier for at personopplysningene ble behandlet forsvarlig av amerikanske myndigheter. Siden Safe Harbor-beslutningen inneholdt generelle unntak fra plikten til å følge personvernprinsippene og gav amerikanske myndigheter ukontrollert tilgang til europeiske personvernopplysninger, åpnet beslutningen for inngrep i personvernet.[163]

4.5.2.3 Var inngrepene Safe Harbor-beslutningen åpnet for, i samsvar med kravene etter EU-retten?

Når EU-domstolen hadde klarlagt vilkårene for å gjøre inngrep i personvernet og hvilke inngrep Safe Harbor-beslutningen åpnet for, vurderte den om inngrepene var lovlige. EU-domstolen kom til at det ikke var et strengt nødvendig inngrep at beslutningen gav amerikanske myndigheter generell adgang til å lagre alle personopplysninger, uten nyanseringer, begrensinger eller unntak ut fra formålet med lagringen eller andre objektive kriterier.[164]

Man kan kritisere EU-domstolens tilnærming. Nasjonal sikkerhet faller utenfor personverndirektivets virkeområde og er EU-landenes ansvar, se avsnitt 2.2. Det kan derfor virke urimelig at domstolen foretar en inngående vurdering av Safe Harbor-beslutningens regulering av personvern og nasjonal sikkerhet uten at domstolen også drøfter lovligheten av EU-landenes regulering av nasjonal sikkerhet og personvern.[165] Dette gjelder særlig fordi kravet til tilstrekkelig beskyttelsesnivå må vurderes i lys av hva som er standarden i EU. Derimot kan man argumentere at EU-lands brudd på grunnleggende rettigheter i alle tilfeller ikke unnskylder tilsvarende brudd fra et tredjeland.[166]

Domstolen anså dessuten den generelle adgangen amerikanske myndigheter hadde til *elektronisk kommunikasjon* etter Safe Harbor-beslutningen som et inngrep i kjernen av den grunn-

[161] Schrems-avgjørelsen (82)
[162] Schrems-avgjørelsen (85)-(86)
[163] Schrems-avgjørelsen (87)
[164] Schrems-avgjørelsen (93)
[165] Kuner (2016) s. 13
[166] Kuner (2016) s. 14

leggende retten til respekt for privatliv i charteret artikkel 7.[167] Domstolen henviste til *Digital Rights Ireland*. I den saken ble datalagringsdirektivet ikke ansett å utgjøre et slikt inngrep fordi direktivet ikke gav tilgang til *innholdet* i den elektroniske kommunikasjonen, kun metadata om kommunikasjonen.[168] Safe Harbor-beslutningen gav derimot de amerikanske myndighetene mulighet til å få tilgang til innholdet i elektronisk kommunikasjon, og inngrepet var derfor i kjernen av artikkel 7.

Hvorfor drøftet ikke EU-domstolen om den generelle adgangen til opplysninger også var en krenkelse av charteret artikkel 8? Masseovervåkning kan tross alt påvirke både individers rett til privatliv og deres rett til beskyttelse av personopplysninger.[169] I *Digital Rights Ireland* uttalte domstolen at siden datalagringsdirektivet inneholdt visse prinsipper om beskyttelse av personopplysninger og datasikkerhet, var ikke inngrepet i kjernen av charteret artikkel 8.[170] Safe Habor-beslutningen inneholdt også visse personvernprinsipper. Det kan ha vært årsaken til at EU-domstolen ikke vurderte om masseovervåkningen også var i strid med charteret artikkel 8.

Kuner er ikke enig i at det kan skilles så tydelig mellom inngrep i charteret artikkel 7 og 8, og han kritiserer domstolens resonnement fordi «*data security, while certainly important, is not one of the central elements of data protection. The Court's interpretation of the essence of the rights to privacy and data protection in* ***Schrems*** *may thus reflect its longstanding confusion about the distinction between these two rights*» (forfatterens utheving).[171]

Som nevnt i avsnitt 1.4.1 er det noe uklarhet i EUs bruk av begrepene «p*rivacy*» og «*data protection*». Man kan dermed argumentere for at Schrems-avgjørelsen er et eksempel på at uklarheter i terminologi kan påvirke tolkningen av den materielle retten. Samtidig kan man spørre om det ville utgjort en reell forskjell om EU-domstolen kom til at Safe Harbor-beslutningen var i strid med både artikkel 7 og 8 i charteret.

4.5.2.4 Schrems-avgjørelsens rolle i utviklingen av en strengere proporsjonalitetsvurdering

Formålet med dette delkapitlet er å vise at EU-domstolen har utviklet et strengere proporsjonalitetsprinsipp ved inngrep i personvern siden Safe Harbor-beslutningen ble truffet i 2000, og

---

167 Schrems-avgjørelsen (94)

168 Case C-293/12 (39)

169 Kuner (2016) s. 9

170 Case C-293/12 (40)

171 Kuner (2016) s. 9-10

at Schrems-avgjørelsen er et ledd i denne utviklingen. EU-domstolen foretar for det første en mer inngående vurdering av inngrepet i den konkrete saken, og for det andre krever domstolen nå at inngrep er strengt nødvendige.

I de første årene etter Safe Harbor-beslutningen fokuserte EU-domstolen på å gi prinsipielle vurderinger av kravet til proporsjonalitet. I sakene *Rechnungshof* og *Lindqvist* fra 2003 oppstilte EU-domstolen krav til proporsjonalitet ved inngrep, men overlot til de nasjonale domstolene å foreta den konkrete proporsjonalitetsvurderingen.[172] I *Huber* fra 2008 gikk derimot EU-domstolen delvis inn i en konkret proporsjonalitetsvurdering; domstolen understreket at registret med personopplysninger som saken gjaldt, ikke måtte inneholde flere opplysninger enn det som var *nødvendig* for registerets formål.[173]

I Schrems-avgjørelsen gikk EU-domstolen et skritt lengre. Domstolen tok også stiling til hvilke inngrep Safe Harbor-beslutningen åpnet for og om inngrepene oppfylte EU-rettens vilkår. Man kan dermed argumentere for at Schrems-avgjørelsen viser en tendens til at EU-domstolen foretar en stadig mer inngående, konkret proporsjonalitetsvurdering ved mulige inngrep i personvernet.

I tillegg krevde EU-domstolen i Schrems-avgjørelsen at inngrep i personvernet var strengt nødvendige. Som nevnt i avsnitt 3.3 mente derimot Artikkel 29-arbeidsgruppen i 2000 at inngrep var lovlige dersom de var nødvendige. Hva skjedde i EU-domstolens rettspraksis etter 2000 som forklarer denne utviklingen?

Samme dag som *Huber* ble avsagt, avsa EU-domstolen den første avgjørelsen som krevde at inngrep i personvernet var strengt nødvendige, *Satamedia*.[174] Hvorfor måtte inngrepet i *Huber* bare være nødvendig, mens inngrepet i *Satamedia* måtte være strengt nødvendig*? Satamedia* gjaldt blant annet avveiningen mellom personvern og ytringsfrihet i personverndirektivet artikkel 9, og domstolen uttalte at

> «*[i]n order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary, first, to interpret notions relating to that freedom, such as journalism, broadly. Secondly, and in order to achieve a balance between the two fundamental rights, the protection of the fundamental right to privacy requires that the derogations and limitations in relation to the protection of data pro-*

[172] Case C-465/00 (88), case C-101/01 (89)-(90), se Bagger Tranberg (2011) s. 242

[173] Case C-524/06, se Bagger Tranberg (2011) s. 242-243

[174] Case C‑73/07

vided for in the chapters of the directive referred to above must apply only in so far as is strictly necessary».[175]

Domstolen gav ingen ytterligere begrunnelse for hvorfor inngrep i personvernet måtte være strengt nødvendige, og det kan bemerkes at ordlyden i personverndirektivet artikkel 9 tyder på at det er tilstrekkelig at inngrep er nødvendige.[176] Siden domstolen krevde at inngrep måtte være strengt nødvendige i *Satamedia*, men ikke av *Huber*, kan man argumentere for at EU-domstolen opprinnelig hadde til hensikt at det strengere proporsjonalitetsprinsippet kun skulle gjelde ved harmonisering av to grunnleggende rettigheter, ikke ved ethvert mulig inngrep i personvern.

Satamedias krav til at inngrep måtte være strengt nødvendige, ble imidlertid gjentatt i de to personvernsakene *Schecke* fra 2010[177] og i *IPI* fra 2013[178] uten at det gis noen nærmere redegjørelse for hvorfor rettssetningen hadde overføringsverdi. Ingen av sakene gjaldt forholdet mellom personvern og en annen grunnleggende rettighet. *Schecke* omhandlet forholdet mellom EU-charteret artikkel 7 og 8 og forordninger som påla offentliggjøring av mottakerne i en støtteordning. *IPI* gjaldt en tolkning av personverndirektivet artikkel 13. I de to sakene *Digital Rights Ireland* og *Ryneš* fra 2014 gjentok EU-domstolen at inngrep i personvernet måtte være strengt nødvendige under henvisning til *IPI*.[179] Sakene gjaldt henholdsvis datalagringsdirektivet og tolkningen av personverndirektivet artikkel 3(2).

Det kan spørres hva som er fellesnevneren for avgjørelsene som krever at inngrep i personvernet er strengt nødvendige. De avgjørelsene som knytter seg til personverndirektivet, gjelder alle de generelle reglene i direktivets kapittel II, med unntak av Schrems-avgjørelsen. Derimot gjelder for eksempel ikke *Digital Rights Ireland* bestemmelser i personverndirektivet. Man kan imidlertid argumentere for at det rettslige bakteppet for alle avgjørelsene er EU-charteret artikkel 7 og 8.

