GDPR & BREXIT

HUR PÅVERKAS AKTÖRERS PERSONUPPGIFTSÖVERFÖRING FRÅN EU NÄR STORBRITANNIEN GÅR FRÅN EU-MEDLEMSSTAT TILL TREDJELAND?

Av: Karin Matsson

Handledare: Andreas Moberg

HANDELSHÖGSKOLAN VID GÖTEBORGS UNIVERSITET

Juridiska institutionen

Kurs HRO800 Examensarbetet 30 hp

Juristprogrammet

HT 2018

Innehållsförteckning

Förkortningar

DPA – Data Protection Act 2018
EES – Europeiska ekonomiska samarbetsområdet
EES-avtalet – Agreement on the European Economic Area (OJ No L 1, 3.1.1994 p. 3; and EFTA States' official gazettes)
EKMR – Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Rom, 4.XI.1950)
EU – Europeiska unionen
EUD – EU-domstolen
FEU – Fördraget om Europeiska unionen (EUT C 202, 7.6.2016, s. 1–388)
FEUF – Fördraget om Europeiska unionens funktionssätt (EUT C 202, 7.6.2016, s. 1–388)
GB – Governing Body
GDPR – 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 hävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1–88)
ICO – Information Commissioner's Office
JC – Joint Committee
OSS – One Stop Shop-mekanismen
PS – Privacy Shield-ramverket
WP29 – Article 29 Data Protection Working Party

1 Problematiken – där GDPR och brexit möts

Den 25 maj 2018 trädde den allmänna dataskyddsförordningen[1] (GDPR) ikraft. I egenskap av att fortfarande vara färsk är regleringens konsekvenser ännu inte klarlagda. Samtidigt lämnar Storbritannien EU den 29 mars 2019. Storbritannien blir således ett tredjeland i förhållande till unionen. Relationen mellan EU:s medlemsstater och Storbritannien blir emellertid inte som den till ett tredjeland, vilket som helst. Istället rör det sig här om ett land med vilket övriga medlemsstater är nära sammansvetsade, ett land vars företag ständigt samverkar med andra medlemsstaters företag och ett land vilket i nuläget omfattats av EU-reglering – inte minst GDPR.

I dagsläget[2] regleras personuppgiftsflöden i Storbritannien och övriga medlemsstater enligt vad som stadgas i GDPR på området inom unionen. Vad som kommer att ske med regleringen av flödet av personuppgifter från EU till Storbritannien efter brexit är dock ännu inte klarlagt. Utifrån de olika alternativ som finns för personuppgiftsöverföring till tredjeland – vilken skillnad innebär det i förhållande till idag? Hur kommer detta att påverka företag i unionen och i Storbritannien, vilka idag kan låta personuppgifter flöda fritt mellan varandra enligt GDPR? Jag vill behandla frågor som dessa i min uppsats, för att få en bild av hur GDPR och brexit kommer att påverka personuppgifternas framtida flöde för företag som vill verka över unionens yttre gräns.

1.1 Syfte – alternativ och skillnader sprungna ur kombinationen GDPR och brexit

Eftersom det varken är självklart eller klart hur flödet av personuppgifter mellan unionen och Storbritannien, efter det senares utträde, kommer att regleras så vill jag studera vilka alternativ som finns. Genom att analysera alternativen och dess konsekvenser för aktörer som vill skicka personuppgifter till Storbritannien vill jag sedermera undersöka om, och i så fall hur, dessa kommer att innebära någon skillnad för aktörerna. Med skillnad avses alternativet efter brexit ställt i förhållande till hur flödet för personuppgifter fungerar *inom unionen*. En generell uppfattning, från såväl EU som andra, verkar vara att ett beslut från kommissionen om att ett land har adekvat skyddsnivå för personuppgifter är det som är att föredra för personuppgiftsflöden till tredjeländer.[3] En anledning till varför adekvansbeslutet lyfts fram som en lösning framför andra är att det anses generera flödesförhållanden för personuppgifter i stort sett som de i EU.[4] Utifrån dessa bakomliggande omständigheter är syftet med min uppsats uppdelat i tre delar. Först och främst är syftet att undersöka om de olika alternativen för flöden av personuppgifter från EU till Storbritannien efter brexit kommer att rendera någon skillnad för aktörerna i förhållande till flödena inom unionen. För det andra är syftet att reda ut hur skillnaden i sådant fall tar sig uttryck – om skillnaderna som eventuellt uppstår genererar sämre[5] flöden. För det tredje, baserat på de

