JURIDISKA FAKULTETEN
vid Lunds universitet

Sofie Wändahl

Skyddsnivån på andra sidan vattnet

- *Om bedömningen av tredjelands skyddsnivå vid överföring av personuppgifter*

JURM02 Examensarbete

Examensarbete på juristprogrammet
30 högskolepoäng

Handledare: Marja-Liisa Öberg

Termin för examen: Period 1 VT2021

Innehåll

Summary

The EU is by many considered to have one of the world's strictest regulations for data protection. However, the Union and its Member States, like the rest of the world, have an interest in being able to transfer personal data to third countries due to global and technological developments. In order to balance the high level of privacy protection against the interest in transferring personal data to third countries, the General Data Protection Regulation contains various mechanisms for carrying out such transfers. One of the options provides the Commission with the possibility to decide that a country ensures an adequate level of protection, which allows for free transfers to that country. The European Court of Justice recently declared, for the second time, such a decision regarding transfers to the United States to be invalid, which shows that the assessment of the level of protection of third countries is not entirely straightforward. In addition, an assessment process of the UK's level of protection is currently under way, due to the country's withdrawal from the Union. This essay mainly aims to examine how the assessment of the level of protection in third countries relates to the level of protection under EU law, and what challenges arise from such an assessment. The investigation has been carried out using the legal dogmatic and the EU legal method and includes a presentation of relevant legislation, a review of the European Court of Justice's case law regarding adequacy decisions and restrictions on privacy protection, and finally a review of the draft decision for the United Kingdom.

When assessing whether third countries ensure an adequate level of protection of personal data, the European Commission shall investigate all circumstances that to some extent affect the protection of personal data. For example, the Commission should look at the country's privacy framework, supervisory mechanisms, access to justice and the public authorities' access to personal data. In its rulings on the level of protection of the United States, the European Court of Justice states that a level of protection in third countries does not have to be identical to that of the Union, only essentially equivalent.

In addition, according to the Court, national surveillance programs without clear objectives, restrictions or safeguard measures constitute such a measure which is in conflict with the principle of proportionality, and the level of protection should not be considered adequate in such circumstances. The Commission considers that the United Kingdom ensures an adequate level of protection. According to the European Data Protection Board, however, there are a number of circumstances that make it possible to question such a claim. For example, the United Kingdom also conducts extensive surveillance, and is also a party to international agreements that enable further transfers to countries that have been considered not to ensure an adequate level of protection, such as the U.S.

The concept of "essentially equivalent level of protection" suggests that the level of protection of third countries does not need to be identical to the level of protection of the EU. However, the scope for deviating from the EU legal level is not entirely clear. The far limit of what is considered acceptable seems to be whether a decision on an adequate level of protection would risk violating the essential content of fundamental rights under the EU Charter. A challenge in assessing the level of protection of third countries is the ability of the European Court of Justice to deal with third country legislation. Another challenge arises when the Court has to assess the level of protection in an area where legislation is not harmonized within the EU, such as national security. In its rulings, the European Court of Justice has placed high demands on what should be considered an adequate level of protection, and it is possible that these requirements create obstacles to the EU's cooperation with third countries with regard to data transmissions.

Sammanfattning

EU anses av många ha en av världens strängaste regleringar för dataskydd. Unionen och dess medlemsstater har dock, likt resten av världen, i och med den globala och tekniska utvecklingen ett intresse av att kunna överföra personuppgifter till tredjeländer. I syfte att balansera det höga integritetsskyddet mot intresset av att överföra personuppgifter till tredjeland, finns i dataskyddsförordningen olika mekanismer för att kunna utföra sådana överföringar. Ett av alternativen tillhandahåller kommissionen möjligheten att fatta beslut om att ett land säkerställer en adekvat skyddsnivå, vilket möjliggör fria överföringar till det landet. Nyligen meddelade EU-domstolen, för andra gången, att ett sådant beslut gällande överföringar till USA ogiltigförklarades, vilket visar på att bedömningen av tredjelands skyddsnivå inte är helt okomplicerad. I dagsläget pågår dessutom en bedömningsprocess av Storbritanniens skyddsnivå, på grund av landets utträde ur unionen. Denna uppsats syftar huvudsakligen till att undersöka hur bedömningen av skyddsnivån i tredjeland förhåller sig till den EU-rättsliga skyddsnivån, samt vilka utmaningar som följer av en sådan bedömning. Utredningen har genomförts med hjälp av den rättsdogmatiska samt EU-rättsliga metoden och innefattar presentation av relevant lagstiftning, genomgång av EU-domstolens praxis vad gäller begränsningar av integritetsskyddet samt adekvansbeslut och slutligen en genomgång av förslaget till beslut för Storbritannien.

Vid bedömning av om tredjeland säkerställer en adekvat skyddsnivå för personuppgifter, ska EU-kommissionen utreda alla omständigheter som i någon mån påverkar skyddet för personuppgifter. Till exempel ska kommissionen se till landets integritetsrättsliga ramar, tillsynsmekanismer, tillgången till rättsmedel samt vilken åtkomst som offentliga myndigheter har till personuppgifter. I avgörandena om USA:s skyddsnivå, uppger EU-domstolen att en skyddsnivå i tredjeland inte behöver vara identisk med unionens utan endast väsentligen likvärdig. Enligt domstolen utgör dessutom

nationella övervakningsprogram utan tydliga syften, begränsningar eller skyddsåtgärder en sådan åtgärd som står i strid med proportionalitetsprincipen, och skyddsnivån ska under sådana omständigheter inte anses adekvat. Kommissionen anser att Storbritannien säkerställer en adekvat skyddsnivå. Enligt europeiska dataskyddstyrelsen föreligger dock ett flertal omständigheter som möjliggör ett ifrågasättande av ett sådant påstående. Till exempel bedriver även Storbritannien omfattande övervakning, och är dessutom part i internationella avtal som möjliggör vidare överföring till länder som inte ansetts säkerställa en adekvat skyddsnivå, som till exempel USA.

Begreppet ”väsentligen likvärdig skyddsnivå” antyder att tredjelands skyddsnivå inte behöver vara identisk med EU:s skyddsnivå. Vilket utrymme som finns för avsteg från den EU-rättsliga nivån, är dock inte helt klarlagt. Den bortre gränsen för vad som anses godtagbart verkar bestämmas av huruvida ett beslut om adekvat skyddsnivå skulle riskera att kränka det väsentliga innehållet i de grundläggande rättigheterna enligt EU-stadgan. En utmaning med att bedöma tredjelands skyddsnivå är EU-domstolens förmåga att behandla tredjelands lagstiftning. Ytterligare en utmaning framträder när domstolen ska bedöma skyddsnivån på ett område där lagstiftningen inte är harmoniserad inom EU, som till exempel nationell säkerhet. EU-domstolen har i och med sina avgöranden satt höga krav på vad som ska anses utgöra en adekvat skyddsnivå, och det är möjligt att dessa krav skapar hinder för EU:s samarbete med tredjeländer vad gäller dataöverföringar.

Förord

I och med inlämnandet av denna uppsats avslutar jag nu fem års studier och en fantastisk tid i Lund. Att skriva uppsatsen har varit krävande, inte minst med tanke på rådande pandemi och dess följder. Jag vill därför särskilt tacka min handledare, Marja-Liisa Öberg, för stöd och väldigt värdefulla synpunkter längs vägen.

De senaste fem åren har varit utmanande och stundvis tuffa. Därför vill jag också säga tack till mina älskade föräldrar. Tack för att ni har funnits och stått bakom mig, och alltid haft era dörrar öppna för mig att komma hem till.

Jag vill också tacka er, Erik, My, Julia och Anna, för att ni har stöttat, peppat och kramat hela vägen igenom.

Tack till mina älskade vänner från Lunds Nation, för att ni visade och påminde mig om att det finns ett liv utanför Juridicums väggar.

Tack till Ida och Amanda för att ni är ni, det vill säga otroliga.

Tack till O, för att du alltid har stått redo med pussar och kramar när så behövts. Jag älskar dig för det.

Slutligen vill jag tacka mig själv. Tack för att jag orkade, även när jag egentligen inte gjorde det.

Sofie

Lund, 25 maj 2021

Förkortningar

Art. 29-gruppen	Arbetsgruppen för skydd av enskilda med avseende på behandling av personuppgifter
CLOUD Act	Clarifying Lawful Overseas Use of Data Act *(USA)*
DPA 2018	Data Protection Act 2018 *(Storbritannien)*
E.O. 12333	Executive Order 12333 *(USA)*
EDPB	European Data Protection Board
EKMR	Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna
EG	Europeiska gemenskapen
EU	Europeiska unionen
EU-domstolen	Europeiska unionens domstol
EU-kommissionen	Europeiska kommissionen
EU-stadgan	Europeiska unionens stadga om de grundläggande rättigheterna
Europadomstolen	Europeiska domstolen för de mänskliga rättigheterna
FISA	Foreign Intelligence Surveillance Act *(USA)*
FoS	Frågor och svar *(i anslutning till beslutet om Safe Harbor)*
GCHQ	Government Communications Headquarters *(Storbritannien)*
GDPR	General Data Protection Regulation
IC	Information Commissioner *(Storbritannien)*
ICO	Information Commissioner's Office *(Storbritannien)*
IPA 2016	Investigatory Powers Act 2016 *(Storbritannien)*
NSA	National Security Agency *(USA)*

OECD	Organisation for Economic Co-operation and Development
PPD-28	Presidential Policy Directive 28 *(USA)*
UK GDPR	United Kingdom General Data Protection Regulation

1 Inledning

1.1 Bakgrund

2018 trädde en ny dataskyddsförordning i kraft inom EU.[1] Förordningen syftar till att harmonisera medlemsstaternas dataskyddslagstiftning så att personliga data ska kunna flöda fritt mellan medlemsstaterna med vetskapen om att det finns ett gemensamt minimiskydd.[2] I juni 2016, bara två år innan förordningens ikraftträdande, röstade Storbritanniens befolkning för att landet skulle lämna EU, vilket efter en lång och omfattande process skedde den 31 januari 2020.[3] Att Storbritannien inte längre är en av EU:s medlemsstater får givetvis många och stora effekter på ett flertal områden, och inte minst för så kallade dataflöden. Dataflöden – att skicka en större mängd uppgifter över landsgränser – är en naturlig följd av informationsteknologins utveckling och en alltmer globaliserad värld, och är i dagsläget essentiella för att marknader och samhällen ska fungera. Både konsumenter, myndigheter och företag är i hög utsträckning beroende av IT-tjänster som tillhandahålls i andra länder både inom och utanför EU.[4]

Att överföra den typen av uppgifter som faller inom ramen för GDPR:s tillämpningsområde till ett land som ligger utanför EU, är inte helt okomplicerat. Dataskyddsförordningen tillhandahåller några olika alternativ beroende på förutsättningar. Ett av alternativen är att EU-kommissionen fattar beslut om att ett visst land har en adekvat skyddsnivå. Om ett sådant beslut finns, krävs inga ytterligare åtgärder för att överföra personuppgifter till det landet. Regleringen i dataskyddsförordningen tillhandahåller viss information

[1] Se Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG, art. 99.2.
[2] Ibid. skäl 1.
[3] Se EU-kommissionen, ’Det nya normala’ <https://ec.europa.eu/info/relations-united-kingdom/new-normal_sv> (besökt 12 maj 2021).
[4] Se kommissionens meddelande ”Utbyte och skydd av personuppgifter i en globaliserad värld”, COM(2017) 7 slutlig, p. 3.

om vad som ska vara föremål för kommissionens utredning, men EU-domstolen har också presenterat och förtydligat faktorer att förhålla sig till för att ett beslut ska kunna anses giltigt. Om det inte finns något beslut om adekvat skyddsnivå för ett land man önskar överföra personuppgifter till, är man hänvisad till användningen av standardavtalsklausuler, bindande företagsbestämmelser, undantagsöverföringar eller andra skyddsåtgärder.[5]

Problematiken med beslut om adekvat skyddsnivå har nyligen dragits upp i ljuset i och med den så kallade Schrems II-domen.[6] Domen behandlade överföring av uppgifter från unionen till USA med Privacy Shield-beslutet som rättslig grund. Privacy Shield var ett avtal mellan EU och USA som möjliggjorde överföringar till företag och organisationer i USA under vissa förutsättningar, och kvalificerade sig därmed som vad man kan kalla ett *partiellt adekvansbeslut*.[7] Avtalet ogiltigförklarades dock av EU-domstolen i och med domen i Schrems II-målet, liksom Privacy Shields föregångare Safe Harbor[8] ogiltigförklarades i Schrems I.[9]

Att Storbritannien inte längre är en av EU:s medlemsstater innebär att något av alternativen för tredjelandsöverföring måste användas för att dataöverföring ska vara möjlig. I dagsläget och fram till och med den 30 juni 2021 regleras frågan av det avtal som förhandlades fram mellan parterna den 24 december 2020.[10] I detta nu pågår processen där EU-kommissionen utreder om den kan fatta beslut om att Storbritannien säkerställer en adekvat

[5] Se förordning (EU) 2016/679 av den 27 april 2016, kap. V.
[6] C-311/18 *Data Protection Commissioner mot Facebook Irland Ltd och Maximillian Schrems*, EU:C:2020:559.
[7] Kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydds säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna.
[8] Kommissionens beslut av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbor Privacy Principles) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat.
[9] C-362/14 *Maximillian Schrems mot Data Protection Commissioner*, EU:C:2015:650.
[10] Se EU-UK Trade and Cooperation Agreement (TCA) 24 december 2020, art. FINPROV.10A.

skyddsnivå och därmed ska anses vara säkert att överföra uppgifter till.[11] I och med utträdet är Storbritannien inte längre bundet av de ramverk som tidigare anses ha tryggat ett adekvat skydd för personuppgifter. Det finns dessutom indikationer på att Storbritannien har övervakningsmekanismer som liknar det amerikanska systemet,[12] ett system som var en av orsakerna till att möjligheten till generella överföringar till USA ströps så sent som förra året. Mot bakgrund av förfarandet med USA och ogiltigförklarandet av tillhörande beslut har det dock blivit påtagligt att gränsen för vad som kan anses godtagbart ur ett EU-rättsligt perspektiv inte är helt tydlig. Vad som kommer att gälla för Storbritanniens del i fråga om överföring av personuppgifter står således inte klart.

Det föreligger en konflikt mellan intresset av gränsöverskridande dataflöden och rätten till privatliv och skyddet för personuppgifter. Data är en av vår tids allra viktigaste handelsvaror och av väsentlig betydelse för många samhälleliga funktioner. Att fritt överföra data till hela världen hade emellertid riskerat att undergräva det skydd för personuppgifter som åtminstone i EU utgör en grundläggande rättighet. Denna konflikt blir särskilt framträdande när kommissionen tar ställning i frågan om ett tredjeland tillhandahåller en adekvat skyddsnivå. Det finns således ett behov av att undersöka hur EU-domstolen resonerar vid bedömning av huruvida beslut om adekvat skyddsnivå ska anses giltiga.

[11] Se pressmeddelande från EU-kommissionen, ‘Data protection: European Commission launches process on personal data flows to UK’ <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661> (besökt 13 mars 2021).
[12] Se Utrikespolitiska institutet, ’Storbritannien – Demokrati och rättigheter’ https://www.ui.se/landguiden/lander-och-omraden/europa/storbritannien/demokrati-och-rattigheter/ (besökt 19 april 2021).

1.2 Syfte och frågeställning

Denna uppsats ämnar utreda hur EU-domstolens bedömning av beslut om adekvat skyddsnivå för tredjeland förhåller sig till den nivå av skydd för integritet och personuppgifter som finns inom EU. Utredningen ska finna svar på hur EU-domstolen bedömer avvikelser från EU:s skyddsnivå, samt vilka utmaningar domstolen möter vid bedömningen av tredjelands skyddsnivå.

Uppsatsen kommer huvudsakligen att svara på följande fråga:

- Hur förhåller sig bedömningen av adekvat skyddsnivå i tredjeland enligt art. 45.1 GDPR till den skyddslagstiftning avseende personuppgifter som gäller inom EU?

För att uppnå syftet kommer följande delfrågor att besvaras:

- Vilka faktorer ska beaktas i bedömningen av tredjelands skyddsnivå?
- Vad utgör en adekvat skyddsnivå under art. 45.1 GDPR?
- Vilka utmaningar uppkommer vid bedömning av tredjelands skyddsnivå, särskilt i ljuset av Schrems II-domen?

1.3 Avgränsningar

Vad gäller rättigheter relevanta för området fokuserar denna uppsats på de som erhålls genom EU-stadgan. Rättighetsskyddet i EKMR kommer således inte behandlas mer än den mån det är nödvändigt för att uppnå uppsatsens syfte. Eventuella grundlagsskydd på nationell nivå kommer heller inte att behandlas.

Dataskyddsförordningen är inte den enda lagstiftning som rör behandling av personuppgifter. Det finns ett flertal mer sektorsspecifika direktiv som reglerar behandling av personuppgifter inom ett visst område, som till

exempel ePrivacy-direktivet[13] eller direktivet om personuppgiftsskydd vid brottsbekämpning[14]. Denna typ av lagstiftning kommer inte att behandlas mer än viss genomgång i samband med presentationen av somliga för framställningen relevanta rättsfall.

En närliggande diskussion på ämnet tredjelandsöverföringar enligt GDPR berör användningen av standardavtalsklausuler som lämplig skyddsåtgärd. Problematiken kring standardavtalsklausuler är i mångt och mycket densamma som vid beslut om adekvat skyddsnivå och dess giltighet genomgick också en prövning i Schrems II-målet. Varken standardavtalsklausulerna eller övriga verktyg för tredjelandsöverföringar kommer att presenteras närmre.

Det finns också anledning att nämna något om behandlingen av lagstiftning i stater som ligger utanför unionens gränser. Eftersom uppsatsens syfte till viss del handlar om den inverkan som tredjelands lagstiftning har, är viss behandling av densamma nödvändig. Fokuset för denna framställning handlar emellertid om den bedömning som sker på EU-rättslig nivå. Behandlingen av amerikansk och brittisk lag sker därför huvudsakligen med utgångspunkt i dess betydelse för EU-rätten, och hur den har tolkats och utretts av EU-kommissionen respektive EU-domstolen.