Charteret ble ikke rettslig bindende før i 2009. Derimot er kun én av de ovennevnte avgjørelsene, *Satamedia*, fra før 2009, og i *Satamedia* kan kravet til streng nødvendighet begrunnes særskilt; dersom retten til ytringsfrihet tolkes vidt, må det være en viss terskel for inngrep i personvernet for å balansere rettighetene mot hverandre. Gjeldende rett i EU-retten virker dermed å være at man må foreta en streng proporsjonalitetsvurdering ved ethvert inngrep i

---

175 Case C‑73/07 (56)

176 Bagger Tranberg (2011) s. 247

177 Case C‑92/09 (77),(86)

178 Case C-473/12 (39)

179 Case C-293/12 (52), case C-212/13 (28)

personvernet, uavhengig av hvilken rettsakt saken gjelder, såfremt rettsakten inkorporerer rettigheter etter EU-charteret artikkel 7 og 8.

Analysen av EU-domstolens rettspraksis tyder altså på at fra Safe Harbor-beslutningen ble truffet og frem til Schrems-avgjørelsen ble avsagt, har EU-domstolen utviklet et strengere proporsjonalitetsprinsipp som har fått bred rekkevidde i europeisk personvernlovgivning, samtidig som domstolen foretar en stadig mer inngående vurderinger av lovligheten av inngrep i personvernet.

Det kan bemerkes at EMD synes å tolke kravet til proporsjonalitet ved inngrep i personvernet på samme måte som EU-domstolen, i alle fall hva gjelder myndigheters masseovervåkning av borgerne. Saken *Szabó and Vissy* fra 2016 gjaldt lovmessigheten av masseovervåkning av to dissidenter i lys av EMK artikkel 8. EMD kom enstemmig til at overvåkningen var et brudd på EMK artikkel 8(2). Slik masseovervåkning kunne bare tillates dersom det var «*strictly necessary*» for å verne demokratiske institusjoner.[180] I avgjørelsen nevnes også praksis fra EU-domstolen, herunder *Digital Rights Ireland* og Schrems-avgjørelsen.[181] Det tyder på at domstolene lar seg påvirke av hverandres praksis i utviklingen av proporsjonalitetsvurderingen ved inngrep i personvernet.[182]

4.5.3 Krav til formell konstatering av tilstrekkelig beskyttelsesnivå

I tillegg til å vurdere det materielle innholdet i Safe Harbor-beslutningen artikkel 1, oppstilte EU-domstolen formelle krav til kommisjonens forsvarlighetsvurdering. Domstolen krevde at kommisjonen eksplisitt gav uttrykk for at den hadde vurdert og kommet til at tredjelandet sikret et tilstrekkelig beskyttelsesnivå.[183] Formelle krav var en mindre fremtredende del av kritikken av Safe Harbor-ordningen, men Reidenberg var inne på problemstillingen, se avsnitt 3.3. Schrems-avgjørelsen belyser derfor sider ved personverndirektivet artikkel 25(6) som har vært mindre i fokus tidligere.

EU-domstolen mente Safe Harbor-beslutningen hadde formelle mangler fordi

---

180 Szabó and Vissy (54). EMD har en lang tradisjon for å kreve streng nødvendighet ved masseovervåkning; kravet stammer fra avgjørelsen Klass and Others v. Germany fra 1978

181 Én av dommerne gav en egen begrunnelse hvor han viser til begge avgjørelsene, mens flertallet viser til *Digital Rights Ireland*, men ikke Schrems-avgjørelsen

182 Se også avsnitt 4.4.2, hvor EU-domstolen henviser til proporsjonalitetsprinsippet og EMDs praksis for å begrunne en inngående overprøving av kommisjonens forsvarlighetsvurdering

183 Schrems-avgjørelsen (97)

> «*Decision 2000/520, pursuant to Article 2 thereof, 'concerns only the adequacy of protection provided in the United States under the [safe harbour principles] implemented in accordance with the FAQs with a view to meeting the requirements of Article 25(1) of Directive [95/46]', without, however, containing sufficient findings regarding the measures by which the United States ensures an adequate level of protection, within the meaning of Article 25(6) of that directive, by reason of its domestic law or its international commitments*».[184]

Safe Harbor-beslutningen var altså mangelfull fordi kommisjonen ikke gav uttrykk for at USAs lovgivning eller internasjonale forpliktelser sikret et tilstrekkelig beskyttelsesnivå. Kan uttalelsen også kan tas til inntekt for at kommisjonen ikke har hjemmel etter direktivet artikkel 25(6) til å vurdere om kun et utvalg av aktører i tredjelandet sikrer et tilstrekkelig beskyttelsesnivå?[185] Man kan argumentere for at dersom kommisjonen ikke kunne godkjenne kun et utvalg av aktører, ville EU-domstolen konstatert det. Den siterte uttalelsen er imidlertid trolig for vag til å gi et klart svar på spørsmålet.

Domstolen uttalte videre at kommisjonen ikke gav uttrykk for om Safe Harbor-beslutningen inneholdt regler som begrenset myndighetenes adgang til å samle inn personopplysninger på bakgrunn av nasjonal sikkerhet, eller om det fantes effektive ordninger for å prøve lovligheten av slike inngrep.[186] Domstolen besluttet derfor at artikkel 1 i Safe Harbor-beslutningen var ugyldig på formelt grunnlag.[187]

Fordi Safe Harbor-beslutningen var ugyldig på formelt grunnlag, mente domstolen det ikke var nødvendig å analysere innholdet i Safe Harbor-prinsippene. Schrems-avgjørelsen gir dermed ikke svar på om Safe Harbor-prinsippene var «*essentially equivalent*» grunnprinsippene i personverndirektivet, eller om de var mangelfulle, slik mange kritiserte dem for å være, se avsnitt 3.3.

Hadde det noen selvstendig betydning at artikkel 1 i Safe Harbor-beslutningen var ugyldig på formelt grunnlag? Man kan problematisere om Safe Harbor-beslutningen også ville blitt erklært ugyldig dersom beslutningen kun hadde formelle mangler. Problemstillingen er imidlertid mest av teoretisk interesse. Kommisjonen kunne rette opp i de formelle manglene ved å endre beslutningen til å imøtekomme domstolens krav.

---

184 Schrems-avgjørelsen (83)

185 Se avsnitt 2.3.2

186 Schrems-avgjørelsen (88)-(89)

187 Schrems-avgjørelsen (97)-(98)

4.5.4 Krav til hjemmel for innskrenkninger av tilsynsmyndighetenes kompetanse

Domstolen drøftet også gyldigheten av artikkel 3 i Safe Harbor-beslutningen. Bakgrunnen var at etter første ledd i artikkel 3 kunne nasjonale datatilsyn kun suspendere overføringer av personopplysninger etter Safe Harbor-ordningen «*under restrictive conditions establishing a high threshold for intervention*».[188] Artikkel 3 var ikke et fokus for kritikken av Safe Harbor-beslutningen. Tvert imot tyder en uttalelse fra Europakommisjonen på at den mente Safe Harbor-beslutningen gav tilsynene større kompetanse enn de hadde etter direktivet, fordi

> «*[i]ndependently of the powers they enjoy under the Safe Harbour Decision, EU national data protection authorities are competent to intervene, including in the case of international transfers, in order to ensure compliance with the general principles of data protection set forth in the 1995 Data Protection Directive*».[189]

Som drøftet i avsnitt 4.3 hadde imidlertid de nasjonale tilsynene kompetanse til å kontrollere gjennomføringen av direktivets artikkel 25, herunder overføringer etter Safe Harbor-beslutningen, i medhold av artikkel 28. Ved å sette ytterligere vilkår for å suspendere overføringer, innskrenket Safe Harbor-beslutningen tilsynenes kompetanse. Domstolen konstaterer at kommisjonen ikke hadde hjemmel etter direktivet artikkel 25(6) til å oppstille vilkår for tilsynenes kontroll, og derfor var artikkel 3 i Safe Harbor-beslutningen ugyldig.[190]

EU-domstolen kom til at når artiklene 1 og 3, som utgjorde sentrale deler av beslutningen, var ugyldige, kunne heller ikke resten av beslutningen bli stående. Domstolen konkluderte derfor at Safe Harbor-beslutningen i sin helhet var ugyldig.[191]

4.5.5 Oppsummering av rettssetningene fra vurderingen av Safe Harbor-beslutningens gyldighet

Schrems-avgjørelsen oppstiller strenge og omfattende krav til en forsvarlighetsvurdering. Et tilstrekkelig beskyttelsesnivå etter personverndirektivet artikkel 25 forutsetter et system som sikrer effektiv håndheving og effektive rettsmidler for de registrerte. Hvis disse kravene er oppfylt, er det derimot uten betydning om systemet bygger på eksempelvis egenerklæringer. Selv om tredjelandet har ordninger for tilsyn og kontroll med behandlingen av personopplys-

---

188 Schrems-avgjørelsen (101)

189 COM(2013) 847 s. 4

190 Schrems-avgjørelsen (103)-(104)

191 Schrems-avgjørelsen (105)-(106)

ningene, har ikke Europakommisjonen hjemmel til å begrense de europeiske datatilsynenes kompetanse til å håndheve direktivet.

Det kan kun gjøres inngrep og unntak i personvernet dersom det er strengt nødvendig, og inngrepet må også ha grunnlag i klare og presise regler. Terskelen er lav for at noe regnes som et inngrep, og dersom myndighetene har adgang til innholdet i elektronisk kommunikasjon, vil inngrepet være i kjernen av EU-charteret artikkel 7. Det må fremgå av kommisjonens forsvarlighetsvurdering at kommisjonen har vurdert de ovennevnte kravene og at resultatet er at tredjelandet sikrer et tilstrekkelig beskyttelsesnivå for personopplysninger gjennom sin lovgiving eller sine internasjonale forpliktelser.

5 Schrems-avgjørelsens rekkevidde

Drøftelsene ovenfor har klargjort hvilke rettssetninger som kan utledes fra Schrems-avgjørelsen. Formålet med dette delkapitlet er å drøfte rekkevidden av rettssetningene. Schrems-avgjørelsen er avsagt i storkammer, og avgjørelsen vil trolig få stor vekt i andre saker, såfremt den er relevant.[192] Av plasshensyn tar avhandlingen kun for seg et utvalg av mulige perspektiver som avgjørelsens rekkevidde kan vurderes ut fra: Betydningen for overføringer på grunnlag av tilstrekkelig beskyttelsesnivå, for alternative måter å overføre personopplysninger og for den kommende personvernforordningen.