[1] 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 hävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1–88) (GDPR).
[2] Januari 2019.
[3] Jämför till exempel GDPR, artikel 44 – 50; om hur Storbritannien vill basera en framtida lösning på adekvansbeslutet se The Government of the United Kingdom, The future relationship between the United Kingdom and the European Union, 2018 (vitboken), 2018, sidan 74, https://www.gov.uk/government/publications/the-future-relationship-between-the-united-kingdom-and-the-european-union?utm_source=e5b3260b-2069-4b57-a5bd-24e9ea02aa88&utm_medium=email&utm_campaign=govuk-notifications&utm_content=immediate, använd den 21 september 2018; samt till exempel Europeiska kommissionen, *Meddelande från kommissionen till Europaparlamentet och rådet, Utbyte och skydd av personuppgifter i en globaliserad värld*, COM(2017) 7 final av den 10 januari 2017, sidan 4.
[4] Europeiska kommissionen, 2017, sidan 6.
[5] En närmare presentation av vad som avses med sämre respektive bättre flöden följer i avsnitt 2.2.

potentiella skillnaderna, är syftet att undersöka om adekvansbeslutet verkligen är det alternativ som innebär minst skillnad för aktörerna i förhållande till flödena i EU.

De alternativ jag kommer att arbeta utifrån för att navigera mig genom mitt syfte är först och främst att Storbritannien behandlas som ett tredjeland enligt GDPR:s bestämmelse om adekvat skyddsnivå efter bedömning av kommissionen.[6] Det andra är den lösning genom ett avtal bortom GDPR som Storbritannien uttryckt att man vill få till stånd i sin vitbok. Jag kommer emellertid att få anledning att beskriva varför min bedömning är att detta inte är ett *reellt* alternativ.[7] Det tredje alternativet är en utblick mot det partiella adekvansbeslut kommissionen fattat i relation till USA och Kanada.[8] Det sista alternativet är tillämpliga övriga tredjelandslösningar i GDPR, det vill säga lämpliga skyddsåtgärder och undantag i särskilda situationer.[9] Anledningen till att jag väljer denna ordning för de olika alternativen är att jag genomgående vill redogöra för de alternativ som bygger på adekvansbeslut, innan jag går in på övriga lösningar. En annan ordning, till exempel med alla lösningar enligt GDPR samlade följt av speciallösningar hade varit möjlig. Dock tror jag att min poäng att adekvansbeslutet generellt lyfts som den främsta lösningen för tredjelandsöverföring av personuppgifter stärks genom den ordning jag beskrivit, varför jag väljer densamma. Detta är också anledningen till att jag löpande i delarna efter adekvansbeslutet i viss mån hänvisar till och jämför med detta. Vad gäller jämförelsen tror jag också att en sådan komparation visar adekvansbeslutets och de övriga alternativens funktion mer tydligt.