1.4 Metod och material

För att uppnå uppsatsens syfte och besvara dess frågeställningar har jag använt mig av den rättsdogmatiska och EU-rättsliga metoden. Den rättsdogmatiska metoden handlar i korthet om att utläsa och tolka en rättsregel

[13] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation).
[14] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

för att finna en lösning på ett juridiskt problem.[15] Det första steget handlar således om att konstruera en relevant och korrekt juridisk frågeställning. I det andra steget, att finna och tolka rättsregler, träder rättskälleläran in. Rättskälleläran används för att systematisera det juridiska regelverket och anger en hierarki för vilka källor som ska, bör och får användas vid uttolkning av gällande rätt.[16] Sammanfattningsvis är alltså rättsdogmatikens huvudsakliga uppgift att beskriva rätten så som den är, med en domares arbetssätt som utgångspunkt.[17] Forskaren har dock på grund av sin roll och sitt syfte en möjlighet att förhålla sig annorlunda till den juridiska metoden och rättskällorna. Då forskarens uppgift bland annat är att granska, analysera och producera kunskap, har denne en möjlighet att dels beakta andra källor än de angivna i rättskälleläran, dels förhålla sig annorlunda till innehållet i källorna.[18]

Den EU-rättsliga metoden kan ses som en metod för att hantera och tolka EU-rättsliga källor. Metoden har arbetats fram då EU är en speciell typ av organisation. I målet *van Gend en Loos*[19] fastslog EU-domstolen att EU-rätten utgjorde en ny och självständig rättsordning inom folkrätten. De bindande rättskällorna består av primärrätten och den bindande sekundärrätten, internationella avtal samt EU-domstolens och tribunalens praxis.[20] Något som kan lyftas som utmärkande för EU-rätten är att oskrivna rättskällor så som allmänna rättsprinciper och domstolarnas rättspraxis generellt har en högre status än vad sådana rättskällor har i till exempel det svenska rättssystemet. En hel del av den gällande rätten har utvecklats genom rättspraxis vilket skapar associationer till det anglosaxiska *Common law*-systemet, där prejudikat och rättspraxis erkänns som den dominerande rättskällan.[21]

[15] Se Kleineman (2018), s. 21.
[16] Ibid. s. 21.
[17] Se Olsen (2004), s. 111 f.
[18] Se Svensson (2014), s. 222 ff.
[19] Se mål 26/62 *Van Gend en Loos*, EU:C:1963:1.
[20] Se Hettne & Otken Eriksson (2011), s. 40.
[21] Ibid. s. 41.

EU:s primärrätt utgörs av fördragen, stadgan och allmänna rättsprinciper.[22] Sekundärrätten består av de rättsakter och beslut som fattats med stöd av fördragen så som förordningar, direktiv och beslut, så kallade bindande rättsakter. Sekundärrätten innefattar dock också icke-bindande rättsakter som till exempel yttranden, rekommendationer, resolutioner och meddelanden.[23] Som namnet antyder är de icke-bindande rättsakterna tillsammans med förarbeten, EU-rättslig doktrin och generaladvokaternas förslag till avgöranden endast riktlinjer och inget som måste beaktas. Även om sådana källor inte är bindande, kan de användas som underlag för att tolka och fylla ut EU-rättsliga bestämmelser och även ha en normerande verkan.[24]

För att beskriva det EU-rättsliga skyddet av personuppgifter redogörs lagstiftningen som sådan samt relevant doktrin. För att beskriva rättsläget ytterligare presenteras också relevanta rättsfall. De behandlade rättsfallen har valts ut för att påvisa rättsläget för begränsningar av grundläggande rättigheter , med särskilt fokus på proportionalitetsbedömningar i förhållande till integritets- och personuppgiftsskyddet. Till hjälp för uppgiften att förklara processen för fattandet av beslut om adekvat skyddsnivå nyttjas även meddelanden från kommissionen samt riktlinjer utgivna av art. 29-gruppen och EDPB. För att visa på det EU-rättsliga perspektivet och rättsläget gällande överföringar av personuppgifter till tredjeland behandlas främst EU-domstolens avgöranden i Schrems I och II.

I syfte att förklara och beskriva processen för tillkomsten av adekvansbeslut och hur EU-kommissionen bedömer tredjelands skyddsnivå i förhållande till EU, ägnas ett kapitel åt den pågående processen för ett eventuellt beslut om adekvat skyddsnivå för Storbritanniens räkning. Detta avsnitt utgår främst från det förslagsutkast till beslut som EU-kommissionen presenterade den 19 februari 2021. I syfte att nyansera kommissionens förslag används också det yttrande som EDPB lämnat över kommissionens förslag. Det ska noteras att

[22] Se Bergström & Hettne (2014), s. 21. Vad gäller de allmänna rättsprincipernas konstitutionella status, se exempelvis C-101/08 *Audiolux*, EU:C:2009:626, p. 63.
[23] Se Hettne & Otken Eriksson (2011), s. 41 f.
[24] Se Reichel (2018), s. 128 f.

denna process är under utveckling, men att ett beslut är väntat att fattas inom kort.

1.5 Forskningsläge

Ämnet som behandlas i denna uppsats är både nytt och gammalt på samma gång. Sen teknologin blev tillgänglig har data transporterats över landsgränser och därmed aktualiserat integritetsskyddsbehovet och eventuella överlappande regleringar. Området har dock varit föremål för en hel del utveckling de senaste åren. I fokus har inte minst varit överföringar av data från EU till USA som har granskats noggrant i och med Schrems I och II.[25] En artikel publicerad i Europarättslig tidskrift behandlar aspekten om relationen mellan dataskydd och undantag för syften som relaterar till nationell säkerhet, i ljuset av Schrems I.[26] Ett flertal publiceringar existerar också som syftar till att jämföra just det amerikanska integritetsskyddet med det europeiska.[27]

Forskningsläget för överföringar till Storbritannien efter landets utträde ur EU, är mer återhållsamt. En rapport har publicerats vid University College London.[28] Författarna utreder Storbritanniens möjligheter att erhålla ett adekvansbeslut mot bakgrund av den EU-rättsliga regleringen, och anlägger ett ekonomiskt perspektiv på konsekvenserna ett beslut eller icke-beslut. Ytterligare en rapport på ämnet har publicerats vid London School of Economics, med särskilt fokus på potentiella hinder för att ett beslut om adekvat skyddsnivå ska kunna komma till stånd.[29] De båda rapporterna publicerades dock innan Schrems II-domen meddelats och dessutom innan det fanns en påbörjad process mellan EU och Storbritannien. Mot bakgrund

[25] C-362/14 *Maximillian Schrems mot Data Protection Commissioner*, EU:C:2015:650; C-311/18 *Data Protection Commissioner mot Facebook Irland Ltd och Maximillian Schrems*, EU:C:2020:559.
[26] Se Colonna (2016).
[27] Se exempelvis Bygrave (2013); Schwartz och Solove (2014).
[28] Se Patel & Lea *(*2019).
[29] Se Murray (2017).

av ovanstående framgår att det föreligger utrymme för mer forskning vad gäller bedömningen av tredjelands skyddsnivå i samband med beslut om adekvat skyddsnivå.

1.6 Disposition

Kapitel två går igenom grunderna i dataskyddsförordningen vad gäller bakgrund, grundläggande begrepp och principer samt bakomliggande skyddsintressen. I den andra delen av kapitel två presenteras regleringen av tredjelandsöverföringar. Ett längre avsnitt behandlar processen för beslut om adekvat skyddsnivå, medan ett kortare presenterar övriga möjligheter för tredjelandsöverföringar enligt GDPR.

Kapitel tre fokuserar på dataöverföring till USA. I kapitlet presenteras de båda beslut som legat till grund för överföringar av personuppgifter från EU till USA samt åtföljande domar som ogiltigförklarat desamma. I slutet av kapitlet redogörs även för den amerikanska regeringens synpunkter på Schrems II-domen.

Kapitel fyra behandlar huvudsakligen det förslagsutkast som i skrivande stund ligger på bordet och behandlar kommissionens utredning av huruvida Storbritannien kan anses säkerställa en adekvat skyddsnivå. I kapitlets andra del presenteras EDPB:s yttrande och kritik mot förslaget.

I **kapitel fem** analyseras och diskuteras den behandlade informationen utifrån uppsatsens syfte och frågeställningar. I det avslutande **kapitel sex** sammanfattas slutsatserna och ges avslutande kommentarer.

2 Om GDPR och tredjelandsöverföringar

2.1 Dataskyddsförordningen

2.1.1 Historia och bakgrund

Den 25 maj 2018 trädde GDPR i kraft, direkt tillämplig i alla EU:s medlemsstater. Förordningen syftar till att säkerställa det skydd för privatliv och personuppgifter som unionsmedborgarna har enligt EU-stadgan samt fördraget om Europeiska unionens funktionssätt.[30] Förordningen ska också säkerställa att personuppgifter kan flöda inom unionen mellan både privata och offentliga aktörer.[31] Enligt uttalanden från EU-kommissionen efter förordningens ikraftträdande, utgör lagstiftningen inte bara en viktig del av EU-rätten utan har också blivit en global referenspunkt inom dataskyddsområdet.[32]

Diskussionen om skydd för personuppgifter startade i Sverige på 1970-talet, då en statlig insamling av personuppgifter initierade en debatt gällande insamling av data i reklamsyfte och hotet en sådan företeelse kunde utgöra mot den personliga integriteten. Debatten ledde så småningom till en flertal lagändringsförslag och att Sverige blev Europas första land att införa en lag om behandling av personuppgifter.[33] Parallellt fördes diskussioner och förhandlingar också på en internationell nivå, vilket ledde fram till att OECD som ett led i att främja tillväxt och gränsöverskridande handel antog riktlinjer för gränsöverskridande överföringar av personuppgifter och skydd för den

[30] Se förordning (EU) 2016/679 av den 27 april 2016, skäl 1.
[31] Ibid. skäl 5.
[32] Se EU-kommissionen, 'Joint statement ahead of the 2nd year anniversary of the General Data Protection Regulation' <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_20_913> (besökt 17 maj 2021).
[33] Se Frydlinger m.fl. (2018), s. 21 f.

personliga integriteten. Med riktlinjerna följde också en rekommendation kring hur medlemsländernas nationella lagstiftning på området borde utformas, och med ett flertal definitioner och begrepp som finns med än idag kan riktlinjerna ses som en förlaga till dagens gällande förordning.[34]

Utvecklingen på internationell nivå skedde ungefär samtidigt som Europarådet antog en konvention för skydd av behandling av personuppgifter. De olika lagstiftningarna och instrumenten kom dock att bli en oro för kommissionen, vilket ledde fram till förhandlingar inom EG. Man var orolig att diskrepansen mellan de olika medlemsstaternas dataskyddslagstiftningar var ett problem för inrättandet och upprätthållandet av den inre marknaden. Förhandlingarna ledde så småningom fram till införlivandet av direktiv 95/46/EG.[35] Syftet med direktivet var tydligt: det skulle dels harmonisera och fastställa det grundläggande skyddet för fysiska personer vad gäller rätten till privatliv i samband med behandling av personuppgifter[36], dels främja det fria flödet av personuppgifter mellan medlemsstaterna.[37] Man upplevde emellertid att skyddet ännu skiljde sig alltför mycket mellan medlemsstaterna. 2009 blev dessutom de grundläggande fri- och rättigheterna i EU-stadgan rättsligt bindande i och med Lissabonfördraget, vilket slutligen ledde till införlivandet av dataskyddsförordningen.[38]

2.1.2 Grundläggande begrepp och struktur

Personuppgifter definieras som ”varje upplysning som avser en identifierad eller identifierbar fysisk person”.[39] Det innebär att personlig data kan vara allt från namn och personnummer till IP-adresser och fotografier.[40] Även om en enskild upplysning inte självständigt kan användas för att identifiera en

[34] Se Frydlinger m.fl. (2018), s. 22.
[35] Ibid. s. 24.
[36] Se Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, skäl 2 och 3.
[37] Ibid. skäl 5 och 6.
[38] Se förordning (EU) 2016/679 av den 27 april 2016, skäl 9 och 10.
[39] Ibid. art. 4.1
[40] Vad gäller IP-adresser, se till exempel C-582/14 *Patrick Breyer mot Bundesrepublik Deutschland*, EU:C:2016:779.

person, så faller den inom definitionen om den i kombination med andra upplysningar kan användas för identifiering av en fysisk person.[41] Olika typer av personuppgifter behandlas olika i förordningen, med hänvisning till att somliga upplysningar klassificeras som ”känsliga personuppgifter”. Till den gruppen hör till exempel uppgifter om etnicitet, sexuell läggning, biometriska uppgifter m.m.[42]

Registrerad är den vars personuppgifter är under sådan behandling som omfattas av förordningen. Endast fysiska personer kan vara registrerade, skyddet omfattar inte juridiska personer.[43]

Behandling är tillsammans med personuppgifter ett av förordningens mest centrala begrepp. Definitionen är bred och innebär att i princip alla åtgärder som utförs i samband med hantering av personuppgifter som till exempel insamling, lagring, strukturering och mycket mer, ska betraktas som behandling av personuppgifter oavsett om åtgärderna sker på automatiserad väg eller ej.[44] Det finns ett fåtal undantag som anger att viss behandling ska falla utanför förordningens tillämpningsområde. Ett av de främsta undantagen är det som omfattar så kallad privat behandling av personuppgifter. Det innebär att behandling av personuppgifter som är privat och helt saknar koppling till yrkes- eller affärsmässig verksamhet inte behöver följa dataskyddsförordningens regler.[45] Dataskyddsförordningens regler omfattar heller inte sådan behandling som sker inom ramen för en verksamhet som inte omfattas av unionsrätten. I praxis har EU-domstolen uttalat att detta undantag ska tolkas restriktivt.[46] Behandling vid frågor som rör nationell säkerhet är ett exempel på sådan verksamhet.[47] EU-domstolen har dock fastslagit att data som överförs till tredjeland ska omfattas av dataskyddsförordningen, även om

[41] Se förordning (EU) 2016/679 av den 27 april 2016, skäl 26.
[42] Ibid. art. 9.1, för en uttömmande lista.
[43] Ibid. art. 1.1 och 4.1.
[44] Ibid. art. 4.2.
[45] Ibid. art. 2.2(c).
[46] Se C-25/17 *Jehovas vittnen*, EU:C:2018:551, p. 37.
[47] Se förordning (EU) 2016/679 av den 27 april 2016, art. 2.2(a).

den kan komma att bli föremål för behandling i syften som rör allmän eller nationell säkerhet.[48]

Personuppgiftsansvarig är den som ansvarar för att se till att personuppgiftsbehandlingen efterlever de principer och skyldigheter som följer av dataskyddsförordningen. Den personuppgiftsansvarige kan vara en fysisk eller juridisk person, en offentlig myndighet eller annat organ eller institution, och är den som bestämmer över syftet med personuppgiftsbehandlingen och på vilken grund som behandlingen ska ske.[49] Om det framkommer att behandlingen inte efterlever dataskyddsförordningens krav och principer är det den personuppgiftsansvarige som tillsammans med personuppgiftsbiträdet kan utkrävas ansvar. Det är de faktiska förhållandena, det vill säga vem som bestämmer över medel och ändamål, som avgör vem som ska anses vara personuppgiftsansvarig.[50]

Personuppgiftsbiträde är i korta drag en fysisk eller juridisk person, myndighet, institution eller annat organ som utför personuppgiftsbehandlingen på uppdrag av den personuppgiftsansvarige.[51] Två kriterier för det tidigare begreppet ”registerförare” uppfördes av art. 29-gruppen. För det första att biträdet ska vara en separat juridisk eller fysisk person i förhållande till den personuppgiftsansvarige, för det andra att denne ska behandla personuppgifter för den personuppgiftsansvariges räkning.[52] Enligt art. 29-gruppen innebär det sistnämnda kriteriet att man tillgodoser någon annans intressen och har blivit delegerad uppgifter. Om ett biträde däremot börjar utföra åtgärder som att till exempel bestämma ändamålet med behandlingen är denne snarare att betrakta som personuppgiftsansvarig.[53]

[48] Se C-311/18 *Data Protection Commissioner mot Facebook Irland Ltd och Maximillian Schrems*, EU:C:2020:559, p. 89.
[49] Se förordning (EU) 2016/679 av den 27 april 2016, art. 4.7.
[50] Se Frydlinger m.fl. (2018), s. 51.
[51] Se förordning (EU) 2016/679 av den 27 april 2016, art. 4.8.
[52] Se art. 29-gruppen, *WP 169*: *Yttrande 1/2010 om begreppen registeransvarig och registerförare*, s. 24.
[53] Ibid. s. 25.