5.1.1 Dommens betydning for overføringer på grunnlag av tilstrekkelig beskyttelsesnivå

Som følge av Schrems-avgjørelsen kan ikke Safe Harbor-beslutningen lenger benyttes som grunnlag for overføringer av personopplysninger fra EU til USA. Men fra hvilket tidspunkt fikk avgjørelsen virkning? EU-domstolen gav selv uttrykk for at avgjørelsen ikke hadde tilbakevirkende kraft.[193] Derimot uttrykte ikke domstolen at det var en karensperiode før avgjørelsen fikk virkning. Derfor er det naturlig å slutte seg til Artikkel 29-arbeidsgrupppens forståelse av dommen; det var lovstridig å foreta overføringer på grunnlag av Safe Harbor-beslutningen fra avgjørelsen ble truffet.[194] De nasjonale tilsynene kunne dermed iverksette tiltak mot selskap som brukte Safe Harbor-ordningen etter 6. oktober 2015.[195]

Kan Schrems-avgjørelsen også få betydning for andre eksisterende og fremtidige forsvarlighetsvurderinger etter personverndirektivet artikkel 25(6)? Europakommisjonen har i en meddelelse fra 2015 gitt uttrykk for at Schrems-avgjørelsens rekkevidde kun omfatter Safe Harbor-beslutningen.[196] Kommisjonen gir ingen begrunnelse for standpunktet, som svekker vekten av det. I praksis beror rekkevidden av EU-domstolens avgjørelser på om rettssetningene har overføringsverdi, eller om de er spesifikke for faktumet i den konkrete avgjørelsen.[197] Det er hensiktsmessig å skille mellom rekkevidden av ulike deler av Schrems-avgjørelsen.

---

192 Fredriksen (2014) s. 244, Craig (2008) s. 67

193 Schrems-avgjørelsen (52)

194 A29WP (2015) s. 2

195 Artikkel 29-arbeidsgruppen har riktignok uttalt at de nasjonale tilsynene først ville iverksette håndhevelse av avgjørelsen dersom en ny ordning med amerikanske myndigheter ikke var på plass innen slutten av januar 2016, jf. A29WP (2015) s. 1, A29WP (2016)a s. 2. Se avsnitt 6.2

196 COM(2015) 566 s. 14

197 Fredriksen (2014) s. 239

I domstolens drøftelser av tilsynsmyndighetenes kompetanse er ikke rekkevidden av formuleringene begrenset til Safe Harbor-beslutningen. EU-domstolen uttaler for eksempel at *«[…] a Commission decision adopted pursuant to Article 25(6) of Directive 95/46,* ***such as*** *Decision 2000/520, cannot prevent persons […]lodging with the national supervisory authorities a claim […]*» (min utheving).[198] Det tilsier at rettssetningen ikke bare gjelder for Safe Harbor-beslutningen.

Om denne delen av avgjørelsen bemerker for øvrig kommisjonen at alle de andre forsvarlighetsbeslutningene inneholder tilsvarende bestemmelser som Safe Harbor-beslutningens artikkel 3, og at den derfor vil «*draw the necessary consequences from the judgment by shortly preparing a decision […] replacing that provision in all existing adequacy decisions*».[199] Kommisjonen tillegger dermed i praksis dommens uttalelser om tilsynsmyndighetenes kompetanse vekt ved tolkningen av de andre forsvarlighetsvurderingene.

Hvilken overføringsverdi har domstolens rettssetninger om vurderingstemaet og terskelen for et tilstrekkelig beskyttelsesnivå og om domstolens grunnlag for prøvingen av kommisjonens beslutninger? I disse vurderingene argumenterer EU-domstolen prinsipielt og uten henvisning til Safe Harbor-beslutningen, se avsnitt 4.4.1 og 4.4.2. Dermed er det rimelig å anvende rettssetningene også ved tolkningen av andre forsvarlighetsvurderinger.

Mer problematisk er overføringsverdien til rettssetningene knyttet til Safe Harbor-beslutningen artikkel 1. På den ene siden var ordlyden i Safe Harbor-beslutningen artikkel 1 særskilt fremforhandlet mellom EU og USA. Det er derfor nærliggende å anta at vurderinger som knytter seg til denne bestemmelsen, er konkret utformet. Dersom man på den andre siden går inn i vurderingene, kan man argumentere for at flere av rettssetningene er prinsipielle og derfor har overføringsverdi.

For eksempel er domstolens beskrivelser av systemet med egenerklæringer i Safe Harbor-beslutningen lite prinsipielle. Uttalelsene om at et system med egenerklæring ikke i seg selv er avgjørende, men at systemet må kombineres med effektiv håndheving og prøving, er imidlertid av prinsipiell karakter, se avsnitt 4.5.1. Selv om domstolen foretar konkrete vurderinger av unntakene fra personvernprinsippene i Safe Harbor-beslutningen, kommer domstolen også med generelle bemerkninger om proporsjonalitetsvurderingen og vilkåret til klare og presise regler ved inngrep i personvernet, se avsnitt 4.5.2.1 og 4.5.2.3. De formelle kravene domsto-

198 Schrems-avgjørelsen (53)

199 COM(2015) 566 s. 14-15

len stiller til Safe Harbor-beslutningen er konkrete, se avsnitt 4.5.3. Derimot er det et prinsipielt poeng at det kreves en formell konstatering av tilstrekkelig beskyttelsesnivå.

For øvrig kan Schrems-avgjørelsen få betydning for overføringer av personopplysninger mellom to land som ikke er tilsluttet personverndirektivet. Dommen er ikke bindende for disse landene, men avgjørelsen kan få indirekte betydning. EUs personvernlovgivning har blitt stadig mer utbredt som en internasjonal standard – den såkalte Brussel-effekten.[200] I Dubai var for eksempel overføringer av personopplysninger til USA tillatt dersom mottakeren var tilsluttet Safe Harbor-ordningen. Etter Schrems-avgjørelsen vil datatilsynet i Dubai måtte ta stilling til om overføringer til USA fremdeles er tillatt.[201]

Man kan spørre hva som førte til at EUs tilnærming til personvern har vunnet så mye terreng blant land utenfor EU mens den amerikanske tilnærmingen ikke har gjort det. Trolig var en viktig årsak at EU var tidlig ute med å utvikle et omfattende regelverk. USA hadde derimot ikke en systematisert regulering av personvern, og det var derfor vanskelig for andre land å innføre en lignende ordning.[202] Samtidig har personverndirektivets regler om overføringer av personopplysninger over landegrensene ekstraterritoriale implikasjoner, se avsnitt 4.3.1. Tredjeland kan dermed ha følt seg presset til å følge personverndirektivets krav for å få handle med EU-landene, se også avsnitt 6.1.

5.1.2 Dommens følger for alternative måter å overføre personopplysninger til tredjeland

I kjølvannet av Schrems-avgjørelsen er det reist spørsmål om lovligheten av å anvende BCR og SCC ved overføringer av personopplysninger fra EU til USA. Forutsetningen for problematikken virker å være at selskaper i USA har forpliktelser etter amerikansk rett som blant annet gir amerikanske myndigheter vid adgang til personopplysninger av hensyn til nasjonal sikkerhet, og at disse forpliktelsene har forrang over forpliktelser selskapene har etter sine BCR eller SCC[203].

Schrems-avgjørelsen fastslår at ved generelle unntak fra retten til beskyttelse av personopplysninger som for eksempel åpner for masseovervåkning, sikres ikke et tilstrekkelig beskyttel-

---

200 Kuner (2016) s. 10-11, Svantesson (2011) s. 184. Land som Japan, Australia og Brasil har latt seg inspirere at EUs personvernlovgivning, uten at de har fått en beslutning om tilstrekkelig beskyttelsesnivå, se Heisenberg (2005) s. 101-113

201 Al Tamimi & Co. (2016)

202 Heisenberg (2005) s. 13

203 Den videre drøftelsen bygger på denne forutsetningen, og av hensyn til ordgrensen foretar ikke avhandlingen en nærmere analyse av amerikansk rett

sesnivå, se avsnitt 4.5.2.3. Dersom kravene i Schrems-avgjørelsen også gjelder for alternative overføringsmetoder, vil følgelig ikke BCR eller SCC gi tilstrekkelige garantier for personvernet ved overføringer til USA.

Vil kravene Schrems-avgjørelsen til overføringer etter direktivet artikkel 25, også helt eller delvis gjelde for overføringer etter artikkel 26(2)? Problemstillingen kan for øvrig bli aktuell for overføringer til et hvilket som helst tredjeland som pålegger dataimportøren forpliktelser i strid med kravene som følger av BCR eller SCC.

Det fremgår ikke uttrykkelig av Schrems-avgjørelsen om uttalelsene om artikkel 25 også er ment å gjelde for artikkel 26(2). Schrems-avgjørelsens overføringsverdi må derfor bero på om vurderingen etter direktivet artikkel 25 har en tilstrekkelig sammenheng med vurderingen som skal foretas etter artikkel 26(2). Man kan argumentere for at overføringsmetodene i artikkel 25 og artikkel 26(2) er to separate systemer. Kuner deler for eksempel reguleringen av overføringer av personopplysninger opp i ulike tilnærminger, hvor regler basert på forsvarlighetsvurderinger i utgangspunktet bygger på en annen tilnærming enn regler basert på tilstrekkelige garantier[204].

I den geografiske tilnærmingen er formålet å stille krav til standarden for og praktiseringen av beskyttelse av personopplysninger i mottakerlandet, slik som i forsvarlighetsvurderingen etter personverndirektivet artikkel 25.[205] I den organisasjonsbaserte tilnærmingen er formålet å pålegge dataeksportøren, og eventuelt dataimportøren, å følge visse personvernprinsipper uavhengig av hvor behandlingen skjer, og man holder dem dermed ansvarlige for behandlingen av personopplysningene.[206] Kuner nevner BCR og SCC som eksempler på den organisasjonsbaserte tilnærmingen[207].

Europakommisjonen synes å ha en lignende forståelse av direktivet og har uttalt at

> «*[t]he rules on international data transfers laid down in Directive 95/46/EC are based on a clear distinction between, on the one hand, transfers to third countries ensuring an adequate level of protection (Article 25 of the Directive) and, on the other hand, transfers to third countries which have not been found to ensure an adequate level of protection (Article 26 of the Directive)*».[208]

---

204 Kuner (2013) s. 61,76

205 Kuner (2013) s. 64

206 Kuner (2013) s. 71-72

207 Kuner (2013) s. 72-73

208 COM(2015) 566 s. 5

Det er nærliggende å forstå uttalelsen som at kommisjonen mener forsvarlighetsvurderingen og vurderingen av tilstrekkelige garantier i utgangspunktet bygger på to forskjellige systemer. Det ville i så fall tilsi at Schrems-avgjørelsen ikke har overføringsverdi til vurderinger etter artikkel 26(2).

Derimot kan man argumentere for at det er unyansert å si at BCR og SCC kun bygger på ansvarliggjøring av dataeksportøren og -importøren, slik at det er uten betydning hvilket beskyttelsesnivå mottakerlandet gir for behandlingen av personopplysninger. Dersom et lands lovgivning gir nesten like høyt beskyttelsesnivå for behandling av personopplysninger som EU, er det mindre betenkelig å tillate bruk av BCR og SCC enn om landets lovgivning har en langt lavere beskyttelse av personopplysninger. Dette kommer på spissen i tilfeller som Schrems-avgjørelsen, der Safe Harbor-beslutningen åpnet for inngrep i strid med helt grunnleggende krav etter EU-retten, se avsnitt 4.5.2.3.

Europakommisjonen har også kommet med en uttalelse som kan moderere den oppfatningen at det er et klart skille mellom artikkel 25 og artikkel 26. Kommisjonen uttalte at

> *«[…] in the absence of a Commission finding of adequacy, the responsibility is on controllers to ensure that their data transfers take place with sufficient safeguards in accordance with Article 26(2) of the Directive. This assessment needs to be carried out in the light of all the circumstances surrounding the transfer at issue. In particular, both the SCCs and BCRs provide that if the data importer has reasons to believe that the legislation applicable in the recipient country may prevent it from fulfilling its obligations, it shall promptly inform the data exporter in the EU*» (kommisjonens fotnoter er utelatt).[209]

Uttalelsen tilsier at også i vurderingen etter artikkel 26(2) skal det foretas en helhetsvurdering hvor beskyttelsesnivået i tredjelandet spiller en rolle. Helhetsvurderingen etter artikkel 26(2) har dermed likhetstrekk med helhetsvurderingen kommisjonen foretar etter artikkel 25(6). Man kan dermed argumentere for at Schrems-avgjørelsen har overføringsverdi til artikkel 26(2).

Man kan også argumentere for at artikkel 25 og artikkel 26(2) begge inkorporerer grunnleggende personvernrettigheter og at det derfor er overføringsverdi mellom vurderingene etter bestemmelsene. Kuner har en tredje tilnærming til regulering av overføringer av personopp-

[209] COM(2015) 566 s. 13

lysninger hvor perspektivet er at beskyttelse av personopplysninger er en grunnleggende rett.[210] I lys av Schrems-avgjørelsen inkorporerer i alle fall artikkel 25 rettighetene i artikkel 7 og 8 i EU-charteret, se avsnitt 4.2. Videre er et grunnleggende hensyn bak personverndirektivet å unngå at beskyttelsen direktivet gir, uthules, se avsnitt 2.1. Man kan dermed argumentere for at også artikkel 26(2) må tolkes i lys av charteret artikkel 7 og 8. I så fall vil kravene Schrems-avgjørelsen stiller til overføringer på bakgrunn av at personvern er en grunnleggende rett, også gjelde for overføringer etter artikkel 26(2).

Artikkel 29-arbeidsgruppen og Büllesbach har kommet med uttalelser som støtter denne tolkningen; SCC og BCR utgjør ikke tilstrekkelige garantier for beskyttelsen av personopplysningene dersom myndighetene i mottakerlandet kan kreve å få adgang til personopplysninger utover det som er forsvarlig etter internasjonale menneskerettighetsstandarder.[211]

Etter Schrems-avgjørelsen tillot arbeidsgruppen inntil videre aktører å bruke BCR og SCC for overføringer til USA.[212] Etter en grundig vurdering har arbeidsgruppen imidlertid uttalt at de kravene til inngrep i grunnleggende rettigheter som følger av Schrems-avgjørelsen og øvrig rettspraksis fra EU-domstolen og EMD, må gjelde for alle overføringer etter personverndirektivet, herunder BCR og SCC.[213] Det gjenstår å se om EU-domstolen har samme syn på problemstillingen.

5.1.3 Dommens betydning for den kommende personvernforordningen

Schrems-avgjørelsen gjelder reglene om overføring av personopplysninger til tredjeland i personverndirektivet. Likevel kan man argumentere for at avgjørelsen også får betydning når EUs personvernforordning trer i kraft i den grad forordningen viderefører direktivets regler. I alle tilfeller fortsetter de eksisterende forsvarlighetsvurderingene etter direktivet artikkel 25(6) å gjelde frem til de blir endret, byttet ut eller trukket tilbake selv etter forordningen trer i kraft, jf. forordningsforslaget artikkel 45(9).

I det følgende drøftes forholdet mellom Schrems-avgjørelsen og forordningsforslagets regler om overføringer til tredjeland. Formålet er å vise at forordningen inkorporerer og bygger på flere av rettssetningene i Schrems-avgjørelsen og at det derfor er nærliggende å tolke forordningens regler i lys av Schrems-avgjørelsen. Av hensyn til ordgrensen behandles kun utvalgte problemstillinger.

---

210 Kuner (2013) s. 62-63

211 A29WP (1998) s. 21-22, Büllesbach (2010) s. 123

212 A29WP (2015) s. 1, A29WP (2016)a s. 2

213 A29WP (2016)d s. 3

Personvernforordningen åpner for at

> «*[a] transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection* », jf. forordningsforslaget art. 45(1) første punktum.

Ordlyden «*adequate level of protection*» er den samme som i direktivet artikkel 25, og det tilsier at forordningen viderefører direktivets system med forsvarlighetsvurderinger.

Forordningen går imidlertid lengre enn direktivet i å klargjøre og utdype hva som ligger i forsvarlighetsvurderingen.[214] Retningslinjene for forsvarlighetsvurderingen i forordningsforslaget artikkel 45(2) viser til flere forhold som ikke er nevnt i direktivet artikkel 25(2). En del av de nye retningslinjene i forordningsforslaget artikkel 45(2) reflekterer kravene som EU-domstolen stilte til Safe Harbor-beslutningen i Schrems-avgjørelsen. Kommisjonen skal blant annet vurdere beskyttelsesnivået basert på

> «*the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data […] as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred* » og «*the existence and effective functioning of one or more independent supervisory authorities […]*», jf. henholdsvis art. 45(2)(a) og (b).

Retningslinjene gjenspeiler Schrems-avgjørelsens fokus på personvern som en grunnleggende rettighet, herunder kravet til effektiv håndheving, se avsnitt 4.5.1.[215] Det fremgår dessuten av forordningsforslaget artikkel 45(3) at kommisjonen må sørge for kontroll med beskyttelsesnivået og vurdere utviklingen på stedet der forsvarlighetsvurderingen gjelder. Dette kravet ble også vektlagt i Schrems-avgjørelsen, se avsnitt 4.4.1.

Videre følger det av punkt 104 i fortalen til forordningsforslaget at for å gi et tilstrekkelig beskyttelsesnivå, burde tredjelandet ha et beskyttelsesnivå som er «*essentially equivalent*» til

---

214 COM(2015) 566 s. 13-14

215 Burton (2016)

det i EU. Dette uttrykket er det samme som EU-domstolen brukte for å presisere forsvarlighetsvurderingen i Schrems-avgjørelsen, og der er derfor nærliggende å se hen til den – om enn noe knappe – veiledningen som EU-domstolen gir om tolkningen av uttrykket, se avsnitt 4.4.1. Det kan bemerkes at selv om fortalen ikke er bindende, gir den veiledning for tolkningen av forordningen.

Det finnes imidlertid også eksempler på at forordningen regulerer spørsmål som EU-domstolen ikke eksplisitt tok stilling til i Schrems-avgjørelsen. Som nevnt i avsnitt 4.5.3 er det uavklart om kommisjonen har hjemmel til å beslutte at en bestemt gruppe i et land sikrer et tilstrekkelig beskyttelsesnivå etter personverndirektivet artikkel 25(6). Det fremgår derimot av den ovenfor siterte ordlyden i forordningsforslaget artikkel 45(1) at forordningen åpner for at kommisjonen kan godkjenne tredjeland, territorier eller sektorer i tredjelandet eller internasjonale organisasjoner.[216]

Rettspolitisk kan denne regelen i forordningsforslaget kritiseres for å lede til omgåelse av personvernet. Blume argumenterer for at særlig ved overføringer til bestemte territorier eller sektorer er det en risiko for at personvernlovgivningen i territoriet eller sektoren må vike for nasjonal rett, og at personopplysningene da ikke gis tilstrekkelig beskyttelse.[217]

Argumentet har likhetstrekk med de betraktningene EU-domstolen gjorde i Schrems-avgjørelsen rundt Safe Harbor-beslutningens begrensede rekkevidde og bestemmelsen om at Safe Harbor-prinsippene måtte vike for amerikansk rett, se avsnitt 4.5.2.2. Erfaringene med Safe Harbor-ordningen viste at det er vanskelig å finne et godt og holdbart system for å godkjenne bestemte aktører når regelverket i landet er grunnleggende ulikt fra EUs. Schrems-avgjørelsen kan dermed brukes som et argument for innskrenkende tolkning av kommisjonens kompetanse etter forordningen til å godkjenne andre aktører enn tredjeland som sådan.