Det finns ett antal principer som genomsyrar dataskyddsförordningen. En primär sådan anger att all personuppgiftsbehandling ska ske på ett lagligt, korrekt och öppet vis. Laglighetskravet innebär att det krävs uttryckligt lagstöd för behandlingen, och att den som behandlar uppgifterna ska ha stöd i någon av de rättsliga grunderna.[54] Så som Frydlinger m.fl. påpekar, är begreppet *korrekthet* en översättning från engelskans *fairness* och innebär att behandlingen ska ske på ett godtagbart sätt. Principen om öppenhet innebär att all personuppgiftsbehandling ska vara transparent gentemot de registrerade och informera om behandlingen samt den registrerades rättigheter.[55]

Personuppgiftsbehandlare ska också förhålla sig till principen om ändamålsbegränsning. Den innebär att behandlingen ska utgå från särskilda och berättigade ändamål och inte får ske på ett godtyckligt vis. Ändamålet med behandlingen ska också kommuniceras till den registrerade, så att denne får möjlighet att göra en bedömning av möjliga konsekvenser. Det inte är förbjudet att använda uppgifterna till annat ändamål än det uppgivna, under förutsättning att det tillkomna ändamålet är förenligt och i linje med det uppgivna.[56] Den som behandlar personuppgifter behöver också förhålla sig till principen om lagringsminimering. Principen innebär att personuppgifter bara får lagras under så lång tid som är motiverat i förhållande till ändamålet, sedan ska uppgifterna raderas eller avidentifieras.[57]

2.1.3 Territoriellt tillämpningsområde

Dataskyddsförordningens territoriella tillämpningsområde framgår av art. 3. Artikeln fastställer att behandling av personuppgifter som sker inom ramarna för en verksamhet som bedrivs på personuppgiftsansvariges eller personuppgiftsbiträdes verksamhetsställe beläget inom unionen, ska tillämpa förordningen oavsett om själva behandlingen sker inom unionens gränser

[54] Se förordning (EU) 2016/679 av den 27 april 2016, art. 6.
[55] Se Frydlinger m.fl. (2018), s. 36 f.
[56] Ibid. s. 37 f.
[57] Se Öman, Dataskyddsförordningen (GDPR) m.m. (29 februari 2020, Version 1A, JUNO), kommentaren till art. 5.1 led (e).

eller ej.[58] Föreskriften kan sammanfattas som ett etableringskriterium. Förordningen reglerar även fallet när personuppgiftsansvarigas eller -biträdens etableringsställe ligger utanför unionens gränser. Förordningen blir under sådana förutsättningar tillämplig om behandlingen rör registrerade som befinner sig inom unionen, och behandlingen knyter an till utbjudning av varor eller tjänster till registrerade inom unionen eller rör övervakning av registrerades beteende inom unionen.[59] Denna formulering kan snarare anses vara ett riktningskriterium. Syftet är att motverka situationer där företag som verkar på den europeiska marknaden etablerar sig utomlands för att undvika skyldighet att följa EU:s lagstiftning.[60]

2.1.4 Skyddsintresset

Ett grundläggande skydd för integritet och personuppgifter återfinns i fördraget om Europeiska unionens funktionssätt[61] och EU:s stadga om de grundläggande rättigheterna. Även EKMR tillhandahåller ett skydd för privat- och familjeliv, och i till exempel Sverige finns också ett skydd föreskrivet i grundlagen.[62]

I EU:s stadga om de grundläggande fri- och rättigheterna är framför allt tre artiklar relevanta att behandla. Artikel 7 föreskriver att ”var och en har rätt till respekt för sitt privat- och familjeliv, sin bostad och sina kommunikationer”. Denna formulering gör bestämmelsen till en mer eller mindre direkt spegling av det skydd för privatliv som erhålls genom art. 8 EKMR, och ska också tolkas så som art. 8 EKMR har tolkats av Europadomstolen.[63] Vad som ska omfattas av skyddet för privatliv är inte helt definierat. Det ska dock utgöra ett starkt skydd för den enskildas autonomi och ge individen en möjlighet att utveckla personlighet och individualitet.

[58] Se förordning (EU) 2016/679 av den 27 april 2016, art. 3.1.
[59] Ibid. art. 3.2.
[60] Se Törngren, förordning (EU) 2016/679 art. 3.2, avsnitt 2.2 Etablering utanför EU, Lexino 2019-04-30 (JUNO).
[61] Se art. 16.1 FEUF.
[62] Se art. 8 EKMR samt 2 kap. 6 § 2 st. RF.
[63] Se Lebeck (2016), s. 278.

Skyddet bör också vara dynamiskt i takt med samhällets och teknikens förändring.[64]

Art. 7 EU-stadgan innefattar visserligen ett skydd för behandling av personlig information och data, men detta har förstärkts genom art. 8 som föreskriver följande:

1. Var och en har rätt till skydd av de personuppgifter som rör honom eller henne.
2. Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem.
3. En oberoende myndighet ska kontrollera att dessa regler efterlevs.

Art. 8 är således den artikel som på det mest konkreta sättet lägger grunden till dataskyddsförordningen och utformningen av skyddet för personuppgifter. Införlivandet av artikeln är en direkt följd av informationsteknikens utveckling och det faktum att personuppgifter med tidens gång har blivit oerhört mycket enklare att samla in, lagra, systematisera och överföra mellan system.[65] Det ska tilläggas att art. 8 har ansetts vara *lex specialis* till det allmänna skyddet för privatlivet, och således också ska tolkas i ljuset av EKMR:s skydd för privatlivet.[66]

I art. 47 EU-stadgan fastställs den grundläggande rätten till ett effektivt rättsmedel och en opartisk domstol. Rätten till domstolsprövning fyller framför allt två huvudsakliga funktioner. Den säkerställer dels enskildas rätt att få sin sak prövad i domstol, dels markerar den att EU vilar på ett rättsligt system där beslut och rättsregler som påverkar enskilda alltid ytterst ska kunna prövas av domstol.[67] En domstol ska vidare vara opartisk, oberoende, ha kompetens för de områden den behandlar, samt fatta sina beslut mot bakgrund av rättsregler. Kravet på oberoende innebär i praktiken att en

[64] Se Lebeck (2016), s. 258.
[65] Ibid. s. 279.
[66] Ibid. s. 310.
[67] Ibid. s. 597.

domstol ska vara en institution som är separerad från den verkställande och beslutsfattande makten.[68] Rätten att få sin sak prövad omfattar samtliga rättigheter och skyldigheter som följer av EU-rätten som påverkar och skapar ett intresse för den enskilde.[69]

Samtliga fri- och rättigheter fastslagna i EU-rätten grundar sig i en tanke om upprätthållandet av en människas värdighet.[70] Principen om upprätthållandet och skyddet av människans värdighet är centralt för EU-rätten och används också som tolkningsprincip av densamma.[71] Vad gäller kopplingen mellan behandling av personuppgifter och människors värdighet kan sägas att mängden av information som finns tillgänglig för andra, påverkar varje individs möjlighet att leva ett oberoende och fritt liv samt utforma egna åsikter, tankar och värderingar.[72] Ett nutida och pedagogiskt exempel på hur behandling av personuppgifter påverkar sådana möjligheter kan hämtas från det som har kommit att kallas för Cambridge Analytica-skandalen.

Under 2018 framkom att data från mer än 85 miljoner Facebook-användare hade läckt ut och hamnat i händerna på ett analysföretag, Cambridge Analytica. Cambridge Analytica var anlitat för att assistera med politiska analyser och marknadsföring för presidentkandidaterna Ted Cruz och Donald Trumps räkning inför det amerikanska presidentvalet 2016. Med hjälp av den data företaget hade fått tillgång till kunde kampanjerna skapa ett system som profilerade[73] individuella väljare och utefter det rikta reklam mot de väljare som av systemet hade identifierats som påverkansbara.[74] Exakt hur och i vilken utsträckning som strategin påverkade utgången av valet är inte klart, men det visar på hur personlig data kan eller skulle kunna påverka människors

[68] Se Lebeck (2016), s. 589.
[69] Ibid. s. 597 ff.
[70] Se Frydlinger m.fl. (2018), s. 32.
[71] Se Lebeck (2016), s. 205.
[72] Se Frydlinger m.fl. (2018), s. 33 f.
[73] Jfr med definitionen av *profilering* i art 4.4 dataskyddsförordningen.
[74] Se Cadwalladr & Graham-Harrison, ’Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach’ <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> (besökt 23 mars 2021).

möjligheter att tänka fritt och självständigt. Vidare kan den kännedom om personlig data som myndigheter och arbetsgivare har, ha en direkt påverkan på vilka möjligheter varje individ har. Som exempel kan lyftas effekten en betalningsanmärkning hos Kronofogdemyndigheten kan ha på möjligheten att skaffa bostad eller hur brottsregisterinformation kan påverka möjligheten att få ett arbete.[75]

Skyddet för privatliv och personuppgiftsbehandling är inte absoluta rättigheter, utan får begränsas.[76] En begränsning av grundläggande fri- och rättigheter ska vara laglig, tjäna ett legitimt syfte och framför allt vara proportionerlig.[77] Kriterierna har utvecklats av Europadomstolen men brukas även av EU-domstolen.[78] Att en begränsning ska vara laglig innebär i korta drag att det ska finnas lagstöd för den. Vidare bör den begränsande normen också vara tillgänglig för individen, förutsebar och precis i den mening att normens räckvidd och begränsning ska framgå. Med legitimt syfte avses att begränsningen ska syfta till att antingen skydda andra grundläggande rättigheter alternativt allmänna intressen. Allmänna intressen ska förstås åtgärder som är till gagn för samhällets medborgare i stort.[79]

Vid en intresseavvägning brukar det dock läggas mest tyngd vid proportionalitetsprincipen. Det innebär att en åtgärd som begränsar en grundläggande rättighet ska vara nödvändig, så avgränsad som möjligt och stå i proportion till åtgärdens syfte.[80] Proportionalitetsbedömningens betydelse kan variera beroende på vilken typ av rättighet det handlar om. Den har generellt behandlats mer utförligt vid begränsningar av person- och opinionsrättigheter jämfört med exempelvis ekonomiska rättigheter.[81]

[75] Se Frydlinger m.fl. (2018), s. 33 f.
[76] Se förordning (EU) 2016/679 av den 27 april 2016, skäl 4.
[77] Se EU-stadgan, art. 52.1.
[78] Se Lebeck (2016), s. 150 f.
[79] Ibid. s. 156 f.
[80] Ibid. s. 163.
[81] Ibid.

Vad gäller proportionalitetsprövningar vid inskränkningar av personuppgiftsskyddet har sådana utförts i ett flertal mål vid EU-domstolen, till exempel i Schrems-målen.[82] Ett annat exempel är målet *Digital Rights Ireland* som huvudsakligen rörde giltigheten av datalagringsdirektivet[83].[84] Direktivet, som i målet ogiltigförklarades av EU-domstolen, tillkom bland annat mot bakgrund av terrorattackerna i London och Madrid och föreskrev en skyldighet för leverantörer av kommunikationstjänster att samla in och tillhandahålla trafik- och lokaliseringsuppgifter till myndigheter i brottsbekämpande syften.[85]

Den hänskjutande domstolen ställde i målet frågan om direktivet var förenligt med skyddet för privatliv och personuppgifter. Domstolen konstaterade att de uppgifter som samlades in gjorde det möjligt att få god insikt i människors privatliv och således utgjorde ett ingrepp i både art. 7 och 8 EU-stadgan.[86] Frågan var om datalagringsdirektivet och följderna av det var av sådan karaktär att det utgjorde en proportionerlig och försvarlig begränsning. Enligt domstolen har bekämpandet av internationell terrorism och grov brottslighet erkänts som ett allmänt samhällsintresse. Betydelsen som personuppgiftsskyddet har för den grundläggande respekten av privatlivet är dock så stor att utrymmet för en skönsmässig bedömning är litet. Inskränkningar av de rättigheterna ska därför begränsas till vad som är strikt nödvändigt.[87] Ogiltigförklaringen motiverades för det första med att det aktuella samhällsintresset inte ensamt motiverade den typ av lagringsåtgärder som direktivet föreskrev. För det andra lyfte domstolen också kravet på precisa och tydliga bestämmelser som reglerar den aktuella åtgärdens tillämplighet och räckvidd. I det här fallet saknades begränsningar bland

[82] Se kapitel 3.
[83] Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG.
[84] Se förenade målen C-293/12 och C-594/12 *Digital Rights Ireland*, EU:C:2014:238.
[85] Se direktiv 2006/24/EG av den 15 mars 2006, art. 1.1.
[86] Se förenade målen C-293/12 och C-594/12 *Digital Rights Ireland*, EU:C:2014:238, p. 27 & 29.
[87] Ibid. p. 42 & 48.

annat vad gällde lagringstid av uppgifterna samt bestämmelser om tillgång till och användning av uppgifterna. Domstolen fastställde därför att insamlingen gick utöver vad som var nödvändigt för att uppnå syftet med direktivet.[88] Direktivet förklarades således ogiltigt på grund av att det enligt domstolen stred mot proportionalitetsprincipen.

Ett annat mål där domstolen gjorde en proportionalitetsprövning vid intrång i privatlivs- och personuppgiftsskyddet var *Tele2/Watson*.[89] Omständigheterna liknade de i Digital Rights Ireland, och nyss nämnda mål utgjorde också en bakgrund till målets uppkomst. Rättsfallet var två förenade mål, där det ena handlade om att telekom-operatören Tele2 hade upphört att lagra uppgifter till följd av Digital Rights-domen. Detta fick svenska Post- och Telestyrelsen att utfärda ett föreläggande om att Tele2 skulle fortsätta med lagringen i enlighet med nationell rätt. Det andra målet kom från appellationsdomstolen för England och Wales. I korthet ställde domstolen frågan om nationell rätt som var hänförlig till det numera ogiltigförklarade datalagringsdirektivet, var förenlig med de grundläggande rättigheterna avseende privatliv och personuppgiftsskydd i EU-stadgan. I båda målen hävdades att den nationella lagstiftningen och lagringen av uppgifter kunde stödjas på det gamla ePrivacy-direktivet, som likt datalagringsdirektivet reglerade trafikuppgifter från elektronisk kommunikation och lagring av sådana. ePrivacy-direktivet föreskrev ett visst skydd för registrerade, men medgav också medlemsstaterna möjlighet att lagstifta om åtgärder för att begränsa dessa rättigheter till syfte för nationell säkerhet och brottsbekämpning.[90]

Domstolen hade återigen att göra en proportionalitetsprövning, och hänvisade i stor utsträckning till den praxis som fastslagits i Digital Rights Ireland. Domstolen tog särskild fasta på det faktum att den nationella lagstiftningen

[88] Se förenade målen C-293/12 och C-594/12 *Digital Rights Ireland*, EU:C:2014:238, p. 54-65.
[89] Se förenade målen C-203/15 och C-698/15 *Tele2 Sverige AB och Secretary of State for the Home Department mot Post- och telestyrelsen m.fl.*, EU:C:2016:970.
[90] Se Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation, art. 15.1.

möjliggjorde en generell lagring och inte gjorde någon skillnad eller begränsningar i insamlingen utifrån det eftersträvade syftet. Lagringen av uppgifterna omfattade samtliga personer som använde sig av elektroniska kommunikationstjänster, oavsett om det fanns anledning att tro att dessa hade ett samband med grov brottslighet. Mot denna bakgrund ansåg domstolen att åtgärden gick utanför vad som kunde anses strängt nödvändigt och godtagbart i ett demokratiskt samhälle.[91] Domstolen förtydligade därtill att den nationella lagstiftningen måste tillhandahålla tydliga och precisa bestämmelser som begränsar lagringsåtgärdens omfattning och tillämplighet. Domstolen fastställde också att myndigheters tillgång till de lagrade uppgifterna måste regleras av objektiva kriterier som fastställer under vilka villkor som tillgång ska ges, och att det i detta fall i princip var begränsat till brottsbekämpning.[92]

Sammanfattningsvis är alltså proportionalitetsbedömningar centrala vid bedömningen av om ingrepp i skyddet för privatliv och personuppgifter ska anses godtagbara. Begränsningar ska minimeras till vad som är strängt nödvändigt och således är omfattande lagring utan tydliga begränsningar och med oklara samband till syftet, inte att anse som godtagbart enligt EU-domstolens praxis.

2.2 Tredjelandsöverföring genom beslut om adekvat skyddsnivå

Överföring av personuppgifter till tredjeland är möjliga om EU-kommissionen har fattat ett beslut om att destinationen för uppgifterna har en sådan adekvat skyddsnivå som motsvarar skyddet inom EU. Om ett sådant beslut finns, behöver inget särskilt tillstånd för överföringen. Beslut om adekvat skyddsnivå kan ges till länder, organisationer eller territorium.[93]

[91] Se förenade målen C-203/15 och C-698/15 *Tele2 Sverige AB och Secretary of State for the Home Department mot Post- och telestyrelsen m.fl.*, EU:C:2016:970, p. 105-107.
[92] Ibid. p. 119.
[93] Se förordning (EU) 2016/679 av den 27 april 2016, art. 45.1.

Processen för att nå ett sådant beslut innefattar ett initialt förslag från kommissionen, ett yttrande från EDPB, ett godkännande från representanter för medlemsstaterna och slutligen att kommissionen antar förslaget.[94] Det är endast kommissionen som har befogenhet att fatta beslut om adekvat skyddsnivå enligt art. 45 GDPR. Det är inte möjligt för en personuppgiftsansvarig att själv göra en bedömning av om ett mottagarland tillhandahåller en adekvat skyddsnivå likvärdig med unionens under art. 45. Efter att ett beslut om adekvat skyddsnivå har fattats, är kommissionen ålagd att kontinuerligt övervaka utvecklingen i landet. Om någon omständighet medför att landet i fråga inte längre kan anses tillhandahålla en adekvat skyddsnivå likvärdig med skyddet inom unionen, ska kommissionen återkalla beslutet.[95]

Exempel på länder som har bedömts ha en adekvat skyddsnivå är Japan, Nya Zeeland, Argentina och Schweiz.[96] Mekanismen har också kommit att utvecklas så att kommissionen kan fatta beslut om att överföring till ett tredjeland är tillåtet under vissa villkor, ett så kallat partiellt adekvansbeslut. Det har funnits sådana beslut för överföringar till USA men dessa har ogiltigförklarats.[97] I ett meddelande från kommissionen förtydligas vilka faktorer som ska styra vilka länder som en dialog om beslut ska initieras med. Kriterierna som ska beaktas är bland annat i vilken utsträckning unionen har affärsförbindelser med landet i fråga, hur stort flödet av personuppgifter till landet är, vilken roll landet spelar i fråga om data- och integritetsskydd samt de allmänna politiska förbindelserna med landet vad gäller gemensamma mål och värderingar.[98]

---

[94] Se EU-kommissionen, ’Adequacy decisions’ <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_sv> (besökt 24 februari 2021).
[95] Se förordning (EU) 2016/679 av den 27 april 2016, art. 45.5.
[96] Se EU-kommissionen, ’Adequacy decisions’ <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_sv> (besökt 24 februari 2021).
[97] Se vidare under kapitel 3.
[98] Se kommissionens meddelande ”Utbyte och skydd av personuppgifter i en globaliserad värld”, COM(2017) 7 slutlig, s. 8.