Forordningen skiller seg også fra direktivet ved at den uttrykkelig regulerer både SCC og BCR, jf. forslaget art. 46 og 47. Det er særlig grunn til å bemerke at det ikke er tilstrekkelig etter forordningsforslaget artikkel 46 at «*the controller or processor has provided appropriate safeguards*», slik som SCC eller BCR. Det kreves i tillegg «*that enforceable data subject rights and effective legal remedies for data subjects are available*», jf. forordningsforslaget art. 46(1). Tilleggskravet ble tilføyd etter Schrems-avgjørelsen, og det er nærliggende å tolke

[216] Blume (2015) s. 36 flg., Kuner (2013) s. 47. Begge baserer seg på tidligere, men tilnærmet likelydende, forordningsforslag. Vurderingene er derfor trolig fremdeles relevante

[217] Blume (2015) s. 37-38

bestemmelsen i lys av de kravene Schrems-avgjørelsen stiller til registrertes prosessuelle rettigheter, se avsnitt 4.5.1.[218]

[218] Burton (2016)

6 Rettspolitiske vurderinger og veien videre

6.1 Rettspolitiske vurderinger rundt rettstilstanden for overføringer av personopplysninger til tredjeland etter Schrems-avgjørelsen

Problemstilling for dette delkapittelet er om Schrems-avgjørelsen realiserer formålene bak reglene om overføring av personopplysninger til tredjeland, se avsnitt 2.1. Drøftelsene ovenfor har vist at EU-domstolen går langt i å ivareta hensynet til personvern som en grunnleggende rettighet. Derimot kan man problematisere om domstolen legger for lite vekt på realpolitiske hensyn som taler for friere flyt av informasjon over landegrensene. Med de siste tiårenes teknologiske fremskritt kan informasjon enkelt sendes over landegrensene. Setter personverndirektivet unødvendige skranker for overføringer av personopplysninger mellom land? Av plasshensyn fokuserer oppgaven på to hensyn som var mindre fremtredende i Schrems-avgjørelsen: Å legge til rette for internasjonal handel og individers velferd.

Man kan argumentere for at reglene i personverndirektivet artikkel 25 og 26 går for langt i å begrense tredjelands muligheter til å handle med EU. Etter personverndirektivet artikkel 25 må et tredjeland i hovedregel ha et tilnærmet kvalitativt likt personvern som EU for å motta personopplysninger derfra. Samtidig følger det av Schrems-avgjørelsen at personvern er en grunnleggende rettighet i EU og at beskyttelsesnivået skal være høyt og effektivt.[219] Et tredjeland som ikke sikrer et tilstrekkelig beskyttelsesnivå, får utfordringer.

Aktører i tredjelandet kan benytte unntakene i direktivet artikkel 26. Som drøftet i avsnitt 5.1.2 er det derimot ikke gitt at BCR eller SCC er aktuelt, og unntakene i direktivet artikkel 26(1) skal heller ikke brukes over lengre tid, se avsnitt 2.3.3. Alternativt kan tredjelandet la være å motta personopplysninger fra EU. Imidlertid er EU en stor aktør på det internasjonale markedet og personopplysninger blir et stadig viktigere kommersielt gode. Man kan spørre hvilke land som reelt sett har denne muligheten. En tredje løsning er å etablere sentre for databehandling i EU.[220] Denne løsningen kan derimot være urealistisk av økonomiske eller andre praktiske grunner for eksempel for små virksomheter.

Alternativt kan tredjelandet endre lovgivingen sin til å samsvare med EUs krav til tilstrekkelig beskyttelsesnivå. Som nevnt i avsnitt 5.1.1 velger stadig flere land denne løsningen. Det er derimot ikke gitt at tredjeland, særlig utviklingsland, har ressurser til å implementere et system for beskyttelse av personvern som er tilnærmet likt EUs. Dessuten er det ikke alle land, slik som USA, som ønsker en slik tilnærming til personvern. Personverndirektivets regler om

[219] Ifølge Loideain (2016) s. 12 setter Schrems-avgjørelsen en uoppnåelig høy standard for personvern

[220] Kuner (2016) s. 31

overføring av personopplysninger kan dermed virke hemmende på internasjonal handel. Mindre handel kan gå utover insentiver til å gjøre teknologiske og forskningsmessige fremskritt.

Ivaretar Schrems-avgjørelsen individers velferd ved å prioritere hensynet til personvern som en grunnleggende rettighet? På overflaten kan det virke som en styrking av individets personvern også øker individets velferd. Man kan derimot argumentere for at et sterkere personvern indirekte kan få negative konsekvenser for individers velferd. For det første kan strenge regler om overføring av personopplysninger til tredjeland hindre individer i å dele opplysninger og utveksle synspunkter. Dette kan i neste omgang ha innvirkning på deres ytringsfrihet og sosiale og kulturelle utfoldelse. For eksempel kan en arbeidstaker i et EU-land ønske å kritisere arbeidsforholdene sine i et innlegg på Facebook. Dersom arbeidstakeren skriver om kollegene sine og det er mulig å identifisere dem, kan det tenkes at innlegget inneholder personopplysninger. I så fall kan det være i strid med personverndirektivet å publisere innlegget.[221]

For det andre kan Schrems-avgjørelsens strenge krav til personvern gjøre det vanskelig for selskaper i tredjeland å tilby tjenester som forutsetter behandling av personopplysninger i EU. Det er i dag et stort antall tjenester, særlig internettjenester, som for eksempel tilbys gratis mot at tilbyderen kan selge eller bruke brukernes personopplysninger. Dersom slike tjenester ikke lenger blir tilbudt til EU-borgere av hensyn til kravene til personvern, kan det få betydning for individenes velferd.

6.2 Den nye Safe Harbor-avtalen: EU-U.S. Privacy Shield

Siden 2014 har Europakommisjonen og amerikanske myndigheter forhandlet om et nytt rammeverk som kunne erstatte Safe Harbor-avtalen.[222] Schrems-avgjørelsen fungerte som en katalysator for å ferdigstille arbeidet. Den 2. februar 2016 kunngjorde Europakommisjonen og amerikanske myndigheter at de hadde blitt enige om et nytt rammeverk, EU-U.S. Privacy Shield, som skulle gi grunnlag for en ny forsvarlighetsvurdering for amerikanske selskaper.[223]

29. februar 2016 publiserte Europakommisjonen utkastet til en ny forsvarlighetsvurdering (heretter «Privacy Shield») som skulle erstatte Safe Harbor-beslutningen og gjenopprette tilliten til transatlantiske overføringer av personopplysninger etter Snowden-avsløringene.[224] Formålet med delkapitlet er å drøfte om Privacy Shield vil oppfylle kravene til «*essentially*

[221] Se til sammenligning case C-101/01 Lindqvist

[222] Europakommisjonen COM(2015) 566 s. 3

[223] IP/16/216

[224] Privacy Shield (2016), IP/16/433

equivalent» beskyttelsesnivå i lys av Schrems-avgjørelsen. Av hensyn til ordgrensen gis det kun en overordnet vurdering av noen aspekter ved det nye rammeverket.

6.2.1 Personvernprinsipper som skal ivareta grunnkravene i direktivet

I likhet med Safe Harbor-beslutningen innebærer Privacy Shield at amerikanske selskaper må være underlagt FTC eller DoTs myndighet, slutte seg til ordningen, implementere ulike personvernprinsipper og publisere personvernerklæringen sin.[225] Personvernprinsippene er «*notice*», «*choice*», «*accountability for onward transfer*», «*security*», «*data integrity and purpose limitation*», «*access*» og «*recourse, enforcement and liability* ».[226] Prinsippene er ifølge kommisjonen ment å etablere omfattende forpliktelser, gjennomsiktighet i behandlingen, kontroll og sanksjoner ved brudd på regelverket og strengere krav til videre overføringer av personopplysningene.[227]

Det kan imidlertid bemerkes at prinsippene hovedsakelig er de samme som i Safe Harbor-ordningen.[228] Derfor kan man argumentere for at kritikken av Safe Harbor-prinsippene fremdeles gjelder for Privacy Shield-prinsippene, se avsnitt 3.3. Prinsippene er riktignok noe mer detaljerte, og noen av dem inneholder også mer omfattende forpliktelser, slik som prinsippene om «*accountability for onward transfer*», og «*recourse, enforcement and liability*».[229]

Artikkel 29-arbeidsgruppen har derimot kritisert Privacy Shield for å utelate prinsippet om at personopplysninger ikke skal lagres lengre enn nødvendig.[230] Heller ikke Safe Harbor-beslutningen inneholdt et slikt prinsipp. Fordi EU-domstolen ikke vurderte Safe Harbor-prinsippene i Schrems-avgjørelsen, er det usikkert om dette vil være en mangel ved Privacy Shield-prinsippene. Likevel kan man spørre hvordan Privacy Shield kan nå opp til den høye terskelen for tilstrekkelig beskyttelsesnivå dersom ordningen ikke engang inkorporerer alle grunnprinsippene i personverndirektivet.

6.2.2 Effektiv håndheving og rettslig og administrativ prøving

Siden Privacy Shield viderefører Safe Harbor-beslutningens ordning med egenerklæringer, kan man problematisere om Privacy Shield sikrer effektive kontrollmekanismer for å identifi-

---

225 MEMO/16/434, Arthur Cox (2016) s. 1-2

226 Privacy Shield Annex II (2016) s. 4-7

227 MEMO/16/434

228 Se avsnitt 3.2, Arthur Cox (2016) s. 2

229 Hogan Lovells (2016) s. 23-24, Kuner (2016) s. 20

230 A29WP (2016)c s.17

sere og sanksjonere brudd på personvernprinsippene, se avsnitt 4.5.1. Privacy Shield legger mye vekt på håndheving og kontroll. Både Europakommisjonen og DoC skal jevnlig vurdere ordningen, det skal arrangeres årlige personvernkonferanser og kommisjonen skal utgi en årlig rapport.[231] Dessuten virker det ikke å være noen innskrenkninger i europeiske datatilsyns kompetanse til å behandle klager fra de registrerte.[232]

Videre satser Privacy Shield på å sikre effektiv beskyttelse av EU-borgernes rettigheter ved at det etableres flere muligheter for prøving av de registrertes klager på gjennomføringen av Privacy Shield. Selskapene som tar del i Privacy Shield, må svare på klager innen 45 dager, de registrerte må tilbys kostnadsfri alternativ tvisteløsning og de registrerte skal få mulighet til å kontakte sitt nasjonale datatilsyn, som vil samarbeide med DoC og FTC for å ordne opp i uløste klagesaker.[233] Privacy Shield etablerer også en voldgiftsløsning, «*Privacy Shield Panel*», som kan benyttes dersom tvisten ikke kan løses på andre måter.[234]

Tvisteløsningsmekanismene kan imidlertid kritiseres for å være for uoversiktlige til å sikre de registrerte effektiv prøving.[235] De registrerte må forholde seg til en håndfull aktører som har forskjellige prosedyrer og oppgaver. Privacy Shield kunne alternativt etablert ett organ som hadde det overordnede ansvaret for å behandle klager, slik som de europeiske datatilsynene har. Dessuten gir ikke tvisteløsningsmekanismene de registrerte rett til prøving ved amerikanske domstoler. Schrems-avgjørelsen kan leses som at for å oppfylle kravene i EU-charteret artikkel 47, kreves det i utgangspunktet at de registrerte kan få prøve saken sin for en domstol.[236]

I februar 2016 ble imidlertid *Judicial Redress Act* vedtatt i USA. Denne loven er ment å gi europeiske borgere en viss rett til å gå til sak om behandlingen av deres personopplysninger.[237] Man kan derimot problematisere om denne lovgivningen oppfyller de strenge kravene til domstolskontroll som følger av Schrems-avgjørelsen, se avsnitt 4.5.1. Rekkevidden av *Judicial Redress Act* er eksempelvis begrenset til å omfatte borgere fra land som ikke «*materially impede the national security interests of the United States*» og til kun å omfatte prøving av vedtak truffet av bestemte forvaltningsorganer, jf. Judicial Redress Act §§ 2(d)(1)(C), 2(e)(1).

---

231 MEMO/16/434

232 Hogan Lovells (2016) s. 41-42

233 MEMO/16/434

234 MEMO/16/434

235 A29WP (2016)c s. 26-27

236 Kuner (2016) s. 23

237 MEMO/16/434

Schrems-avgjørelsens krav til en uavhengig kontroll med myndighetsovervåkning implementeres ved at det opprettes et personvernombud i USA.[238] Man kan derimot problematisere om denne ombudsordningen vil oppfylle de europeiske standardene for uavhengighet fordi ombudet skal velges blant de som har stilling som «*Under Secretary*» i det amerikanske «*Department of State*».[239] Vedkommende er dermed ikke uavhengig fra den amerikanske regjeringen. Det er heller ikke gitt at kravet til uavhengighet ville vært oppfylt dersom ombudet var uten tilknytning til regjeringen. For å være uavhengig i henhold til EU-retten, må ombudet i tillegg blant annet ha kompetanse til å foreta selvstendige undersøkelser av grunnlaget for klagen og myndighet til å rette opp i lovstridige forhold dersom klagen fører frem.[240] Det fremgår ikke klart av Privacy Shield om personvernombudet vil ha tilstrekkelig innsyn i de amerikanske myndighetenes aktiviteter til å foreta selvstendige undersøkelser og i hvilken grad de amerikanske myndighetene er bundet av ombudets vurderinger.[241]

6.2.3 Klart og presist formulerte begrensninger og strengt nødvendige inngrep i personvernprinsippene

Privacy Shield vedlegg II I.5 har tilsvarende ordlyd som tidligere Safe Harbor vedlegg I fjerde avsnitt, som ble kritisert av EU-domstolen for å gi amerikanske myndigheter generell adgang til masseovervåkning, se avsnitt 4.5.2.2.[242] Oppfyller da Privacy Shield kravet til klart og presist formulerte og strengt nødvendige inngrep i personvernprinsippene?

Det kan bemerkes at det etter ordlyden i Privacy Shield vedlegg II I.5 ikke kreves at inngrep i personvernprinsippene er strengt nødvendige, i motsetning til hva som ble uttalt i Schrems-avgjørelsen, se avsnitt 4.5.2.1. Hogan Lovells argumenterer likevel for at inngrepene som Privacy Shield åpner for, er forholdsmessige og strengt nødvendige: Overvåkning er blant annet kun tillatt i bestemte tilfeller og for bestemte formål og for et bestemt tidsrom, nasjonale sikkerhetsmyndigheter må anvende de minst inngripende tiltakene.[243] Disse skrankene følger hovedsakelig av to grunnlag.

For det første har et utvalg av høytstående individer i den amerikanske regjeringen gitt skriftlige forsikringer om vern mot og begrensninger i myndighetenes adgang til personopplys-

238 MEMO/16/434

239 A29WP (2016)c s. 49

240 A29WP (2016)c s. 50

241 A29WP (2016)c s. 50-51

242 Privacy Shield Annex II (2016) s. 2

243 Hogan Lovells (2016) s. 43-45

ninger fra europeiske borgere.[244] Det kan problematiseres om slike forsikringer er klare, presise og tilgjengelige regler i henhold til Schrems-avgjørelsens krav og om de i det hele tatt kan tillegges noen rettslig betydning. Det er for eksempel uklart om europeiske borgere kan bygge et krav på brudd på forsikringene. Kuner mener dessuten at mange av forsikringene kan endres eller trekkes tilbake av de som gav dem.[245] Det tyder på at forsikringene primært har en politisk funksjon. Videre er det usikkert om forsikringene har virkning for andre enn den sittende administrasjonen i USA. Det er presidentvalg i USA i 2016, og det er ikke gitt at den nye administrasjonen vil ha samme syn på Privacy Shield.

For det andre har president Obama utstedt *Presidential Policy Directive 28* («PPD-28»), som begrenser etterretningsmyndighetenes innhenting av personopplysninger.[246] Kommisjonen tolker PPD-28 som bindende for de amerikanske etterretningsmyndighetene, også ved regjeringsskifte.[247] Dersom forsikringene fra de amerikanske myndighetene som ble diskutert i forrige avsnitt, ikke er bindende, kan man stille spørsmål ved om de kravene til behandlingen av personopplysninger som følger av PPD-28 i seg selv sikrer tilstrekkelige begrensninger for myndighetenes overvåkning.

Selv om forsikringene fra amerikanske myndigheter og PPD-28 skulle angi klare og presise begrensninger for adgangen til personopplysninger, kan det argumenteres for at Privacy Shield likevel ikke går langt nok i å hindre amerikanske myndigheters adgang til elektronisk kommunikasjon. I Schrems-avgjørelsen understreket EU-domstolen at muligheten for slik masseovervåkning var i strid med kjernen i EU-charteret artikkel 7, se avsnitt 4.5.2.3. Europakommisjonen har gitt uttrykk for at Privacy Shield ikke åpner for slik overvåkning.[248] Kuner poengterer likevel at

> «*On the one hand, […] the US notes that under US law, bulk collection of data or mass surveillance is "prohibited". On the other hand, the US also states in the documentation that "signals intelligence collected in bulk can only be used for six specific purposes", and that "any bulk collection activities regarding Internet communications that the U.S. Intelligence Community performs through signals intelligence operate on a small proportion of the Internet", suggesting that bulk collection does occur*» (forfatterens fotnoter er utelatt).[249]

---

244 MEMO/16/434

245 Kuner (2016) s. 22

246 MEMO/16/434

247 Privacy Shield (2016) fortalen (57)

248 MEMO/16/434

249 Kuner (2016) s. 21

Kuner legger altså til grunn at Privacy Shield fremdeles gir amerikanske etterretningsmyndigheter en viss adgang til masseovervåkning av elektronisk kommunikasjon. Samtidig tolker han Schrems-avgjørelsen som at EU-charteret artikkel 7 forbyr *enhver* generell adgang til elektronisk kommunikasjon.[250] I så fall oppfyller ikke Privacy Shield kravene til tilstrekkelig beskyttelsesnivå etter Schrems-avgjørelsen.

6.2.4 Veien videre

Før Privacy Shield eventuelt kan vedtas, må utkastet gjennom prosedyren for forsvarlighetsvurderinger. Det kan imidlertid allerede nå spørres om Privacy Shield rettspolitisk sett er en hensiktsmessig måte å regulere transatlantiske overføringer av personopplysninger.

Privacy Shield viderefører i stor grad Safe Harbor-beslutningen, og EU og USA har fremdeles grunnleggende ulik tilnærming til personvern. Det er derfor trolig at EU-domstolen vil prøve om Privacy Shield tilfredsstiller kravene i Schrems-avgjørelsen. Det kan ta år før saken blir avgjort i domstolen, og i mellomtiden forblir det usikkerhet rundt fortolkningen av regelverket for transatlantiske overføringer av personopplysninger.

Dersom EU-domstolen skulle komme til at Privacy Shield ikke oppfyller kravene i Schrems-avgjørelsen, vil det kreve tid og ressurser både for EU og USA å bli enige om enda en ny ordning. I tillegg har Snowden-avsløringene allerede svekket tilliten til transatlantiske overføringer, og det er ikke sikkert at den tredje ordningen vil kunne gjenopprette tilliten.

I lys av erfaringene med Safe Harbor-avtalen kan man også spørre om EUs regler om overføring av personopplysninger er for inngripende i andre lands regulering av personvern. Tendensen er at EUs ordning med krav til tilstrekkelig beskyttelsesnivå får stadig større utbredelse gjennom Brussel-effekten, se avsnitt 5.1.1. Det blir mindre rom for andre tilnærminger til personvern, som USAs sektorspesifikke og mindre inngripende lovregulering. Er det ønskelig at EUs standard og tilnærming til personvern gradvis blir den eneste akseptable? Man kan spørre om tiden heller er moden for å utarbeide en internasjonal og bindende konvensjon som harmoniserer personvernstandarden globalt.