2.2.1 Allmänt om kravet på adekvat skyddsnivå

Det finns ingen exakt definition av vad som utgör en adekvat skyddsnivå, i stället anges i lagtexten ett antal omständigheter som ska beaktas. Definitionen har också utvecklats i praxis av EU-domstolen.[99] Domstolen har till exempel förtydligat att det inte krävs att mottagarlandets skyddsnivå är identisk med den som är fastställd inom unionen.[100] Det handlar snarare om att göra en helhetsbedömning av samtliga faktorer som påverkar integritetsskyddet och se till hur skyddet kan genomföras och verkställas i praktiken. Av de beslut som hittills har fattats framgår att mottagarlandets rättsliga ramar inte nödvändigtvis behöver härröra ur samma rättsliga traditioner som unionens.[101]

2.2.2 Relevant lagstiftning

I art. 45.2 GDPR ställs upp ett flertal omständigheter som kommissionen ska ta hänsyn till i sin bedömning. Art. 29-gruppen har också tagit fram arbetsdokument som förtydligar vad kommissionen ska beakta. Av ett sådant framgår att en analys av tredjelands skyddsnivå ska omfatta en bedömning av innehållet i relevanta regelverk samt vilka medel som finns tillgängliga för att säkerställa efterlevnaden av dessa regelverk.[102]

Vad gäller bedömning av innehållet i relevant lagstiftning, lyfter art. 29-gruppen fram ett antal faktorer som måste finnas. För det första ska det i landet finnas grundläggande dataskyddskoncept som i någon mån speglar innehållet i dataskyddsförordningen. Som exempel på bärande idéer i GDPR lyfts begreppen ’personuppgift’, ’behandling av personuppgifter’, ’personuppgiftsansvarig’ och ’känsliga personuppgifter’.[103] Vidare ska också

[99] Se till exempel EU-domstolens resonemang i mål C-362/14 och C-311/18 samt avsnitt 3.1 och 3.2.
[100] Se C-362/14 *Maximillian Schrems mot Data Protection Commissioner*, EU:C:2015:560, p. 73.
[101] Se kommissionens meddelande ”Utbyte och skydd av personuppgifter i en globaliserad värld”, COM(2017) 7 slutlig, s. 7.
[102] Se art. 29-gruppen, *WP 254 rev.01: Adequacy Referential*.
[103] Ibid. kap. 3.A.

landets regler för personuppgiftsbehandling spegla några av de principer som dataskyddförordningen i mångt och mycket bygger på, så som proportionalitets-, ändamåls- och öppenhetsprincipen samt principen att all personuppgiftsbehandling ska ske på ett legitimt och rättvist sätt. Registrerade bör också tillskrivas rätten att få tillgång till sina uppgifter, samt rätten att ändra dem och få dem raderade. Vad gäller vidare överföring har art. 29-gruppen uttryckt att sådan ska accepteras under förutsättning att den tredje parten också omfattas av samma regler som den initiala mottagaren, så att integritetsskyddet inte undergrävs.[104]

Slutligen ska också beaktas vilka internationella åtaganden landet har, särskilt rörande skydd för personuppgifter. Det typiska för kommissionen att titta på i detta avseende är till exempel att undersöka landets eventuella anslutning till det enda multilaterala instrumentet på området, Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (konvention 108).[105]

2.2.3 Tillsyn, efterlevnad och rättsmedel

Kommissionen ska också ta hänsyn till huruvida det finns en fungerande och relevant tillsynsmyndighet som ser till att dataskyddsregler efterlevs, samt existensen av tillgängliga rättsmedel. Enligt art. 29-gruppen ska somliga element existera för att skyddsnivån ska anses adekvat på detta område. För det första bör det finnas en oberoende tillsynsmyndighet som har till uppgift att överse och verkställa efterlevnad av dataskyddsreglerna. Hänsyn ska också tas till vilka resurser myndigheten har till sitt förfogande, samt dess möjligheter att själva initiera granskningar.[106] För det andra bör landet i fråga också säkerställa efterlevnad av regelverken, dels genom tydlig ansvarsfördelning, dels med andra mekanismer som till exempel sanktioner vid överträdelser. Slutligen bör landet i fråga också tillhandahålla effektiva

[104] Se art. 29-gruppen, *WP 254 rev.01: Adequacy Referential*, kap. 3.A.
[105] Ibid. kap. 1.
[106] Ibid. kap. 3.C.

och billiga rättsmedel för registrerade att använda vid överträdelser och missbruk, inklusive möjlighet att erhålla ekonomisk kompensation.[107]

2.2.4 Offentliga myndigheters åtkomst till personuppgifter

Av art. 45.2(a) GDPR framgår att kommissionen i sin bedömning ska se till all relevant lagstiftning, inkluderat sådan som rör nationell säkerhet, försvar och den åtkomst till personuppgifter som offentliga myndigheter i landet har. Mot bakgrund av domsluten i Schrems I och II tog EDPB fram rekommendationer om nödvändiga garantier för övervakningsåtgärder vid överföringar.[108] Syftet var att förtydliga vilka faktorer som ska beaktas och hur de ska vägas mot varandra, vid bedömningen av om övervakningsåtgärder i ett mottagarland som ger offentliga myndigheter tillgång till personuppgifter kan anses vara motiverade. Rekommendationerna riktade sig främst till nationella dataskyddsmyndigheter då dessa är skyldiga att, på eget initiativ eller efter att ha mottagit klagomål, bedöma enskilda fall och sedan antingen hänskjuta till domstol eller avbryta överföringen om skyddsnivån i mottagarlandet inte kan anses väsentligen likvärdig med EU-rättens.[109]

Enligt EDPB kan de faktorer som ska användas vid bedömningen av om ett ingrepp ska anses motiverat sammanfattas genom fyra garantier.[110] Den första garantin anger att uppgifter bör behandlas utifrån tydliga, precisa och tillgängliga bestämmelser. Det innebär att ett ingrepp ska vara baserat på lagstiftning. Relevanta bestämmelser ska på tydligt sätt precisera omfattningen och tillämpligheten av åtgärden, samt under vilka villkor som åtgärden får vidtas.[111] Europadomstolen har i praxis uttalat att bestämmelser rörande avlyssning av enskild kommunikation och allmänna övervakningsprogram bör ange vilket förfarande som används vid insamling

[107] Se art. 29-gruppen, *WP 254 rev.01: Adequacy Referential*, kap. 3.C.
[108] Se EDPB, *Rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder*.
[109] Ibid. p. 6.
[110] Ibid. p. 24.
[111] Ibid. p. 27-28.

och lagring av uppgifter, en tidsgräns för hur länge åtgärden får vidtas, en definition av den kategori människor som kan komma att bli föremål för övervakning samt skyddsåtgärder för eventuell vidare överföring av uppgifterna.[112]

Den andra garantin anger att nödvändighet och proportionalitet ska säkerställas för legitima mål. Garantin syftar till att spegla innehållet i art. 52.1 EU-stadgan, som anger att begränsningar av grundläggande fri- och rättigheter endast får genomföras om de svarar mot ett erkänt mål av allmänt intresse eller skydd av andra fri- och rättigheter och bedöms som nödvändiga.[113] Vid proportionalitetsprövningen ska hänsyn tas till hur allvarligt ingreppet är samt huruvida betydelsen av det eftersträvade målet står i proportion till ingreppets allvarlighet.[114] EU-domstolen konstaterade i målet *La Quadrature du Net* att syftet att skydda nationell säkerhet kan motivera mer långtgående åtgärder än exempelvis åtgärder i brottsbekämpande syften, under förutsättning att det kan visas att det föreligger ett hot mot den nationella säkerheten.[115]

Enligt den tredje garantin bör det finnas en oberoende tillsynsmekanism. EU-domstolen har i praxis angett att vissa åtgärder som utgör en begränsning av de grundläggande fri- och rättigheterna endast är lagenliga om de är föremål för kontroll av antingen domstol eller förvaltningsmyndighet. Kontrollen ska säkerställa att det föreligger en situation som motiverar åtgärden, att villkoren för att vidta åtgärden är uppfyllda och att skyddsåtgärder tillämpas.[116] En tillsynsmyndighet ska vara oberoende i mening att den är självständig i förhållande till den verkställande makten.[117]

---

[112] Se *Weber och Saravia v. Tyskland*, no. 54934/00, ECHR 2006-XI, § 95.
[113] Se EDPB, *Rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder*, p. 32.
[114] Ibid. p. 33.
[115] Se förenade målen C-511/18, C-512/18 och C-520/18 *La Quadrature du Net mot Premier ministre m.fl.*, EU:C:2020:791.
[116] Ibid. p. 168 & 189.
[117] Se EDPB, *Rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder*, p. 42.

Den fjärde och sista garantin anger att enskilda personer ska ha tillgång till effektiva rättsmedel. Garantin syftar till att säkerställa att enskilda har möjlighet att klaga hos domstol eller motsvarande organ om denne anser att en åtgärd på något sätt har kränkt dennes grundläggande rättigheter.[118] EU-domstolen har konstaterat att en registrerad även bör informeras om att insamlingen har skett för att få möjlighet att utöva sina rättigheter.[119] Domstolen har även angett att kraven enligt art. 47 EU-stadgan ska vara uppfyllda, vilket innebär att domstolen ska vara oavhängig i förhållande till den verkställande makten och ha befogenhet att fatta bindande beslut i förhållande till relevanta myndigheter.[120]

[118] Se EDPB, *Rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder*, p. 43 & 47.
[119] Se förenade målen C-511/18, C-512/18 och C-520/18 *La Quadrature du Net mot Premier ministre m.fl.*, EU:C:2020:791, p. 190.
[120] Se C-311/18 *Data Protection Commissioner mot Facebook Irland Ltd och Maximillian Schrems*, EU:C:2020:559, p. 195-196.

3 USA - ogiltigförklarade beslut

När det kommer till tredjelandsöverföringar och adekvansbeslut har USA stått i rampljuset den senaste tiden. På grund av de olika rättsliga traditionerna och varierande synerna på integritets- och dataskydd, har kommissionen fattat så kallade partiella adekvansbeslut för USA:s del.[121] USA saknar nämligen en generell dataskyddslag motsvarande dataskyddsförordningen och hanterar integritetsskydd på ett annorlunda sätt än EU.[122] På grund av affärsförbindelserna USA och EU emellan har det dock funnits en stark gemensam vilja att skapa grunder för att möjliggöra överföring av data över Atlanten.[123] Denna vilja har lett till två beslut, Safe Harbor och Privacy Shield. Båda besluten har ogiltigförklarats av EU-domstolen, och därför har samarbetet återupptagits på nytt för att träffa en överenskommelse som lever upp till de EU-rättsliga kraven.[124]

3.1 Safe Harbor och Schrems I

3.1.1 Safe Harbors innehåll och principer

Med strävan att underlätta affärsverksamhet och handel mellan USA och EU, arbetade parterna under slutet av 90-talet gemensamt fram en mekanism som kom att kallas för *Safe Harbor*. En organisation som önskade ta emot data

[121] Se pressmeddelande från kommissionen, ’Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers’ <https://ec.europa.eu/commission/presscorner/detail/sv/MEMO_17_15> (besökt 8 mars 2021).
[122] Se kommissionens genomförandebeslut 2000/520/EG, bilaga I, s. 1.
[123] Se kommissionens meddelande ”Om överföring av personuppgifter från EU till Amerikas förenta stater enligt direktiv 95/46/EG med anledning av domstolens dom i mål C-362/14 (Schrems)”, COM(2015) 566 slutlig, s. 2.
[124] Se pressmeddelande från EU-kommissionär Didier Reynders och USA:s dåvarande handelsminister Wilbur Ross, ’Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross’ <https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_sv> (besökt 24 mars 2021).

från EU kunde på frivillig basis ansluta sig till systemet och på så sätt bli godkänd för personuppgiftsöverföring. Syftet med anslutning till Safe Harbor var att organisationerna skulle uppfylla den presumtion om adekvat skyddsnivå som principerna och tillhörande skäl skapade.[125]

Genom att ansluta sig till Safe Harbor åtog sig berörd organisation att efterleva sju principer.[126] Den första, meddelandeprincipen, utgjorde ett krav på transparens, där organisationen i fråga skulle meddela den enskilde att personuppgifter samlades in och behandlades, i vilket syfte insamlingen skedde, den registrerades rättigheter samt var denne kunde vända sig med frågor eller klagomål. Enligt valmöjlighetsprincipen skulle den enskilde ges möjlighet att välja dels om dennes uppgifter skulle få utlämnas till en tredje part, dels om uppgifterna kunde användas till ett ändamål som sträckte sig utanför det syfte som uppgifterna ursprungligen hade samlats in för. Den tredje principen angav att uppfyllandet av principerna om meddelande och valmöjlighet var ett villkor för att överhuvudtaget få överföra uppgifter vidare till tredje part. Om en tredje part agerade på uppdrag av den anslutna organisationen, var organisationen också skyldig att säkerställa att tredje part antingen var ansluten till Safe Harbor, eller säkerställde en adekvat skyddsnivå på annat vis.

Principen om säkerhet innebar att alla organisationer som behandlade personuppgifter enligt Safe Harbor var skyldiga att vidta sådana försiktighetsåtgärder att personuppgifter inte riskerade att försvinna, missbrukas eller förstöras. Den femte principen uttryckte ett krav på att organisationerna inte fick använda personuppgifterna till något annat än det ändamål som de ursprungligen samlats in för, så till vida inte den enskilda gett sin tillåtelse. Tillgångsprincipen innebar att registrerade skulle ha samma tillgång till sina personuppgifter som den behandlande organisationen, samt rätten att både rätta uppgifterna och få dem raderade.

[125] Se kommissionens genomförandebeslut 2000/520/EG, bilaga I, 2 st.
[126] Ibid. bilaga I.

Den sista principen i Safe Harbor berörde de mekanismer som ansågs nödvändiga för att säkerställa efterlevnaden av integritetsskyddet. Mekanismerna skulle omfatta lättillgängliga rättsmedel för handläggning av enskildas klagomål, kontroll av de anslutna organisationernas åtgärder för att leva upp till integritetsskyddet samt åtgärder samt påföljder för problem som uppstått till följd av att organisationerna inte levt upp till principerna.

Utöver principerna bestod beslutet dessutom av vägledande frågor och svar utfärdade av USA:s regering.[127] Av dessa framgick att anslutna organisationer i viss mån kunde uppfylla principen om genomförande och uppföljning genom att samtycka till ett samarbete med de europeiska dataskyddsmyndigheterna, men att ett sådant åtagande var på frivillig basis.[128] Vidare förtydligade också frågorna samt tillhörande svar att Safe Harbor byggde på ett självcertifieringssystem. Det innebar i praktiken att organisationerna själva anmälde sig till det amerikanska handelsministeriet med uppgifter om hur de arbetade med sitt integritetsskydd, vilken kontrollmekanism som skulle användas, förfarande för att lösa tvister vid klagomål och lite därtill. Efter en sådan anmälan var det tillåtet för den anslutna organisationen att ta emot personuppgifter från EU:s medlemsstater.[129] Den amerikanska regeringen yttrade sig också i frågan vad gällde eventuella konflikter mellan uppfyllandet av Safe Harbor-principerna och amerikansk lag. Den amerikanska regeringen uppgav gällande denna konflikt att de organisationer och företag som anslutit sig till systemet behövde göra avsteg från efterlevnaden av principerna i den mån det var nödvändigt för att följa amerikansk lag.[130]

[127] Se kommissionens genomförandebeslut 2000/520/EG, skäl 5.
[128] Ibid. bilaga II, FoS 5.
[129] Ibid. bilaga II, FoS 6.
[130] Ibid. bilaga IV, p. B.

3.1.2 Kritiken och ogiltigförklaringen av Safe Harbor

Safe Harbor kom dock att bli föremål för kritik.[131] I ett meddelande från EU-kommissionen själv, framhölls att europeiska medborgares rätt till privatliv och skydd för personuppgifter hotades av amerikanska underrättelsetjänsters övervakningsverksamhet och storskaliga insamling av personuppgifter. Av meddelandet framkom att en majoritet av de företag som var berörda av amerikanska övervakningsprogram var certifierade enligt Safe Harbor-systemet.[132] Man menade att systemet därför behövde ses över i syfte att återuppbygga förtroendet för transatlantiska överföringar av personuppgifter och förhindra en misstro mot den växande digitala ekonomin, då en sådan misstro riskerade att skapa negativa konsekvenser för tillväxten.[133] I ett efterföljande meddelande från kommissionen framkom ytterligare kritik mot Safe Harbor-beslutet. Till exempel framgick att en väsentlig andel av de anslutna företagen inte alls eller bara till viss del följde principerna.[134] Dessutom uppgav kommissionen att tillgången till prövningsmekanismer och rättsmedel var kraftigt begränsade för EU-medborgare.[135]

Så småningom kom giltigheten av beslutet om Safe Harbor att prövas i EU-domstolen i och med målet som kom att få namnet Schrems I.[136] Dataskyddsaktivisten och juristen Maximilian Schrems var likt många andra en användare av den sociala plattformen Facebook. Han lämnade in ett klagomål till ombudsmannen då han ansåg det vara felaktigt att Facebook tilläts skicka uppgifter till servrar i USA. Detta gjorde han bland annat mot bakgrund av de avslöjanden som gjordes av Edward Snowden 2013 om de amerikanska underrättelsetjänsternas verksamhet. Schrems ansåg att den data

[131] Se kommissionens meddelande ”Återskapande av förtroendet för dataflödet mellan EU och Förenta staterna”, KOM(2013) 846 slutlig.
[132] Ibid. s. 4.
[133] Ibid. s. 2 f.
[134] Se kommissionens meddelande “om hur principerna om integritetsskydd (Safe Harbor) fungerar när det gäller EU:s medborgare och företag som är etablerade i EU”, KOM(2013) 847 slutlig, s. 8 f.
[135] Ibid. s. 18.
[136] C-362/14 *Maximillian Schrems mot Data Protection Commissioner*, EU:C:2015:560.

som överfördes inte skyddades mot eventuell myndighetsövervakning. Klagomålet avslogs med motiveringen att överföring av personuppgifter till USA genom beslut ansetts säkerställa en adekvat skyddsnivå så till vida det skedde i enlighet med Safe Harbor-systemet.[137] Målet kom dock så småningom upp till Irlands högsta domstolsinstans, som skickade frågan om huruvida Safe Harbor skulle anses säkerställa en adekvat skyddsnivå vidare till EU-domstolen.