En fordel med en internasjonal avtale er at flere aktører, for eksempel fra asiatiske og afrikanske land, kan bli representert. I tillegg kan partene forhandle om en personvernstandard som åpner for andre tilnærminger til personvern enn EUs. En internasjonal regulering av

[250] Kuner (2016) s. 21

overføringer av personopplysninger fremmer også synet på personvern som en grunnleggende rettighet; grunnleggende rettigheter bør sikre individer en viss beskyttelse uansett hvor de befinner seg. Det er ikke utenkelig at avtalen ville bli et minste felles multiplum og at personvernstandarden blir lavere enn gjeldende rett i EU. Likevel får man et felles, internasjonalt utgangspunkt for videreutviklingen av reglene om overføring av personopplysninger mellom land.

Det er imidlertid ikke uproblematisk å utarbeide en slik internasjonal avtale. Bygrave har blant annet problematisert hvordan avtalen skal balansere ulike aspekter ved personvern, som menneskerettigheter, handel og nasjonal sikkerhet.[251] Kuner mener dessuten det vil ta lang tid, opptil flere tiår, å bli enige om en avtale, og avtalen kan derfor vanskelig holde følge med utviklingen i sedvane og teknologi.[252]

Begge teoretikere stiller også spørsmål ved hvilket organ som kan sørge for at det blir fremforhandlet en avtale med klare forpliktelser, selv om de synes positive til å ta utgangspunkt i Europarådets personvernkonvensjon.[253] Personvernkonvensjonen har imidlertid den samme svakheten som personverndirektivet fordi den er utformet fra et europeisk ståsted som ikke nødvendigvis åpner for et bredt spekter av måter å regulere personvern.

Selv om det synes problematisk å forhandle frem en internasjonal, bindende avtale som forener de ulike tilnærmingene og standardene for personvern, kan man i alle tilfeller argumentere for at tiden er moden for at land utenfor EU og EØS får mulighet til å utfordre Brusseleffekten og EUs innflytelse over internasjonale overføringer av personopplysninger.

[251] Bygrave (2014) s. 206

[252] Kuner (2013) s. 162

[253] Bygrave (2014) s. 206, Kuner (2013) s. 163

7 Oppsummering

En rød tråd i Schrems-avgjørelsen er kravet til et høyt og effektivt beskyttelsesnivå for behandling av personopplysninger som følge av at personvern er en grunnleggende rettighet i EU-retten. Avhandlingen har vist at det særlig er to forhold som er bakteppet for kravet: Fokuset på myndigheters masseovervåkning i lys av Snowden-avsløringene og personvernets sterke forankring i EU-retten gjennom EU-charteret.

Avhandlingen har videre argumentert for at Schrems-avgjørelsen er et ledd i en pågående utvikling i europeisk rettspraksis hvor personopplysninger gis en stadig sterkere og mer omfattende beskyttelse. Samtidig har avhandlingen drøftet om domstolen fra et rettspolitisk synspunkt legger for stor vekt på personvern som grunnleggende rettighet på bekostning av andre hensyn bak reglene om overføring av personopplysninger til tredjeland.

I tillegg har oppgaven argumentert for at det kan utledes flere rettssetninger fra Schrems-avgjørelsen som gir veiledning for hvordan man skal tolke både personverndirektivets og personvernforordningens regler om overføring av personopplysninger til tredjeland. Fordi det er få avgjørelser fra EU-domstolen som avklarer hvordan reglene om overføring av personopplysninger til tredjeland skal tolkes, vil Schrems-avgjørelsen trolig få betydning for tolkningen av disse reglene, både hva gjelder forsvarlighetsvurderinger og alternative overføringsmåter.

Videre har avhandlingen fokusert på årsakene til at Safe Harbor-beslutningen ble erklært ugyldig. Beslutningen var kritisert, og det var derfor ikke uventet at den ble erklært ugyldig i Schrems-avgjørelsen. Særlig mangelen på effektiv kontroll var en gjenganger både i kritikken og i Schrems-avgjørelsen. Derimot viser drøftelsene ovenfor at beslutningen ble erklært ugyldig også av grunner som var lite fremtredende i kritikken: Kravet til formell konstatering og innskrenkningen av de nasjonale tilsynsmyndighetenes kompetanse. Domstolen gikk derimot ikke inn på innholdet i Safe Harbor-prinsippene, som var kritisert forut for Schrems-avgjørelsen.

Det gjenstår å se om Privacy Shield vil lide samme skjebne som sin forgjenger. Oppgaven har vist at det er usikkert om ordningen fullt ut tilfredsstiller Schrems-avgjørelsens krav. Samtidig har avhandlingen åpnet for diskusjon rundt alternativer til EUs tilnærming til overføringer av personopplysninger over landegrensen. Regulering av overføringer av personopplysninger mellom land har internasjonale implikasjoner, og det er derfor hensiktsmessig å vurdere en internasjonal harmonisering av de nasjonale regelverkene.

Litteraturliste

Internasjonalt og nasjonalt lov- og forarbeidsregister

Traktater

EMK — Convention for the Protection of Human Rights and Fundamental Freedoms, 4. november 1950. Sitert fra Lovdata

OECDs personvernretningslinjer — OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal data, 23. september 1980. Tilgjengelig på http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [sitert 21.04.16]

Europarådets personvernkonvensjon — Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108), 28. januar 1981. Tilgjengelig på http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm [sitert 21.04.16]

EU-charteret — Charter of Fundamental Rights of the European Union, 7. desember 2000. Sitert fra EUR-LEX

TEUV — Consolidated version of the Treaty on the Functioning of the European Union, 13. desember 2007. Sitert fra EUR-LEX

Sekundærlovgivning

Direktiv 95/46/EC — *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (personverndirektivet). Sitert fra EUR-LEX

Forordningsforslag av 6. april 2016 — *Position of the Council at first reading with a view to the adoption of a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* (forordningsforslaget), 6. april 2016. Sitert fra EUR-LEX

Norsk lovgivning

1992 — Lov 27. november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven). Sitert fra Lovdata

2000 — Lov 14. april 2000 nr. 31 om behandling av personopplysninger (Personopplysningsloven). Sitert fra Lovdata

2000 — Forskrift 15. desember 2000 nr. 1265 om behandling av personopplysninger (personopplysningsforskriften). Sitert fra Lovdata

Norske forarbeider

Ot.prp.nr. 92 (1998-1999) — *Om lov om behandling av personopplysninger (personopplysningsloven).* Sitert fra Lovdata

St.prp. nr. 34 (1999-2000) — *Om samtykke til godkjenning av EØS-komiteens beslutning nr. 83/1999 av 25. juni 1999 om endring av EØS-avtalens protokoll 37 og vedlegg XI (telekommunikasjonstjenester).* Sitert fra Lovdata

Offentlige amerikanske dokumenter

Safe Harbor (2000) — Issuance of Safe Harbor Principles and

Transmission to European Commission; Notice, 24. juli 2000. Tilgjengelig på https://www.gpo.gov/fdsys/pkg/FR-2000-07-24/pdf/00-18489.pdf [sitert 21.04.16]

Judicial Redress Act — Judicial Redress Act of 2015, Public Law 114-126, 24. februar 2016. Tilgjengelig på https://www.congress.gov/114/plaws/publ126/PLAW-114publ126.pdf [sitert 21.04.16]

Domsregister

EU-domstolen og domstolens generaladvokater

Case C-465/00 Rechnungshof — Joined cases Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk, 20. mai 2003, ECLI:EU:C:2003:294

Case C-101/01 Lindqvist — Case C-101/01 Criminal proceedings against Bodil Lindqvist, 6. november 2003, ECLI:EU:C:2003:596

Case C-524/06 Huber — Case C-524/06 Heinz Huber v Bundesrepublik Deutschland, 16. desember 2008, ECLI:EU:C:2008:724

Case C-73/07 Satamedia — Case C-73/07 Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, 16. desember 2008, ECLI:EU:C:2008:727

Case C-92/09 Schecke — Joined cases Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen, 9. november 2010, ECLI:EU:C:2010:662

Case C-473/12 IPI — Case C-473/12 Institut professionnel des agents immobiliers (IPI) v Geoffrey Eng-

	lebert and Others, 7. november 2013, ECLI:EU:C:2013:715
Case C-293/12 Digital Rights Ireland	Joined cases Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others, 8. april 2014, ECLI:EU:C:2014:238
Case C-131/12 Google Spain	Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 13. mai 2014, ECLI:EU:C:2014:317
Case C-212/13 Ryneš	Case C-212/13 František Ryneš v Úřad pro ochranu osobních údajů, 11. desember 2014, ECLI:EU:C:2014:2428
Case C-362/14 Schrems	Case C-362/14 Maximillian Schrems v Data Protection Commissioner, 6. oktober 2015, ECLI:EU:C:2015:650
Generaladvokat Bot (2015)	*OPINION OF ADVOCATE GENERAL BOT delivered on 23 September 2015 Case C-362/14 Maximillian Schrems v Data Protection Commissioner*, sitert fra CURIA

Den europeiske menneskerettsdomstol

Klass and Others v. Germany	Case of Klass and Others v. Germany. Application no. 5029/71, 6. september 1978. Sitert fra HUDOC
Szabó and Vissy	Case of Szabó and Vissy v. Hungary. Application no. 37138/14, 12. januar 2016. Sitert fra HUDOC

Andre EU- og EØS-rettslige kilder

Europakommisjonen

Decision 2000/520/EC	*Commission Decision of 26 July 2000 pursu-*

	ant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (Safe Harbor-beslutningen). Sitert fra EUR-LEX
COM(2013) 846	*COM(2013) 846 final, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, Rebuilding Trust in EU-US Data Flows*, 27. november 2013. Tilgjengelig på http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf [sitert 21.04.16]
COM(2013) 847	*COM(2013) 847 final, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, 27. november 2013. Tilgjengelig på http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf [sitert 21.04.16]
COM(2015) 566	*COM(2015) 566 final, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)*, 6. november 2015. Tilgjengelig på http://ec.europa.eu/justice/data-protection/international-

transfers/adequacy/files/eu-us_data_flows_communication_final.pdf [sitert 21.04.16]

IP/16/216 — *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield*, 2. februar 2016. Tilgjengelig på http://europa.eu/rapid/press-release_IP-16-216_en.htm [sitert 21.04.16]

IP/16/433 — *Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield*, 29. februar 2016. Tilgjengelig på http://europa.eu/rapid/press-release_IP-16-433_en.htm [sitert 21.04.16]

MEMO/16/434 — *EU-U.S. Privacy Shield: Frequently Asked Questions*, 29. februar 2016. Tilgjengelig på http://europa.eu/rapid/press-release_MEMO-16-434_en.htm [sitert 21.04.16]

Privacy Shield (2016) — *COMMISSION IMPLEMENTING DECISION of XXX pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, 29. februar 2016. Tilgjengelig på http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf [sitert 21.04.16]

Privacy Shield Annex II (2016) — *Annex II, EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce*, 29. februar 2016. Tilgjengelig på http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-

decision-annex-2_en.pdf [sitert 21.04.16]

Europaparlamentet

Resolution A5-0177/2000 — *REPORT on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce (C5-0280/2000 - 2000/2144(COS))*, 22. juni 2000. Tilgjengelig på http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/0117-02_en.pdf [sitert 21.04.16]

EØS-komiteen

EØS-komiteen (1999) — *Decision of the EEA Joint Committee No 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI (Telecommunication services) to the EEA Agreement*. Sitert fra EUR-LEX

EØS-komiteen (2000) — *Decision of the EEA Joint Committee No 108/2000 of 30 November 2000 amending Annex XI (Telecommunication services) to the EEA Agreement*. Sitert fra EUR-LEX

Artikkel 29-arbeidsgruppen

A29WP (1998) — *Working Document, Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, 24. juli 1998. Tilgjengelig på http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf [sitert 21.04.16]

A29WP (2000) — *Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles"*,

16. mai 2000. Tilgjengelig på http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp32_en.pdf [sitert 21.04.16]

A29WP (2005) *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 199*, 25. november 2005. Tilgjengelig på http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf [sitert 21.04.16]

A29WP (2015) *Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14)*, 16. oktober 2015. Tilgjengelig på http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf [sitert 21.04.16]

A29WP (2016)a *Statement of the Article 29 Working Party on the Consequences of the Schrems* Judgment, 3. februar 2016. Tilgjengelig på http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf [sitert 21.04.16]

A29WP (2016)b *Statement of the Article 29 Working Party on the Presentation by the European Commis-*

sion of the EU-U.S. Privacy Shield, 29. februar 2016. Tilgjengelig på http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160229-press-rel_publication_europeancommission_eu-us_privacy_shield.pdf [sitert 21.04.16]

A29WP (2016)c — *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, 13. april 2016. Tilgjengelig på http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf [sitert 21.04.16]

A29WP (2016)d — *Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures*, 13. april 2016. Tilgjengelig på http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf [sitert 21.04.16]

Litteratur

Bøker

Arnesen (2015) — Arnesen, Finn og Are Stenvik, *Internasjonalisering og juridisk metode*, 2. utgave, 2015, Universitetsforlaget

Büllesbach (2010) — Büllesback, Alfred (red.), *Concise European IT Law*, 2. utgave, 2010, Kluwer Law International

Bygrave (2002) — Bygrave Lee Andrew, *Data Protection La:*

Approaching Its Rationale, Logic and Limits, 2002, Kluwer Law International

Bygrave (2014) — Bygrave, Lee Andrew, *Data Privacy Law: An International Perspective*, 2014. Oxford Scholarship Online. DOI:10.1093/acprof:oso/9780199675555.001.0001

Craig (2008) — Craig, Paul and Gráinne De Búrca, *EU law: Text, cases and materials*, 4. utgave, 2008, Oxford University Press

Determann (2015) — Determann, Lothar, *Determann's Field Guide to Data Privacy Law*, 2. utgave, 2015, Edward Elgar

Fredriksen (2014) — Fredriksen, Halvard Haukeland og Gjermund Mathisen, *EØS-rett*, 2. utgave 2014, Fagbokforlaget

Heisenberg (2005) — Heisenberg, Dorothee, *Negotiating Privacy*, 2005, Lynne Rienner

Kuner (2013) — Kuner, Christopher, *Transborder Data Flows and Data Privacy Law*, 2013, Oxford Scholarship Online. DOI:10.1093/acprof:oso/9780199674619.001.0001

Sejersted (2011) — Sejersted, Fredrik, Finn Arnesen, Ole-Andreas Rognstad, Olav Kolstad m.fl., *EØS-rett*, 3. utgave, 2011, Universitetsforlaget

Schartum (2011) — Schartum, Dag Wiese og Lee Andrew Bygrave, *Personvern i informasjonssamfunnet*, 2. utgave, 2011, Fagbokforlaget

Tønseth (2016) — Tønseth, Malin, Marit Stubø, Thomas Olsen

og Rune Ljostad, *Personvernhåndboken*, 2016, Gyldendal juridisk

Artikler

Bagger Tranberg (2011) — Bagger Tranberg, Charlotte, «Proportionality and data protection in the case law of the European Court of Justice», *International Data Privacy Law* vol. 1 nr. 4 (2011), s. 239-248, sitert fra Oxford Journals

Bing (2014) — Bing, Jon, «Overføring av personopplysninger til utlandet – noen grunnleggende problemstillinger», *Lov og rett* (2014), s. 127-146, sitert fra Lovdata

Blume (2015) — Blume, Peter, «EU adequacy decisions: the proposed new possibilities », *International Data Privacy Law* vol. 5 nr. 1 (2015), s. 34-39

Bourgeois (2016) — Bourgeois, Jaques, Cameron F. Kerry, William R. M. Long og Maarten Meulenbelt m.fl., «Essentially Equivalent: A Comparison of the Legal Orders for Privacy and Data Protection in the European Union and United States», *Sidley Austin LLP* (2016). Tilgjengelig på http://www.sidley.com/~/media/publications/essentially-equivalent---final.pdf [sitert 21.04.16]

Colonna (2014) — Colonna, Liane, «Article 4 of the EU Data Protection Directive and the irrelevance of the EU-US Safe Harbor Program?», *International Data Privacy Law* vol. 4 nr. 3 (2014), s. 203-221

Connolly (2008) — Connolly, Chris, «The US Safe Harbor – Fact or Fiction? », *Galexia* (2008).

Tilgjengelig på http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/08_galexia_safe_harbor_/08_galexia_safe_harbor_en.pdf [sitert 21.04.16]

Kuner (2016) — Kuner, Christopher, «Reality and Illusion in EU Data Transfer Regulation Post Schrems», *University of Cambridge Faculty of Law Research Paper* nr. 14 (2016). Tilgjengelig på http://ssrn.com/abstract=2732346 [sitert 21.04.16]

Loideain (2016) — Loideain, Nora Ni, «The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law», *Journal of Internet Law* vol. 19, nr. 8 (2016) s. 1, 8-14. Tilgjengelig på http://ssrn.com/abstract=2734698 [sitert 21.04.16]

Reidenberg (2001-2002) — Reidenberg, Joel R., «E-Commerce and Trans-Atlantic Privacy», *Houston Law Review* vol. 38, nr. 3 s. 717-750 (2001-2002). Tilgjengelig på http://ir.lawnet.fordham.edu/faculty_scholarship/38 [sitert 21.04.16]

Shaffer (2000) — Shaffer, Gregory, «Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards», *Yale Journal of International Law*, vol. 25 (2000), s. 1-88, sitert fra HeinOnline

Svantesson (2011) — Svantesson, Dan Jerker B., «The regulation of cross-border data flows», *International Data Privacy Law* vol. 1 nr. 3 (2011), s. 180-198, sitert fra Oxford Journals

Treacy (2014) — Treacy, Bridget og Anita Bapat, Hunton & Williams, «Scrapping Safe Harbor: European scare mongering or a real possibility?», *Privacy & Data Protection*, vol. 15 nr. 2 (2014), s. 4-6, sitert fra Westlaw UK

Weber (2013) — Weber, Rolf H., «Transborder data transfers: concepts, regulatory approaches and new legislative initiatives», *International Data Privacy Law*, vol. 4 nr. 2 (2013), s. 117-130

Nettsider

Al Tamimi & Co. (2016) — Al Tamimi & Co., *European Court of Justice Decision Impacts on DIFC Data Protection* (2016), http://www.tamimi.com/en/magazine/law-update/section-14/december-january-3/european-court-of-justice-decision-impacts-on-difc-data-protection.html [sitert 21.04.16]

Arthur Cox (2016) — Arthur Cox, *Privacy Shield Update* (2016), http://www.arthurcox.com/wp-content/uploads/2016/03/Privacy-Shield-Update-March-2016.pdf [sitert 21.04.16]

Burton (2016) — Burton, Cedric, Laura De Boel, Christopher Kuner og Anna Pateraki m.fl., *The Final European Union General Data Protection Regulation* (2016), http://www.bna.com/final-european-union-n57982067329/ [sitert 21.04.16]

Europakommisjonen (2015) — Europakommisjonen, *Model Contracts for the transfer of personal data to third countries* (2015), http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm [sitert

21.04.16]

Europakommisjonen (2016)a — Europakommisjonen, *EU Charter of Fundamental Rights* (2016), http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm [sitert 21.04.16]

Europakommisjonen (2016)b — Europakommisjonen, *Commission decisions on the adequacy of the protection of personal data in third countries* (2016), http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm [sitert 21.04.16]

Export.gov (2016) — Export.gov, *The U.S.-EU Safe Harbor Framework* (2016), http://www.export.gov/safeharbor/ [sitert 21.04.16]

Hogan Lovells (2016) — Hogan Lovells, *Legal Analysis of the EU-U.S: Privacy Shield* (2016), http://www.hoganlovells.com/files/Uploads/Documents/Privacy%20Shield%20Legal%20Analysis%20by%20Hogan%20Lovells%20(2016-03-31).pdf [sitert 31.3.16]. Arkivert utgave tilgjengelig på http://goo.gl/StIvG2 [sitert 22.04.16]

Restad (2015) — Restad, Hilde, *Edward Snowden* (2015), Store norske leksikon. Tilgjengelig på https://snl.no/Edward_Snowden [sitert 21.04.16]