Förfarandet vid den irländska domstolen och EU-domstolen skedde innan dataskyddsförordningens ikraftträdande och frågorna behandlades därför enligt regleringen i direktiv 95/46/EG. Formuleringen av den artikel som reglerade beslut om adekvat skyddsnivå var dock snarlik den idag gällande regleringen i dataskyddsförordningen.

Målet behandlade huvudsakligen två frågor. Den första frågan handlade om huruvida ett beslut som Safe Harbor utgör ett hinder för en nationell tillsynsmyndighet att utreda en klagandes begäran rörande skydd för sina personuppgifter vid överföring av dessa till ett land, vars regelverk klaganden anser inte uppfyller kravet på en adekvat skyddsnivå.[138]

Domstolen kom fram till att ett sådant beslut inte utgjorde ett hinder för en utredning i frågan av den nationella tillsynsmyndigheten. Domstolen menade att ett beslut fattat av kommissionen enligt art. 25.6 i direktiv 95/46/EG[139] visserligen är bindande för medlemsstaterna och att de ska vidta de åtgärder som är nödvändiga för att följa beslutet, men att det följer av art. 8 EU-stadgan samt art. 28 i direktiv 95/46/EG att de nationella tillsynsmyndigheterna har befogenhet att utreda om en överföring till tredjeland uppfyller unionsrättens krav.[140]

[137] Se C-362/14 *Maximillian Schrems mot Data Protection Commissioner*, EU:C:2015:560, p. 28 och 29.
[138] Ibid. p. 37.
[139] Motsvarande art. 45.3 GDPR.
[140] Se C-362/14 *Maximillian Schrems mot Data Protection Commissioner*, EU:C:2015:560, p. 47, 51, 63 & 66.

Domstolens huvudsakliga prövning handlade dock om giltigheten av beslutet om Safe Harbor, och dess uppfyllelse av unionsrättens krav på överföringar av personuppgifter till tredjeland samt det grundläggande skyddet för privatliv och personuppgifter. Inledningsvis konstaterade domstolen att lagstiftningen saknar en definition av begreppet adekvat skyddsnivå, men att det i praktiken innebär att mottagarlandet genom intern lagstiftning och/eller internationella åtaganden ska säkerställa en nivå som är väsentligen likvärdig med det skydd som finns inom EU. Syftet med bestämmelsen och dess formulering är att upprätthålla det höga skydd för personuppgifter som tillhandahålls inom unionen och undvika ett kringgående av skyddet.[141] Formuleringen *väsentligen likvärdig skyddsnivå* innebär dock att mottagarlandets skydd för personuppgifter inte nödvändigtvis behöver vara identiskt med unionens. Enligt domstolen kan landet i fråga använda sig av andra medel jämfört med de använda inom unionen, bedömningen ska utgå från om resultatet i praktiken medför en väsentligen likvärdig skyddsnivå.[142] Därutöver framhöll domstolen, bland annat med hänvisning till Digital Rights Ireland-målet, att kommissionens möjligheter att göra en skönsmässig bedömning av ett tredjelands skyddsnivå är begränsade, med hänsyn till det stora antal människor som riskerar att få rätten till sina privatliv kränkt.[143]

EU-domstolen ogiltigförklarade beslutet om Safe Harbor av ett flertal anledningar. Den första berörde beslutets form av ett så kallat självcertifieringssystem. Formen som sådan strider inte nödvändigtvis mot kravet på att ett tredjeland ska säkerställa en adekvat skyddsnivå genom intern lagstiftning eller internationella förpliktelser, men är däremot beroende av fungerande kontroll- och tillsynsmekanismer som kan upptäcka eventuella överträdelser av de principer företagen åtagit sig att efterleva. Självcertifieringsmekanismen medför också att det endast är de företag och

[141] Se C-362/14 *Maximillian Schrems mot Data Protection Commissioner*, EU:C:2015:560, p. 73.
[142] Ibid. p. 73-74.
[143] Ibid. p. 78.

organisationer som har anslutit sig till den som är bundna av beslutet och dess principer, till skillnad från de amerikanska myndigheterna.[144]

Ytterligare anledning till att beslutet förklarades ogiltigt var just Safe Harbor-principernas status i förhållande till amerikansk lagstiftning. I beslutet uttrycktes att amerikanska organisationer och företag oavsett om de anslutit sig till Safe Harbor eller ej, är tvungna att följa lagen. Dessutom angav beslutet att krav från amerikanska myndigheters håll vad gäller nationell säkerhet, rättsefterlevnad och allmänintresse skulle ges företräde framför Safe Harbor-principerna.[145] Sammantaget möjliggjorde dessa regleringar ingrepp i det personliga integritetsskyddet enligt EU-domstolen. Undantag och begränsningar från privatlivs- och personuppgiftsskyddet ska endast uppgå till vad som kan anses vara strikt nödvändigt, och enligt domstolen var den amerikanska hanteringen av personuppgifter av alltför generell karaktär för att anses godtagbar ur ett EU-rättsligt perspektiv.[146] Avslutningsvis pekade domstolen också på det faktum att då amerikansk lagstiftning saknar en möjlighet för icke-amerikanska medborgare att vidta rättsmedel vid inskränkningar i integritets- och personuppgiftsskyddet, uppfylldes inte rätten till ett effektivt domstolsskydd som garanteras i art. 47 EU-stadgan.[147]

3.2 Privacy Shield och Schrems II

3.2.1 Privacy Shields innehåll och principer

Efter att Safe Harbor ogiltigförklarats av EU-domstolen gjordes ett nytt försök att möjliggöra överföringar till USA genom ett beslut som kom att kallas för *Privacy Shield*.[148] Tanken med beslutet var att anpassa mekanismen

[144] Se C-362/14 *Maximillian Schrems mot Data Protection Commissioner*, EU:C:2015:560, p. 81-82.
[145] Se kommissionens genomförandebeslut 2000/520/EG, bilaga I, 4 st.
[146] Se C-362/14 *Maximillian Schrems mot Data Protection Commissioner*, EU:C:2015:560, p. 91-93.
[147] Ibid. p. 95.
[148] Se kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016.

utifrån den kritik som riktats mot Safe Harbor i kommissionens meddelande samt Schrems I.[149] Strukturmässigt utgjordes beslutet av 115 skäl, sex artiklar och fyra bilagor. Bedömningen av huruvida skyddsnivån numera skulle anses adekvat utgick från fyra huvudsakliga områden: principerna, tillsyn och efterlevnad, klagomål och prövning samt Förenta staternas myndigheters tillgång till och användning av de personuppgifter som överförts inom ramen för skölden av privatlivet.

De grundläggande principerna var huvudsakligen desamma som de presenterats i beslutet om Safe Harbor. Skillnaden bestod i att principernas innehåll utvecklades och blev mer detaljerat i fråga om organisationernas skyldigheter i förhållande till respektive princip.[150] Däremot gjordes ett krafttag vad gällde tillsyn och efterlevnad. I och med det nya beslutet fick till exempel det amerikanska handelsministeriet en framträdande roll, då de fick i uppgift att upprätta och offentligt tillhandahålla en förteckning över de företag och organisationer som var anslutna till skölden. Handelsministeriet uppdrogs också att kontinuerligt göra efterlevnadskontroller, både på eget initiativ och efter att ha mottagit klagomål.[151]

Vad gällde just klagomålshantering och prövningsmekanismer, framhöll beslutet att registrerade hade ett flertal möjligheter att använda sig av vid missnöje. Exempelvis kunde en registrerad framställa klagomål direkt till den behandlande organisationen, till tvistlösningsorgan som utsetts av organisationen, dataskyddsmyndigheter i den egna medlemsstaten eller till FTC (*Federal Trade Commission*). Om en lösning inte skulle kunna nås genom någon av dessa instanser, erhöll den registrerade också möjligheten att begära ett skiljedomsförfarande hos arbetsgruppen för Privacy Shield.[152] Därutöver åtog sig också amerikanska handelsministeriet uppdraget att efter bästa förmåga hantera och lösa klagomål från enskilda.[153]

[149] Se kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016, skäl 7.
[150] Ibid. bilaga II.
[151] Ibid. skäl 31-37.
[152] Ibid. skäl 41-42.
[153] Ibid, skäl 52.

En väsentlig del av beslutet om Privacy Shield berörde tillgång till och användning av personuppgifter av de amerikanska myndigheterna till ändamål för intressen rörande nationell säkerhet, brottsbekämpning och andra syften av allmänt intresse. Kommissionen ansåg att den amerikanska lagstiftningen innehöll tydliga begränsningar samt tillhandahöll ett tillräckligt rättsligt skydd mot eventuella ingrepp och missbruk.[154] I skälen framhölls de begränsningar som amerikanska underrättelsetjänster har att förhålla sig till genom bland annat PPD-28, ett direktiv som är av särskild betydelse för icke-amerikanska medborgare. Exempel på sådana begränsningar är till exempel legalitetskravet vid insamling genom signalspaning, att insamling endast får ske för vissa specifika ändamål samt de interna prioriteringsregler som uppger att underrättelsetjänster ska prioritera riktad insamling över bulkinsamling.[155] Kommissionens bedömning var sammanfattningsvis att den amerikanska lagstiftningen och utfästelserna från regeringen nu kunde säkerställa en adekvat skyddsnivå i enlighet med vad domstolen hade yttrat i Schrems I.[156]

För att möta kritiken mot bristande tillgång till rättsmedel, beslutade USA även att införa en oberoende ombudsman. Ombudsmannens huvudsakliga uppgift gick ut på att utreda, granska och lösa klagomål samt säkerställa att registrerade fick en oberoende prövning av huruvida den amerikanska lagstiftningen hade följts.[157] På basis av ombudsmannamekanismens införande ansåg kommissionen att USA kunde garantera ett rättsligt skydd mot ingrepp i integritetsskyddet av de amerikanska underrättelsetjänsterna.[158]

3.2.2 Ogiltigförklaringen av Privacy Shield

Så småningom kom även Privacy Shield-beslutet att bli föremål för prövning i EU-domstolens kammare, även denna gång drivet av Maximilian Schrems. Schrems ansåg, trots beslutet om Privacy Shield, att den personliga data som

[154] Se kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016, skäl 67.
[155] Ibid, skäl 69-71.
[156] Ibid, skäl 90.
[157] Ibid, skäl 117-121.
[158] Ibid. skäl 123.

överfördes till USA kunde bli föremål för övervakning och att USA således inte säkerställde en adekvat skyddsnivå.

Vad gällde huruvida Privacy Shield-beslutet skulle anses säkerställa en adekvat skyddsnivå konstaterade domstolen inledningsvis, mot bakgrund av stadgan, att tillgång till personuppgifter för lagring eller behandling påverkar den grundläggande rätten till respekt för privatlivet. Att uppgifterna är av så kallad känslig karaktär eller inte är irrelevant; ett utlämnande av uppgifter till tredje man, till exempel en myndighet, utgör ett ingrepp mot de grundläggande rättigheterna som fastslås i art. 7 och 8 i EU-stadgan.[159] Domstolen fastslog att skyddet för privatliv och personuppgifter inte är absoluta rättigheter. Begränsande åtgärder får vidtas under förutsättning att de inte kränker det väsentliga innehållet i rättigheterna, och i den utsträckning som de är nödvändiga i enlighet med proportionalitetsprincipen och i syfte att tillgodose ett annat allmänt samhällsintresse som erkänts av unionen. Lagstiftningen som möjliggör ingreppet måste därutöver vara preciserad och ange vilka omständigheter som rättfärdigar behandlingen och vilka åtgärder som får vidtas.[160]

Domstolens främsta fokus i bedömningen av Privacy Shields giltighet handlade om huruvida de övervakningsprogram som används i USA omfattades av sådana krav som säkerställer en väsentligen likvärdig skyddsnivå. Vad gällde avsnitt 702 i FISA som utgör grunden för ett flertal amerikanska övervakningsprogram, uttryckte domstolen att det inte var möjligt att uttolka några begränsningar i behörigheten att inhämta utländska underrättelseuppgifter.[161] Samma sak konstaterades gälla för de övervakningsprogram som stödjer sig på dekret E.O. 12333 och möjliggör tillgång till uppgifter som är i transit till USA. Vid användning av övervakningsprogrammen ska underrättelsetjänsterna iaktta PPD-28, som i Privacy Shield återkommande lyftes fram som en begränsning av

[159] Se C-311/18 *Data Protection Commissioner mot Facebook Irland Ltd och Maximillian Schrems*, EU:C:2020:559, p. 170 & 171.
[160] Ibid. p. 172-176.
[161] Ibid. p. 180.

underrättelsetjänsternas befogenheter. Domstolen pekade dock på det faktum att PPD-28 också möjliggör så kallad bulkinsamling av personuppgifter, och att denna möjlighet inte var fastställd så att dess omfattning var tydligt och precist reglerad.[162] Domstolen menade att de åtgärder som möjliggjorde offentliga myndigheters åtkomst till personuppgifter inte var begränsade till vad som var strikt nödvändigt, och således stred mot proportionalitetsprincipen.

Domstolen framhävde att rätten till en effektiv domstolsprövning vid överträdelser av grundläggande fri- och rättigheter enligt unionsrätten är en grundförutsättning för en rättsstat. Domstolen menade vidare att det, framför allt vid överföringar av personuppgifter till tredjeland, är av betydelse vilka möjligheter till rättslig prövning en unionsmedborgare har i tredjelandet, då medlemsstaternas myndigheter kan ha begränsade befogenheter vid klagomål som gäller behandlingen av personuppgifter i tredjeland.[163] Som nämnt ovan motiverade kommissionen beslutet vad gäller möjligheten till rättslig prövning bland annat med inrättandet av en oberoende ombudsman. Domstolen konstaterade dock för det första att ombudsmannen utses av utrikesministern och utgör en del av USA:s försvarsdepartement, men också att det inte finns några garantier för att ombudsmannens befogenheter inte kan återkallas eller förändras. Ombudsmannen har heller inte, som påpekas i domen, befogenheter att fatta bindande beslut i förhållande till de amerikanska myndigheterna.[164] Mot bakgrund av ovanstående argument konstaterade domstolen att den mekanism med ombudsman som tillhandahålls i och med Privacy Shield, inte utgör ett väsentligen likvärdigt skydd som det som erhålls enligt art. 47 i EU-stadgan. Domstolen kunde också konstatera att FISA inte lämnade några garantier för icke-amerikanska medborgare som omfattades av övervakningsprogrammen.[165] Inte heller E.O.

[162] Se C-311/18 *Data Protection Commissioner mot Facebook Irland Ltd och Maximillian Schrems*, EU:C:2020:559, p. 182-183.
[163] Ibid, p. 187 & 189.
[164] Ibid. p. 195-197.
[165] Ibid, p. 180.

12333 eller PPD-28 medgav några rättigheter för EU-medborgare som kunde göras gällande i domstol gentemot amerikanska myndigheter.[166]

Sammanfattningsvis landade domstolen i att kommissionen genom beslutet om Privacy Shield och konstaterandet av en adekvat skyddsnivå i USA, inte levde upp till kraven i art. 45.1 GDPR mot bakgrund av artiklarna 7, 8 och 47 i EU-stadgan.[167] Privacy Shield ogiltigförklarades därmed, och var pågående diskussion om en lösning för framtida överföringar kommer att landa är troligen långt ifrån klart.

3.2.3 USA:s reaktion efter Schrems II

Åsikterna och diskussionerna om Schrems II och dess konsekvenser harvarit omfattande. Det amerikanska handelsdepartementet publicerade i september 2020 en vitbok i syfte att tydliggöra information om integritetsskydd i USA och den verksamhet som rör myndigheters tillgång till data som samlas in i syfte att skydda nationell säkerhet.[168] Vitboken ämnade framför allt att hjälpa företag som överför data till USA genom användning av standardavtalsklausuler och tillhandahålla närmare information om de områden EU-domstolen bedömt som problematiska.[169]

Inledningsvis framhävde amerikanska handelsdepartementet det faktum att amerikanska underrättelsetjänsters åtkomst till data under dekret E.O. 12333 eller FISA avsnitt 702 inte är ett problem i praktiken, eftersom majoriteten av den data som överförs till amerikanska företag inte är av intresse för underrättelsetjänsterna. Enligt handelsdepartementet skiljer sig den teoretiska möjligheten för amerikanska underrättelsetjänster att få åtkomst till data inte från andra staters, inkluderat EU:s medlemsstaters, underrättelsetjänsters

[166] Se C-311/18 *Data Protection Commissioner mot Facebook Irland Ltd och Maximillian Schrems*, EU:C:2020:559, p. 181, 182 & 192.
[167] Ibid, p. 198.
[168] Se amerikanska handelsdepartementet, '*White Paper – Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II'*.
[169] Ibid. s. 1.

möjligheter att få tillgång till data.[170] På samma tema uttryckte handelsdepartementet att ett flertal övervakningsprogram bland EU:s medlemsstater ger samma eller mer långtgående befogenheter än vad FISA gör, och att data som överförs till USA därför ges ett likvärdigt eller större integritetsskydd än vad som kan tillhandahållas av vissa medlemsstater i EU.[171]

Avslutningsvis framhöll det amerikanska handelsdepartementet att det finns ett flertal skyddsåtgärder och rättsmedelsverktyg relevanta för de amerikanska underrättelsetjänsternas verksamhet som inte uppmärksammades av EU-domstolen i Schrems II.[172]

[170] Se amerikanska handelsdepartementet '*White Paper – Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II'*, s. 2 f.
[171] Ibid, s. 15 f.
[172] Ibid, s. 22.

4 Skydd av personuppgifter i Storbritannien

I och med Storbritanniens utträde ur EU och övergångsperiodens slut, är landet inte längre bundet av EU-rättslig reglering. Unionen och Storbritannien har dock uttryckt att avsikten är att även fortsättningsvis samarbeta på ett flertal områden. Att möjliggöra dataflöden genom säkerställandet av en hög dataskyddsnivå är ett exempel på vad parterna har kommit överens om att gemensamt sträva efter.[173] Redan av en deklaration framtagen under övergångsperioden från EU-kommissionens arbetsgrupp gällande framtida samarbete, framgick att målet var att ta fram ett beslut om adekvat skyddsnivå för Storbritanniens räkning.[174]

Ett utkast till beslut publicerades av kommissionen den 19 februari 2021 och utgör det första steget mot ett sådant beslut. Därefter har EDPB publicerat ett yttrande över förslaget den 13 april 2021. Vad som återstår är att få utkastet godkänt av en kommitté med representanter från medlemsstaterna, innan ett beslut kan fattas.[175]

Förslaget kommer presenteras utifrån följande områden: konstitutionellt ramverk och nationella dataskyddsregler, tillsyn och rättsmedel samt offentliga myndigheters åtkomst till uppgifter.

[173] Se kommissionens arbetsgrupp för förberedelser och förhandlingar inför Storbritanniens utträde under art. 50 EUF (Task Force for the preparation and conduct of the negotiations with the United Kingdom under art. 50 TEU), "Politisk förklaring om de framtida förbindelserna mellan Europeiska unionen och Förenade Kungariket", EUT 2019 C 384 I/02, p. 8-9.
[174] Ibid.
[175] Se EU-kommissionen, 'Brexit' <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/brexit_sv> (besökt 28 februari 2021).

4.1 Kommissionens förslag till beslut om adekvat skyddsnivå

4.1.1 Konstitutionellt ramverk och nationellt dataskydd

Kommissionen inleder sin bedömning med en granskning av Storbritanniens konstitutionella uppbyggnad. Den uppger att Storbritannien är en demokrati som har ett suveränt parlament överordnat alla andra statliga institutioner, ett oberoende rättsväsende samt en verkställande makt som får sin befogenhet från och svarar inför parlamentet.[176] Lagstiftningen på dataskyddsområdet gäller över hela landet, det vill säga England, Wales, Skottland och Nordirland. Viss lagstiftning relevant för bedömningen av skyddsnivån, som till exempel om rättsväsendet, är dock delegerad till respektive lagstiftande organ i de olika riksdelarna.[177]

Storbritannien har ingen skriven konstitution. Grundläggande principer har i stället utvecklats över tid genom rättspraxis och det faktum att domstolarna har erkänt värdet av författningar så som Magna Carta, Bill of Rights och Human Rights Act. Vad gäller grundläggande rättigheter är Storbritannien anslutet till EKMR sedan 1951. EKMR har inkorporerats i landets lag genom införandet av the Human Rights Act 1998.[178] Landet är också anslutet till Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter sedan 1987.[179]

[176] Se EU-kommissionens utkast till beslut om adekvat skyddsnivå för Storbritannien, ”Commission Implementing Decision of XXX pursuant Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom”, skäl 7.
[177] Ibid. skäl 8.
[178] Ibid. skäl 9.
[179] Ibid. skäl 8.

Det ska dock noteras att Storbritannien i och med sitt utträde inte längre kommer vara bundna av EU-stadgan.[180] Den brittiska avdelningen för utträdesprocessen menade dock att intentionen var att enskildas rättigheter inte skulle komma att påverkas på ett substantiellt sätt, utan att de grundläggande fri- och rättigheterna redan var eller skulle bli inkorporerade i den brittiska lagstiftningen alternativt följa av landets internationella åtaganden.[181]

Inför sitt utträde ur unionen antog Storbritannien *the European Union (Withdrawal) Act 2018*. I och med detta antagande importerade Storbritannien i princip dataskyddsförordningen och skapade med mindre anpassningar sin egen variant, UK GDPR.[182] Implementeringen av nämnda innebär att den grundläggande strukturen i GDPR och dess begrepp och principer numera också finns självständigt i den brittiska lagstiftningen. Sedan tidigare finns också den nationella författningen Data Protection Act 2018.[183] DPA 2018 instiftades ursprungligen för att införliva den av Europarådet antagna konventionen om skydd för automatisk behandling för personuppgifter. Numera är det dock den huvudsakliga regleringen för hantering och skydd av personuppgifter i Storbritannien.[184] Det ska tilläggas att genom befogenheter givna genom respektive akt, har ministrarna möjlighet att besluta om sekundärlagstiftning för att ändra eller göra tillägg till vissa bestämmelser.[185]

Förutom den allmänna behandlingen av personuppgifter, innefattar DPA 2018 också reglering för behandling av personuppgifter för brottsbekämpande myndigheter samt underrättelsetjänster.[186] Dessa delar

[180] Se Storbritanniens regering (Department for Exiting the European Union), '*Legislating for the United Kingdom's withdrawal from the European Union'*, 2 kap. 23 p.
[181] Ibid. 2 kap. 25 p.
[182] Se EU-kommissionens utkast till beslut om adekvat skyddsnivå för Storbritannien, skäl 12.
[183] Ibid. skäl 11.
[184] Se ICO, 'About the DPA 2018' <https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/#1> (besökt 20 april 2021).
[185] Se EU-kommissionens utkast till beslut om adekvat skyddsnivå för Storbritannien, skäl 13 & 16.
[186] Se DPA 2018, avdelning 3 och 4.

som berör offentliga myndigheters tillgång till uppgifter kommer att behandlas nedan i avsnitt 4.3.

Sammanfattningsvis finner man de grundläggande rättigheterna vad gäller skydd för privatliv och personuppgifter i Storbritannien i UK GDPR och DPA 2018. EU-kommissionen framhåller i sitt förslag att det brittiska ramverket vad gäller struktur och huvudkomponenter för databehandling är mycket likt det som tillämpas inom EU. Detta dels på grund av att den nationella lagstiftningen på området i mångt och mycket har formats av EU-rätten, dels på grund av landets bundenhet till internationella instrument så som EKMR och Europarådets konvention 108.[187]

I DPA 2018 medger den brittiska lagstiftningen vissa begränsningar av de individuella rättigheterna som ger registrerade rätten till tillgång, ändring, och radering av personuppgifter bland annat. Begränsningarna är utformade för att endast kunna användas under vissa specifika omständigheter, och under förutsättning att det är nödvändigt och proportionerligt i förhållande till syftet. Till exempel tillhandahålls möjligheten att begränsa de individuella rättigheterna i samband med behandling av personuppgifter vid invandringskontroller. Brittisk domstol har uttryckt att begränsningen är en fråga som är menad att tillgodose ett allmänt samhällsintresse och legitimt syfte. [188] Kommissionen framhåller att begränsningen visserligen är vid till sin formulering, men att praxis och riktlinjer från ICO också ställer upp strikta krav på användningen av undantaget och därmed kan anses godtagbart.[189]

[187] Se EU-kommissionens utkast till beslut om adekvat skyddsnivå för Storbritannien, skäl 18.
[188] Ibid. skäl 62.
[189] Ibid. skäl 65.

4.1.2 Efterlevnad, verkställighet och tillgängliga rättsmedel

Ansvaret för att databehandling i Storbritannien sker i enlighet med UK GDPR och DPA 2018 ligger hos en *Information Commissioner* (hädanefter endast benämnd som IC). IC ska agera som en självständig och oberoende juridisk enhet, och inte ta emot vare sig instruktioner eller råd från externa parter. Till stöd har IC myndigheten *Information Commissioner's Office*.[190] IC:s uppgifter handlar i stort om att upprätthålla efterlevnad av dataskyddslagstiftning, informera allmänheten om dataskydd och rättigheter, agera rådgivare till parlamentet och andra relevanta institutioner vad gäller lagstiftnings- och administrativa åtgärder på dataskyddsområdet, hantera inkomna klagomål samt granska behandlare av personuppgifter.[191] Befogenheterna och uppgifterna är alltså motsvarande de som tillsynsmyndigheter inom EU har.[192] Vid överträdelser och bristande efterlevnad har IC också rätten att dela ut varningar, reprimander, besluta om begränsning eller förbud mot behandling av personuppgifter samt påföra administrativa sanktionsavgifter m.m.[193]

En viktig aspekt av huruvida ett beslut om adekvat skyddsnivå kan fattas är de registrerades möjlighet och tillgång till rättsmedel och någon form av domstolsprövning, i enlighet med art. 47 EU-stadgan. Om en registrerad anser att personuppgiftsbehandlingen inte har skett på ett lagenligt vis, har denne ett flertal möjligheter att söka upprättelse på.

Först och främst kan man vända sig till ICO för att lämna klagomål. Motsvarande tillsynsmyndigheternas roll enligt dataskyddsförordningen, är ICO skyldigt att utreda klagomålet och bedöma den behandlande aktörens

[190] Se EU-kommissionens utkast till beslut om adekvat skyddsnivå för Storbritannien, skäl 86-87.
[191] Ibid. skäl 91.
[192] Jfr förordning (EU) 2016/679 av den 27 april 2016, art. 57.
[193] Se EU-kommissionens utkast till beslut om adekvat skyddsnivå för Storbritannien, skäl 92.

regelefterlevnad. Som har nämnts ovan har ICO befogenhet att vidta åtgärder så som utdelning av böter, om en överträdelse kan konstateras.[194] För det andra har man också rätten att klaga hos domstol om man har fått ett beslut emot sig av IC eller anser att ett inlämnat klagomål inte har hanterats på ett korrekt sätt.[195]

UK GDPR och DPA 2018 tillhandahåller också möjligheten för registrerade att klaga direkt inför domstol. Om domstolen kan fastställa att en överträdelse har skett i samband med personuppgiftsbehandling, har den möjlighet att förelägga den personuppgiftsansvarige- eller biträdet att vidta åtgärder så att behandlingen blir lagenlig.[196] I likhet med dataskyddsförordningen har registrerade enligt den brittiska lagstiftningen också rätt att få ersättning för eventuell skada på grund av felaktig behandling.[197]

Slutligen har registrerade också möjlighet att klaga hos brittiska domstolar under Human Rights Act, om man anser att myndigheterna på något sätt har inkräktat på ens privatlivs- och personuppgiftsskydd och således agerat i strid med grundläggande rättigheter enligt EKMR.[198] Om man sedan har uttömt alla rättsliga medel tillgängliga under nationell rätt, har man givetvis möjligheten att också klaga inför Europadomstolen.[199]

4.1.3 Offentliga myndigheters tillgång till personuppgifter

En av anledningarna till att Safe Harbor och Privacy Shield ogiltigförklarades handlade om det faktum att offentliga myndigheter med stöd av amerikansk lag hade åtkomst till personuppgifter på ett sätt som inte var begränsat till vad som var strikt nödvändigt. Det är därmed av intresse att undersöka hur brittisk

[194] Se EU-kommissionens utkast till beslut om adekvat skyddsnivå för Storbritannien, skäl 105.
[195] Ibid. skäl 106.
[196] Ibid. skäl 107.
[197] Ibid. skäl 108.
[198] Ibid. skäl 109.
[199] Ibid. skäl 111.

lagstiftning reglerar tillgång till personuppgifter och på vilka villkor det får ske. Kommissionen har undersökt regleringen utifrån två huvudsakliga områden: myndigheters tillgång till uppgifter för brottsbekämpande syften samt för syften sammankopplade med den nationella säkerheten.

Som tidigare nämnts reglerar Storbritannien personuppgiftsbehandling för brottsbekämpande myndigheter samt underrättelsetjänster i DPA 2018. Enligt DPA 2018 får personuppgiftsbehandling för sådana syften endast ske när det finns lagstöd för behandlingen och den registrerade antingen har gett sitt samtycke till behandlingen eller behandlingen är nödvändig för att en brottsbekämpande myndighet ska kunna utföra sina uppgifter.[200]

Brottsbekämpande myndigheter i Storbritannien kan samla in data från affärsverksamheter antingen genom en husrannsakningsorder eller en begäran om utlämnande av uppgifter. I båda fallen behövs tillstånd utfärdade av domstol. Omfattningen av en husrannsakningsorder styrs av vad domstolen har beslutat om, och ska utgå från vad som är relevant för syftet med utredningen. Vid en begäran av utlämnande av material ska den sökande myndigheten uppge varför utlämnandet är nödvändigt i förhållande till det allmänna intresset.[201] En begäran om personuppgiftsbehandling av en brottsbekämpande myndighet ska ske i enlighet med de krav som följer av DPA 2018, och måste därför följa av ett ändamål som är legitimt, tydligt och specificerat och inte går utöver vad som är nödvändigt.[202]

I syfte att förhindra eller upptäcka vissa allvarligare brott, har somliga myndigheter befogenhet att använda sig av så kallad riktad övervakning eller avlyssning enligt den brittiska *Investigatory Powers Act 2016*. Lagen tillhandahåller mekanismer som möjliggör avlyssning av innehållet i kommunikationsdata samt anskaffning och lagring av data som ger information om en viss kommunikation, så som vem, var och när någon har

[200] Se EU-kommissionens utkast till beslut om adekvat skyddsnivå för Storbritannien, skäl 132.
[201] Ibid. skäl 134.
[202] Ibid. skäl 135.

kommunicerat. För att få använda sig av dessa verktyg behöver den brottsbekämpande myndigheten ansöka om tillstånd. Ett sådant tillstånd kommer till stånd genom en ”double-lock procedure”, där ansökan först behöver godkännas av ansvarig minister och sedan även av en ”Judicial Commissioner”[203].[204] Båda instanserna har att pröva om åtgärden är nödvändig och proportionerlig i förhållande till syftet.[205]

Rätten att samla in data från behandlare av personuppgifter i syfte att skydda den nationella säkerheten är i Storbritannien förbehållen underrättelsetjänsterna. Den grupp som anses relevant för adekvansbeslutet utgörs av *the Security Service* (MI5), *the Secret Intelligence Service* (SIS) samt *the Government Communications Headquarters* (GCHQ).[206]

Likt de brottsbekämpande myndigheterna, har även myndigheter för nationell säkerhet och underrättelsetjänster möjlighet att bruka de mekanismer för datainsamling som tillhandahålls genom IPA 2016.[207] Även i detta sammanhang får verktygen användas först efter att ha bedömts och godkänts av ansvarig minister och en rättslig kommissionär. IPA 2016 har kompletterats med uppförandekoder som har utfärdats av inrikesministern samt godkänts av parlamentet. Uppförandekoderna anger under vilka förutsättningar som datainsamlingsverktygen får och bör användas.[208] En ansökan ska endast godkännas om den föreslagna åtgärden är proportionerlig i förhållande till vad den ämnar att uppnå. En avvägning måste således göras mellan integritetsingreppet och ändamålet. Bedömningen ska också se till varför den valda metoden är den som orsakar minsta möjliga ingrepp, varför

[203] ”Judicial Commissioners” är en funktion inom myndigheten IPC, en myndighet som har till uppgift att bevaka underrättelsetjänsternas verksamhet.
[204] Se EU-kommissionens utkast till beslut om adekvat skyddsnivå för Storbritannien, skäl 139.
[205] Ibid. skäl 139.
[206] Ibid. skäl 172.
[207] Ibid. skäl 174.
[208] Ibid. skäl 176.

andra metoder är otillräckliga och om den är i linje med hur lagen är tänkt att verkställas.[209]

IPA 2016 tillhandahåller också möjligheten att samla in uppgifter i bulk. Mekanismen är förbehållen underrättelsetjänsterna. Det finns ingen tydlig definition av vad bulkinsamling är i lagen, men regeringen har själv beskrivit det som en metod för att samla in och lagra större mängder av data. En oberoende granskare av lagen har också uttryckt att begreppet inte är att likställa med massövervakning, då verktyget är omgärdat av begränsningar och skyddsåtgärder som ska säkerställa att data inte kan samlas in på obefogade eller diskriminerande grunder.[210]

Att samla in data i bulk kan göras på flera olika sätt. Vid val av metod ska hänsyn tas till huruvida ändamålet kan uppnås med mindre inkräktande medel. Detta följer av att lagstiftningen bygger på proportionalitetsprincipen och innebär att riktad insamling ska prioriteras över bulkinsamling.[211]

I syfte att skydda den nationella säkerheten har underrättelsetjänsterna möjlighet att använda sig av bulkavlyssning. Sådan avlyssning är begränsad till att omfatta kommunikation som tas emot eller skickas av personer som befinner sig utanför de brittiska öarna.[212] För att få tillstånd att utföra en sådan åtgärd krävs att det finns en koppling mellan föremålen för avlyssning och syftet med åtgärden, som till exempel att skydda den nationella säkerheten eller att bekämpa eller upptäcka allvarliga brott.[213] Syftet med åtgärden ska också styra hur urvalet av data som ska undersökas sker.[214] Innan en ansökan godkänns, måste det göras en bedömning av om åtgärden står i proportion till

[209] Se EU-kommissionens utkast till beslut om adekvat skyddsnivå för Storbritannien, skäl 179.
[210] Ibid. skäl 211.
[211] Ibid. skäl 212.
[212] Ibid. skäl 214.
[213] Ibid. skäl 215.
[214] Ibid. skäl 217.

det eftersträvade syftet. Om en annan metod som inkräktar mindre på integritet och privatliv kan användas, ska ansökan inte godkännas.[215]

Om ett tillstånd att utföra bulkavlyssning utfärdas, finns det ett antal begränsningar att förhålla sig till. För det första är bemyndigandet endast giltigt i sex månader. Vid ändringar av ansökan eller förnyelse behöver ansökan prövas igen.[216] För det andra måste kopior av det material som samlats in hanteras och lagras på ett säkert sätt, och när materialet inte längre är relevant ska det förstöras. Antalet personer som omfattas av avlyssningen ska också begränsas till vad som är nödvändigt för att uppnå de i lagen angivna syftena.[217] Slutligen ska valet av vilken data som väljs ut för vidare undersökning också genomgå en proportionalitetsprövning. När data har samlats in sker först en automatisk filtrering med syftet att rensa ut de uppgifter som inte är av intresse för myndigheterna. Därefter väljs den data ut som är relevant för de syften som uppgetts och godkänts i ansökan.[218]

Kommissionen gör en bedömning av Storbritanniens reglering av myndigheters möjligheter att föra vidare insamlade uppgifter. Av särskilt intresse är den utredning som görs gällande Storbritanniens möjligheter och skyldigheter att lämna ut data till tredjeland och i synnerhet USA. Bedömningen görs mot bakgrund av den amerikanska lagen CLOUD Act som i sin tur möjliggör verkställande avtal med andra länder. Avtalet mellan USA och Storbritannien, som dock ännu inte trätt i kraft, kan få följden att data hos brittiska tjänsteleverantörer blir föremål för krav på utlämning till amerikanska brottsbekämpningsmyndigheter.[219]

Kommissionen framhåller de villkor som ställs för att sådan utlämning ska bli aktuell. Till exempel är det endast data kopplad till vissa allvarligare brottsutredningar som komma att bli föremål för utlämning, och varje beslut

[215] Se EU-kommissionens utkast till beslut om adekvat skyddsnivå för Storbritannien, skäl 218.
[216] Ibid. skäl 221.
[217] Ibid. skäl 222.
[218] Ibid. skäl 223.
[219] Ibid. skäl 151.

om utlämning av uppgifter ska vara föremål för granskning och tillsyn av en oberoende entitet så som en domstol, domare eller annan självständig myndighet.[220] Enligt kommissionen ska också data som lämnas ut under avtalet skyddas av skyddsåtgärder liknande sådana som tillhandahålls i ett motsvarande avtal mellan EU och USA i dagsläget. Detta har den brittiska regeringen bekräftat, samtidigt som den också uppger att diskussionerna kring detaljerna för skyddsåtgärderna fortfarande pågår. Kommissionen uttrycker att utvecklingen kring avtalet, dess innehåll och eventuella skyddsåtgärder är av hög relevans för adekvansbeslutet och därför bör övervakas noga framöver.[221]

Vad gäller tillsyn av offentliga myndigheters personuppgiftsbehandling, är ett antal olika organ inblandade, beroende av vilken lag som utgör grund för behandlingen. All behandling av data som sker på basis av DPA 2018 faller inom IC:s granskningsområde. Brottsbekämpande myndigheters och nationella säkerhetstjänsters utredningsbefogenheter som följer av IPA 2016 granskas av en *Investigatory Powers Commissioner* och tillhörande myndighet, *Investigatory Powers Commissioner's Office*. Verksamheten hos säkerhets- och underrättelsetjänster är också föremål för tillsyn av en kommitté för underrättelse- och säkerhetsfrågor[222] under parlamentet.

Det finns flera tillgängliga rättsmedel för en registrerad som vill klaga på databehandling som utförts av brottsbekämpande myndigheter eller nationella säkerhets- eller underrättelsetjänster. För mål som rör behandling utförd mot bakgrund av IPA 2016 har Storbritannien inrättat en särskild domstol, *Investigatory Powers Tribunal*. Domstolen har i praxis erkänts av Europadomstolen.[223]

[220] Se EU-kommissionens utkast till beslut om adekvat skyddsnivå för Storbritannien, skäl 152.
[221] Ibid. skäl 153.
[222] The Intelligence and Security Committe (ISC).
[223] Se *Big Brother Watch and others v. United Kingdom*, no. 58170/13, 62322/14, 24960/15, ECHR 2006-XI.

4.2 EDPB:s yttrande

Den 13 april 2021 publicerade EPBD ett yttrande över kommissions förslag till beslut om adekvat skyddsnivå för Storbritannien.[224] Till grund för yttrandet låg dels förslaget i sig, dels den dokumentation och det material som tillhandahållits av kommissionen.[225]

EDPB anför att man funnit att den brittiska lagstiftningen i hög utsträckning överensstämmer med kärnan i EU:s dataskyddslagstiftning, framför allt mot bakgrund av att den brittiska lagstiftningen bygger på den EU-rättsliga.[226] Samtidigt lyfter dataskyddsstyrelsen också fram ett antal utmaningar som man uppmanar kommissionen att undersöka närmre, innan ett beslut kan fattas.

Inledningsvis lyfter EDPB vikten av att noggrant övervaka utvecklingen på dataskyddsområdet, med hänsyn till de indikationer från den brittiska regeringen om att utveckla lagstiftningen i detta avseende.[227] Eftersom ändringar kan komma att påverka skyddsnivån i Storbritannien, uppmanar EDPB kommissionen att bevaka alla eventuella och relevanta förändringar och, i den mån det kan påverka bedömningen av huruvida Storbritanniens skyddsnivå är att anse som adekvat, ändra eller upphäva beslutet.[228]

Vidare kritiserar EDPB Storbritanniens reglering om undantag av vissa rättigheter vid så kallade invandringskontroller, närmare bestämt rätten till tillgång, rätten till radering, och rätten att begränsa eller neka behandling. EDPB pekar på att begränsningen är brett formulerad och inte specificerar vilka skyddsåtgärder som tillämpas för att förhindra missbruk, vilka personuppgiftsansvariga som får använda undantaget, vilka risker som finns

[224] Se EDPB, *Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom*.
[225] Ibid. p. 2.
[226] Ibid. p. 6 & 7.
[227] Ibid. p. 11
[228] Ibid. p. 55.

för grundläggande fri- och rättigheter eller den registrerades rättighet att få information om undantaget. Mot denna bakgrund uppmanar EDPB kommissionen att undersöka begränsningen närmre.[229]

Ett annat område som EDPB lyfter som problematiskt, är Storbritanniens reglering av vidare överföring av data. Detta område berör dels Storbritanniens bestämmelser om tredjelandsöverföringar motsvarande dataskyddsförordningens bestämmelser, dels andra internationella avtal och åtaganden som påverkar vidare överföring från Storbritannien. Vad gäller det förstnämnda, relaterar EDPB:s oro till den ovan beskrivna problematiken med en utveckling där Storbritannien avviker från den EU-rättsliga regleringen.[230] Vad gäller Storbritanniens internationella åtaganden, lägger EDPB sitt fokus på avtalet mellan USA och Storbritannien framtaget under CLOUD Act.[231] Dataskyddsstyrelsen menar att data som behandlas hos personuppgiftsansvariga och -biträden i Storbritannien genom avtalet kan bli direkt tillgängligt för amerikanska myndigheter, vilket i så fall kan påverka bedömningen av skyddsnivån i Storbritannien. EDPB pekar också på det faktum att kommissionen i sitt förslag inte tillhandahåller några uttryckliga garantier från den brittiska regeringen eller myndigheter gällande data som kan bli föremål för utlämning under avtalet.[232] Dataskyddsstyrelsen har redan tidigare lyft denna problematik inför EU-parlamentet. Den yttrade då att ett sådant avtal bör omfattas av skyddsåtgärder som inkluderar någon form av föregående rättslig prövning innan data lämnas ut, för att regleringen skulle kunna anses som väsentligen likvärdig med det skydd som erhålls inom EU.[233] EDPB lyfter vidare att kommissionen inte har bedömt Storbritanniens avtal med tredje länder vad gäller delande av information mellan underrättelsetjänster. Som exempel lyfter EDPB ytterligare ett avtal mellan

[229] Se EDPB, *Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom*, p. 61, 69 & 73.
[230] Ibid. p. 80-81.
[231] Se avsnitt 4.1.3.
[232] Se EDPB, *Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom*, p. 88.
[233] Ibid. p. 89-90.

Storbritannien och USA, ”*the UK-US Communication Intelligence Agreement*”, som innefattar ett samarbete mellan USA:s nationella säkerhetsbyrå NSA och den brittiska motsvarigheten GCHQ. Enligt EDPB utgör avtalets hemlighetsfulla karaktär ett problem när det kommer till tydlighet och förutsebarhet för brittiska underrättelsetjänsters och nationella säkerhetsbyråers vidare överföring och delning till tredjeland av insamlad data.[234]

EDPB lyfter också viss kritik och riktar uppmärksamhet mot bedömningen av brittiska offentliga myndigheters tillgång till personuppgifter. Dataskyddsstyrelsen pekar på ett flertal osäkra faktorer. Till exempel kritiserar den kommissionens uttalande om att utredningsbefogenheterna under IPA 2016 är desamma för brottsbekämpande myndigheter och nationella säkerhetstjänster och att tillämpliga villkor, skyddsåtgärder och begränsningar därför kan behandlas samtidigt, oavsett vilket syfte som står bakom åtgärden. EDPB menar med hänvisning till EU-domstolens praxis att en sådan bedömning kan bli oriktig, då olika syften kan rättfärdiga olika typer av åtgärder.[235]

EDPB anför också generella anmärkningar mot bedömningen av villkoren för användning av befogenheterna givna under IPA 2016. Kritiken behandlar det faktum att befogenheternas tillåtlighet är kopplad till brett angivna syften, och inte anger en koppling mellan de kategorier av människor som kan bli föremål för datainsamling och de syften som anges i lagstiftningen.[236] Dataskyddsstyrelsen lyfter också det faktum att de kriterier som ska beaktas i bedömningen av en åtgärds nödvändighet och proportionalitet inte återfinns i lagstiftningen, utan kan hittas i andra vägledande dokument.[237]

[234] Se EDPB, *Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom*, p. 191-193.
[235] Ibid. p. 127.
[236] Ibid. p. 151.
[237] Ibid. p. 153.

Vad gäller bulkinsamling uttrycker EDPB en oro över att det är svårt att bedöma omfattningen av de operativa syften som en bulkinsamling ska baseras på, och om de är tillräckligt avgränsade för att leva upp till de krav som satts upp av EU-domstolen. Även villkoren för lagringstiden av insamlad data kritiseras, då villkoret att data eller kopior av data får lagras så länge det anses nödvändigt anses vara för vagt och brett formulerat.[238]

Sammanfattningsvis anser dataskyddsstyrelsen att det brittiska regelverket i hög utsträckning överensstämmer med det EU-rättsliga, och att bedömningen är unik i det avseendet att Storbritannien tidigare har varit en av EU:s medlemsstater. Samtidigt återfinns ett flertal utmaningar som EDPB uppmanar kommissionen att både undersöka närmre och noggrant bevaka framöver i syfte att möta kravet på en adekvat skyddsnivå.[239]

[238] Se EDPB, *Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom*, p. 170-171.
[239] Ibid. p. 35-37.

5 Bedömning av tredjelands skyddsnivå

Av dataskyddsförordningens skäl och uttalanden från kommissionen framgår att dataöverföringar numera är av största vikt för den internationella handeln. Överföringarna vållar dock en intressekonflikt mellan viljan av att underlätta handeln och viljan att upprätthålla det skydd som EU-rätten tillhandahåller.

5.1 En väsentligen likvärdig skyddsnivå

I bedömningen av huruvida ett tredjeland tillhandahåller en väsentligen likvärdig skyddsnivå ska ett flertal faktorer beaktas. EU-domstolen uttalade explicit i Schrems I att ett konstaterande om adekvat skyddsnivå inte innebär att ett tredjeland måste tillhandahålla en reglering som är identisk med den EU-rättsliga regleringen. Konstaterandet lade grunden till en introduktion av begreppet *väsentligen likvärdig skyddsnivå*. Av praxis och rekommendationer framgår att den slutgiltiga frågan handlar om huruvida dataöverföring till ett tredjeland riskerar att kränka det väsentliga innehållet i EU-medborgares grundläggande rättigheter. I praktiken verkar det innebära att åtgärder som begränsar rättigheter bör tillåtas om de kan anses proportionerliga i förhållande till ett erkänt syfte.

Trots konstaterandet från EDPB om att adekvansbeslut kan fattas för länder med rättssystem som härstammar ur andra rättsliga traditioner än EU:s, framkommer krav på tredjelandets regelverk som utgör villkor för att ett beslut ska kunna fattas och anses giltigt. Inledningsvis har art. 29-gruppen uttryckt att det bör finnas grundläggande dataskyddskoncept som i någon mån motsvarar EU:s. Som exempel lyfts fram befintlighet och definition av begrepp så som ’personuppgifter’, ’behandling’ och ’känsliga personuppgifter’. Det framhävs också som önskvärt att tredjelandets

lagstiftning anger att behandling ska ske i enlighet med vissa principer, som till exempel proportionalitets-, ändamåls- och legitimitetsprincipen. Vidare bör registrerade också tillskrivas någon form av rättigheter i samband med personuppgiftsbehandling. Det är dock otydligt i vilken mån avsteg får göras från de koncept som EU:s regler innehåller, och i vilken omfattning landets dataskyddslagstiftning ska överensstämma med EU:s för att anses uppfylla kravet på en väsentligen likvärdig skyddsnivå i detta avseende. I EDPB:s yttrande till förslagsutkastet om adekvat skyddsnivå för Storbritannien lyfts kritik mot de undantag från lagstiftningen som får göras i samband med behandling av personuppgifter vid invandringskontroller. Kritiken baseras på att bruk av undantaget medför en inskränkning av registrerades rättigheter och att det förefaller oklart under vilka villkor som undantaget får användas. Huruvida begränsningen skulle kunna ses som ett godtagbart avsteg från den av EU tillhandahållna skyddsnivån av EU-domstolen, är osäkert.

Vidare framgår också av dataskyddsförordningen, riktlinjer och praxis att tredjelandets regelverk ska tillhandahålla någon form av oberoende tillsynsmekanism. Hänsyn ska också tas till vilka resurser och befogenheter en sådan mekanism har. Exakt vilka resurser och befogenheter som krävs för att skyddsnivån ska anses adekvat i detta avseende, är inte klarlagt. Som exempel på något som inte uppfyllde kriterierna kan lyftas EU-domstolens kritik mot det självcertifieringssystem som Safe Harbor byggde på. Enligt domstolen utgjorde systemet som sådant inte ett problem, däremot uttrycktes att funktionen av sådant system är beroende av fungerande tillsynsmekanismer, vilket inte kunde visas existera. Vad gäller tillsynsmekanismens oberoende, var denna aspekt föremål för bedömning av EU-domstolen i Schrems II. Domstolen argumenterade för att ombudsmannamekanismen som införlivades i och med Privacy Shield-beslutet inte kunde anses vara oberoende, med hänvisning till det faktum att positionen tillsattes av det amerikanska utrikesdepartementet och att det inte fanns några garantier för att ombudsmannens tillsättning eller befogenheter inte kunde återkallas. Det kan argumenteras för att utrymmet för en skönsmässig bedömning av just tillsynsmekanismer torde vara relativt

begränsad, med hänsyn till att det EU-rättsliga skyddet av personuppgifter uttryckligen omfattar ett krav på att en oberoende tillsynsmyndighet ska tillse efterlevnad av personuppgiftshantering.

Området som lämnar störst utrymme för diskussion är dock det som rör offentliga myndigheters tillgång till personuppgifter. Vad som kan fastställas är att både brottsbekämpning och nationell säkerhet är erkända syften som motiverar begränsande åtgärder. I både Schrems I och II utgjorde de amerikanska övervakningssystemen en central anledning till ogiltigförklaringarna av Safe Harbor och Privacy Shield. EU-domstolen framhävde att det inte framkom några uppgifter om att behörigheten att genomföra övervakningsprogramgrundade på FISA avsnitt 702 var omgärdad av någon form av begränsningar. Domstolen kritiserade även möjligheten att bulkinsamla uppgifter enligt PPD-28, och pekade på att underrättelsetjänsterna inte behövde rikta insamlingen genom användningen av identifieringsfaktorer kopplade till ett specifikt uttryckt mål. Av kritiken kan slutsatsen dras att insamling som kan anses vara godtycklig och inte är kopplad till ett erkänt syfte, är inte en godtagbar begränsning och således inte uppfyller kraven för en väsentligen likvärdig skyddsnivå. Av domen framgår också att om en åtgärd kränker det väsentliga innehållet i antingen art. 7 eller 8 är den i sig inte godtagbar i förhållande till den EU-rättsliga skyddsnivån, och det finns då inget behov av att utföra en proportionalitetsprövning. Vad som krävs för att en åtgärd ska anses kränka det väsentliga innehållet i en grundläggande rättighet, är dock inte helt klarlagt.

Av kommissionens förslag till beslut om adekvat skyddsnivå för Storbritannien, kan uttolkas en vilja att tydliggöra att den datainsamling som sker av brittiska underrättelsetjänster inte är att likställa med massövervakning. Tvärtom framhävs att den verksamhet som bedrivs av underrättelsetjänsterna och klassificeras som bulkinsamling är omgärdad av begränsningar. Av förslaget framgår att det existerar begränsningar och skyddsåtgärder att förhålla sig till vid sådan verksamhet. Frågan är huruvida mekanismen är reglerad i den omfattning att den motsvarar de krav som

återges i riktlinjer och praxis. Som EDPB framhåller i sitt yttrande, kan de angivna syftena med åtgärden i praktiken medföra att underrättelsetjänsterna får tillstånd att samla in data från ett litet geografiskt område likväl som från hela EU. Det ska också tilläggas att även om ett tillstånd att genomföra en bulkinsamling är begränsat i tid, så har underrättelseverksamheterna i praktiken möjlighet att spara data så länge som det anses nödvändigt. De så kallade begränsningarna är således i viss mån brett hållna, och det är oklart om åtgärderna och mekanismerna kan anses vara begränsade till vad som är strikt nödvändigt. Av EU-domstolens praxis framgår nämligen klart och tydligt att en inskränkning i skyddet för personuppgifter måste ange exakt vilka omständigheter och villkor som möjliggör en sådan inskränkning. Således verkar det av domstolens resonemang i Schrems II som att det är irrelevant om insamling som inte är riktad kallas för massövervakning eller bulkinsamling, det avgörande för domstolens bedömning är vilken utsträckning som insamlingen omfattas av tydliga begränsningar och skyddsåtgärder. Vad gäller fallet Storbritannien, har det ansetts vara ett unikt fall då Storbritannien tidigare har varit en av EU:s medlemsstater och har en dataskyddslagstiftning som i mångt och mycket har formats av EU-rätten. Vid studerandet av Safe Harbor och framför allt Privacy Shield, framkommer att besluten hade en tydlig utgångspunkt i EU:s lagstiftning om skydd för personuppgifter och i stor utsträckning speglade de essentiella koncepten och principerna däri. Det faktumet saknade dock betydelse eftersom de amerikanska övervakningsprogrammen inte ansågs tillräckligt begränsade för att säkerställa en adekvat skyddsnivå. Mot den bakgrunden kan Storbritanniens unika status som en före detta medlemsstat och utförliga personuppgiftsskydd komma att spela en mindre roll, om tillgängliga övervakningsåtgärder inte anses tillräckligt begränsade och proportionerliga.

Förhållandet mellan bedömningen av tredjeländers åtgärder som inskränker på integritetsskyddet och syftar till att skydda nationell säkerhet och motsvarande åtgärder inom medlemsstaterna, utgör ett komplicerat område då alla frågor som rör nationell säkerhet faller inom medlemsstaternas kompetensområde och inte EU:s. Det föreligger en generell osäkerhet kring

hur personuppgiftsbehandling av kommersiella aktörer som kan bli föremål för behandling av nationella säkerhetsbyråer eller underrättelsetjänster ska hanteras i ljuset av dataskyddsförordningen. Av EU-domstolens resonemang i Schrems II följer att all insamling av personlig data utgör ett intrång i rätten till privatliv och skyddet för personuppgifter enligt EU-stadgan. Om åtgärden dessutom samlar in innehåll i kommunikationsdata och inte omfattas av lämpliga skyddsåtgärder, riskerar åtgärden att kränka det väsentliga innehållet i art. 7 och 8 EU-stadgan. Det följer således av domstolens uttalanden i Schrems II att om medlemsstaternas underrättelsetjänster använder sig av sådana mekanismer, utgör de en kränkning av EU-medborgares fri- och rättigheter. Schrems-målen kan därför komma att leda till en utveckling där medlemsstaternas underrättelseverksamheter i större utsträckning blir föremål för en granskning av EU-domstolen, gällande huruvida dessa verksamheter är i linje med de grundläggande fri- och rättigheterna i EU-stadgan.[240] Domstolens uttalade i Schrems II att personuppgifter som överförs till tredjeland och kan bli föremål för behandling för ändamål som rör försvar eller nationell säkerhet ska omfattas av förordningens tillämpningsområde. Av detta uttalande kan slutsatsen dras att bedömningen av tredjelands skyddsnivå i detta avseende ställer högre krav på tredjelands skyddsnivå jämfört med skyddsnivån som säkerställs inom EU.

Domstolen har genom tillämpning av proportionalitetsprincipen lämnat ett mycket smalt utrymme för åtgärder som inskränker privatlivs- och personuppgiftsskyddet i art. 7 och 8 EU-stadgan. Även om rättigheterna inte är absoluta och inskränkande åtgärder är tillåtna under vissa förutsättningar, kan domstolens resonemang och slutsatser tolkas så att intresset att upprätthålla skyddet för personuppgifter och rätten till privatliv prioriteras över staters rätt att vidta vissa åtgärder i syfte att skydda den nationella säkerheten. Vad gäller Storbritannien kan regleringen av exempelvis

[240] Den 25 maj 2021, dagen innan denna uppsats slutligen lämnas in, meddelar Europadomstolen att Sverige fälls för brister i FRA-lagen. Bristerna handlar i korthet om att det saknas tillräckligt skydd för organisationers korrespondens, inte framkommer krav på vidare överföring eller finns tillräcklig efterhandsgranskning om hur enskilda fått sina uppgifter avlyssnade. Domstolen hänvisar bland annat till Schrems II-domen.

bulkinsamling vara avgörande för giltigheten av ett eventuellt framtida beslut om adekvat skyddsnivå, med hänsyn till EU-domstolens relativt starka ställningstagande i frågan.

En annan intressant faktor i bedömningen av tredjelands skyddsnivå är den del som rör vidare överföring till andra tredjeländer eller organisationer. Likt ovan saknas en gemensam referenspunkt inom EU och hur medlemsstaternas internationella avtal och samarbeten ska hanteras i ljuset av dataskyddsförordningen. När det kommer till samarbete mellan underrättelsetjänster präglas den verksamheten till sin natur dessutom av sekretess. Samarbetet mellan olika länders underrättelsetjänster togs aldrig upp för bedömning i varken Schrems I eller II, men med hänsyn till att det lyftes som ett orosmoment av EDPB angående Storbritanniens skyddsnivå är det mycket möjligt att denna faktor så småningom kommer att bli föremål för bedömning av EU-domstolen. Det ter sig rimligt att avtal som till exempel det mellan brittiska GCHQ och amerikanska NSA undersöks närmre, då vidare överföring från Storbritannien till USA riskerar att undergräva integritetsskyddet med hänsyn till utfallet i Schrems II. Mot den bakgrunden kan det också, liksom när det kommer till medlemsstaternas underrättelseverksamheter generellt, finnas incitament för att medlemsstaternas internationella avtal och samarbeten bör undersökas och utredas närmre i förhållande till skyddet för personuppgifter och rätten till privatliv.

Sammanfattningsvis kan sägas att det inte är helt klarlagt exakt vad som skiljer en väsentligen likvärdig skyddsnivå från en identisk sådan. Vad gäller bedömning av åtgärder som vidtas i syfte för nationell säkerhet, uppstår en problematik redan vid fastställandet av vad som gäller rent EU-rättsligt eftersom området inte är harmoniserat.

5.2 Utmaningar vid bedömningen av adekvat skyddsnivå

Bedömningen och giltigheten av adekvansbeslut aktualiserar för det första frågan om EU-domstolens möjligheter att bedöma tredjeländers lagstiftning. Problemen framhävs till exempel av det amerikanska handelsdepartementets vitbok efter Schrems II, som lyfter det faktum att den amerikanska lagstiftningen tillhandahåller både skyddsåtgärder och rättsmedel som EU-domstolen överhuvudtaget inte adresserar i domen. Det följer av sakens natur, det vill säga bedömningen av tredjelands skyddsnivå, att utredning av tredjelands lagstiftning är nödvändig. En sådan utredning bör dock baseras på att domstolen har fått fullgod information om all relevant lagstiftning. Om domstolen grundar sina beslut på endast en del av alla relevanta fakta, kan det på lång sikt leda till ifrågasättanden av domstolens legitimitet.

Som diskuterats ovan, är bedömningen av ett lands skydd för personuppgifter mer eller mindre komplicerad beroende av vilket område av tredjelands lagstiftning som behandlas. Vad gäller dataskyddskoncept, krav på tillsynsmekanismer och rätten till prövning och effektiva rättsmedel är bedömningen tydligare och framstår som enklare då det finns tydliga referenspunkter att utgå från i EU-stadgan och dataskyddsförordningen. Problematiken blir mer påtaglig när det kommer till att avgöra om tredjelands lagstiftning utgör en väsentligen likvärdig skyddsnivå när motsvarande skyddsnivå inom EU inte är harmoniserad, utan skiljer sig mellan medlemsstaterna. Utifrån kan det dessutom uppfattas som att EU-domstolen använder sig av olika måttstockar till medlemsstaternas favör.

EU-kommissionen har uttryckt att målet är att den europeiska modellen för skydd av personuppgifter ska vara normgivande även på en global nivå. Till viss del har denna önskan uppfyllts då ett flertal länder följer i unionens fotspår vad gäller uppbyggnad av regelverk om skydd av personuppgifter. Det finns dock en risk att domstolens ställningstagande i avvägningen mellan

integritetsskydd och nationella säkerhetsfrågor kan komma att utgöra ett hinder för tredjeländers intresse och möjlighet att både följa efter och samarbeta med unionen angående dataskyddsfrågor. EU-domstolens praxis belyser intressekonflikten mellan ett högt och omfattande skydd av personuppgifter och utrymmet att bedriva verksamheter och åtgärder som syftar till att upprätthålla och skydda nationell säkerhet. Huruvida det är möjligt att skapa förutsättningar för internationella dataflöden som upprätthåller integritetsskyddet, samtidigt som offentliga myndigheter bibehåller utrymme att bedriva verksamhet gällande nationell säkerhet i nödvändig omfattning, återstår att se.

6 Avslutande kommentarer

Att bedöma huruvida tredjeland tillhandahåller en adekvat skyddsnivå är en komplex och omfattande utredning. Beslutet ska baseras på en helhetsbedömning av alla relevanta omständigheter som inverkar på integritets- och personuppgiftsskyddet. Underlaget behöver inte spegla en skyddsnivå som är identisk med den europeiska dataskyddslagstiftningen, utan om det kan visas att tredjelandet tillhandahåller en väsentligen likvärdig skyddsnivå ska beslutet anses godtagbart. Den bortre gränsen förefaller utgöras av huruvida tredjelands lagstiftning och reglering kränker det väsentliga innehållet i de grundläggande rättigheterna i EU-stadgan. Vad som krävs för att en sådan kränkning ska anses föreligga, är inte helt tydliggjort. Detta utgör en av utmaningarna i bedömningen av huruvida tredjelands skyddsnivå ska anses adekvat under art. 45.1 GDPR.

En annan utmaning vars diskussion förts upp i ljuset av Schrems-målen är EU-domstolens förmåga att behandla utländsk rätt. Trots att detta görs i ljuset av EU-rätten, är det inte omöjligt att tänka sig att domstolen kommer få motta kritik om inblandade parter menar att domstolen inte har haft alla relevanta fakta till hands i sin bedömning.

Det står tydligt att diskussionen gällande konflikten mellan intresset av att möjliggöra internationella dataflöden och samtidigt upprätthålla ett omfattande skydd för personuppgifter, inte är avslutad än. Om det inom en snar framtid fattas ett beslut om adekvat skyddsnivå för Storbritannien, vilket ett flertal faktorer pekar på, är det mycket möjligt att EU-domstolen får tillfälle att utveckla sina resonemang gällande vad som ska anses falla inom ramarna för en väsentligen likvärdig skyddsnivå. En sådan tvist kan också ge upphov till en vidare diskussion av skyddsnivån inom EU, vad gäller exempelvis skyddet för personuppgifter i förhållande till medlemsstaternas verksamheter som inte styrs av EU-rätten.

Eftersom utvecklingen på området pågår i skrivande stund, blir framtidsprognoser om densamma lätt spekulativa. Av den anledningen ska det bli mycket spännande att se vilken väg rättsutvecklingen tar, och om det finns möjligheter att överbrygga intressekonflikterna eller om dessa riskerar att fördjupas ytterligare under en tid framöver.

Käll- och litteraturförteckning

Källor

Offentligt tryck

Art. 29-gruppen och Europeiska dataskyddsstyrelsen

Art. 29-gruppen, *WP 169: Yttrande 01/2010 om begreppen registeransvarig och registerförare*. Antaget den 16 februari 2010.

Art. 29-gruppen, *WP 254 rev.01: Adequacy Referential*. Antaget den 6 februari 2018.

Se EDPB, *Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom*. Antagen den 13 april 2021.

EDPB, *Rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder*. Antagna den 10 november 2020.

EU-kommissionen

Kommissionens beslut av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbor Privacy Principles) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat (2000/520/EG).

Meddelande från kommissionen till Europaparlamentet och rådet, ”Återskapande av förtroendet för dataflödet mellan EU och Förenta staterna”, KOM(2013) 846 slutlig.

Meddelande från kommissionen till Europaparlamentet och rådet, "om hur principerna om integritetsskydd (Safe Harbor) fungerar när det gäller EU:s medborgare och företag som är etablerade i EU", KOM(2013) 847 slutlig.

Meddelande från kommissionen till Europaparlamentet och rådet, "Om överföring av personuppgifter från EU till Amerikas förenta stater enligt direktiv 95/46/EG med anledning av domstolens dom i mål C-362/14 (Schrems)", COM(2015) 566 slutlig.

Kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydds säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna.

Meddelande från kommissionen till Europaparlamentet och rådet, "Utbyte och skydd av personuppgifter i en globaliserad värld", COM(2017) 7 slutlig.

Politisk förklaring om de framtida förbindelserna mellan Europeiska unionen och Förenade Kungariket, EUT 2019 C 384 I/02.

Storbritanniens regering

Department for Exiting the European Union, *'Legislating for the United Kingdom's Withdrawal from the European Union'*. Publicerad mars 2017.

USA:s regering

Amerikanska handelsdepartementet, '*White Paper – Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II'*. Publicerad september 2020.

Elektroniska källor

Cadwalladr, Carole & Graham-Harrison, Emma, ‘Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach’, <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>, publicerad i The Guardian 17 mars 2018 (besökt 23 mars 2021).

EU-kommissionen, ’Adequacy decisions’ <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_sv> (besökt 24 februari 2021).

EU-kommissionen, ’Brexit’ <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/brexit_sv> (besökt 28 februari 2021).

EU-kommissionen, ’Det nya normala’ <https://ec.europa.eu/info/relations-united-kingdom/new-normal_sv> (besökt 12 maj 2021).

EU-kommissionen, ‘Data protection: European Commission launches process on personal data flows to UK’ <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661> (besökt 13 mars 2021).

EU-kommissionen, ’Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers’ <https://ec.europa.eu/commission/presscorner/detail/sv/MEMO_17_15> (besökt 8 mars 2021).

EU-kommissionen, utkast till beslut om adekvat skyddsnivå för Storbritannien, ”Commission Implementing Decision of XXX pursuant Regulation (EU) 2016/679 of the European Parliament and of the Council

on the adequate protection of personal data by the United Kingdom”, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/brexit_sv. Publicerad 19 februari 2021.

EU-kommissionen, ’Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross’ <https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_sv> (besökt 24 mars 2021).

EU-kommissionen, ’Joint statement ahead of the 2nd year anniversary of the General Data Protection Regulation’ <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_20_913> (besökt 17 maj 2021).

Utrikespolitiska institutet, ’Storbritannien – Demokrati och rättigheter’ https://www.ui.se/landguiden/lander-och-omraden/europa/storbritannien/demokrati-och-rattigheter/ (besökt 19 april 2021).

Litteratur

Bergström, Carl Fredrik & Hettne, Jörgen (2014), *Introduktion till EU-rätten*. 1 uppl., Studentlitteratur AB.

Bygrave, Lee A. (2013), *‘Transatlantic Tensions on Data Privacy’*. Transworld Papers nr. 19, ISSN 2281-5252.

Colonna, Liane (2016), *’Schrems vs. Commissioner: A precedent for the CJEU to intervene in the national intelligence surveillance activities of Member States?’*. Europarättslig tidskrift nr. 2 s. 208-224.

Frydlinger, David, Edvardsson, Tobias, Olstedt Carlström, Caroline & Beyer, Sandra (2018), *GDPR – Juridik, organisation och säkerhet enligt dataskyddsförordningen*. 1 uppl., Norstedts Juridik AB.

Hettne, Jörgen & Otken Eriksson, Ida (2011), *EU-rättslig metod – Teori och genomslag i svensk rättstillämpning*. 2:a uppl., Norstedts Juridik AB.

Kleineman, Jan (2018), ’Rättsdogmatisk metod’ i: Nääv, Maria & Zamboni, Mauro (red.), *Juridisk metodlära*. 2:a uppl., Studentlitteratur AB s. 21-46.

Lebeck, Carl (2016), *’EU-stadgan om grundläggande rättigheter’*. 2:a uppl., Studentlitteratur AB.

Murray, Andrew D. (2017), *’Data transfers between the EU and UK post Brexit?’*. International Data Privacy Law vol. 7 nr. 3 s. 149-164.

Olsen, Lena (2004), *’Rättsvetenskapliga perspektiv’*. SvJT s. 105-145.

Patel, Oliver & Lea, Nathan (2019), *’EU-UK Data Flows, Brexit and No-Deal: Adequacy or Disarray?’*. Brexit Insights Series, UCL European Institute.

Reichel, Jane (2018), ’EU-rättslig metod’ i: Nääv, Maria & Zamboni, Mauro (red.), *Juridisk metodlära*. 2:a uppl., Studentlitteratur AB s. 109-142.

Schwartz, Paul M. & Solove, Daniel J. (2014), *‘Reconciling Personal Information in the United States and European Union’*. California Law Review vol. 102 nr. 4 s. 877-916.

Svensson, Eva-Maria (2014), *’De lege interpretata – om behovet av metodologisk reflektion’*. Juridisk Publikation s. 211-226.

Törngren, David, förordning (EU) 2016/679, Lexino lagkommentar (JUNO) 2019-04-30.

Öman, Sören, Dataskyddsförordningen (GDPR) m.m., Norstedts Juridiks lagkommentarer (JUNO) 2020-02-29.

Rättsfallsförteckning

EU-domstolen

C-26/62 *Van Gend en Loos*, EU:C:1963:1.

C-101/08 *Audiolux*, EU:C:2009:626.

C-293/12 och C-594/12 *Digital Rights Ireland Ltd mot Minister for Communications, Marine and Natural Resources m.fl.*, EU:C:2014:238.

C-362/14 *Maximillian Schrems mot Data Protection Commissioner*, EU:C:2015:650.

C-582/14 *Patrick Breyer mot Bundesrepublik Deutschland*, EU:C:2016:779.

C-203/15 och C-698/15 *Tele2 Sverige AB och Secretary of State for the Home Department mot Post- och telestyrelsen m.fl.*, EU:C:2016:970.

C-25/17 *Jehovas vittnen*, EU:C:2018:551.

C-311/18 *Data Protection Commissioner mot Facebook Irland Ltd och Maximillian Schrems*, EU:C:2020:559.

C-511/18, C-512/18 och C-520/18 *La Quadrature du Net mot Premier ministre m.fl.*, EU:C:2020:791.

Europadomstolen

Weber och Saravia v. Tyskland, no. 54934/00, ECHR 2006-XI.