Det ska nämnas att min infallsvinkel endast omfattar överföring av personuppgifter från EU till Storbritannien, inte tvärtom. För att göra en fullständig utredning av hur den framtida situationen skulle se ut för personuppgiftsflöden mellan EU och Storbritannien skulle de omvända flödena också behöva undersökas.[10] Dock, med hänsyn till att jag vill studera mötet mellan GDPR:s reglering och brexit utelämnas den omvända riktningen. Vidare, eftersom jag vill undersöka olika alternativ och deras betydelse i förhållande till skillnader i flödena från EU till Storbritannien har jag heller inte för avsikt att gå in närmare på sanktioner vid brott mot skyddet för personuppgifter. Jag kommer emellertid att i viss mån lyfta tillsynsmyndigheters befogenheter liksom aktörers ansvar.[11]

Skälen till att jag väljer just de alternativ som nämnts är flera. Först och främst är alternativen i GDPR för tredjelandsöverföring något jag vill behandla – inte bara på förekommen anledning – utan också eftersom de inbjuder till diskussion. Till exempel innebär adekvansprövningen i artikel 45 GDPR en bred översyn av Storbritanniens efterlevnad av mänskliga rättigheter.[12] Vidare, som nämnts, är adekvansbeslutet den lösning som allmänt sett verkar ses som den primära för tredjelandsöverföringar av personuppgifter.[13] Vad undantag i särskilda situationer angår, enligt

[6] GDPR, artikel 45.
[7] Avsnitt 4.3.
[8] Det så kallade ”Privacy Shield”(PS)-ramverket och lösningen för kommersiella aktörer i Kanada, Europeiska kommissionen, 2018, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en, använd den 14 december 2018.
[9] GDPR, artikel 46 och 49. GDPR, artikel 47 tas inte upp av skäl som förklaras i kapitel 6.
[10] Kommerskollegium, *Efter brexit – en analys av svenska intressen inför kommande förhandlingar*, 2018, sidorna 148 och 153.
[11] För sanktioner och ansvar, se GDPR kapitel VIII.
[12] Se kapitel 3.
[13] Europeiska kommissionen, 2017, sidan 6; vitboken sidan 74.

artikel 49 GDPR, kommer jag att begränsa mig till att behandla samtycke.[14] Detta främst eftersom samtycke är det mest välkända undantaget,[15] men också på grund av att individens obenägenhet att läsa villkor för samtycket leder mig till slutsatsen att det är det mest praktiskt användbara.[16] Samma skäl motiverar varför jag vid förklaring av vad som gäller för överföring inom unionen också endast behandlar samtycke.[17] Dessutom vill jag begränsa utredningen av lämpliga skyddsåtgärder i artikel 46 GDPR till förmån för samtycket i artikel 49.[18] De olika delarna i artikel 46 är snarlika varandra och innebär således likartade konsekvenser, medan samtycket innehåller många olika parametrar att diskutera.

Mitt val att analysera Storbritanniens vitbok tar avstamp i att det inledningsvis i detta arbete var en potentiell väg att gå för hanteringen av personuppgifter efter brexit. Synen på detta har emellertid ändrats under mitt arbetes gång, men vitboken tjänar fortfarande som ett underlag till hur man kan argumentera för en speciallösning för personuppgiftsflöden. Dessutom fungerar vitboken som ett sätt att visa hur speciallösningar egentligen inte ryms inom GDPR, liksom att den är en språngbräda till en redogörelse för speciallösningar som *ändå finns*. Dessa utgörs av konstruktioner för personuppgiftsflöden mellan EU och USA respektive Kanada.[19] I kapitel fem tittar jag närmare på båda dessa alternativ, vilka består i ett självcertifieringssystem för USA:s del, liksom ett beslut begränsat till nationell reglering för privata företag för Kanada.[20]

Alternativens substans är en viktig del i mina val. Det är emellertid också de signaler EU och Storbritannien sänt och sänder ut som ligger bakom mina alternativ. Till exempel har Storbritannien i förhållande till den relation EU har med Norge valts bort i kommande avsnitt till förmån för mina alternativ. Förvisso har en konstruktion som den EU har med Norge nämnts i debatten, som förslag till lösning för framtiden mellan EU och Storbritannien.[21] Dock, utifrån de uttalanden som finns från Storbritannien verkar det inte troligt att man skulle bli annat än ett tredjeland i förhållande till EU.[22] I sammanhanget vill *tredjeland* säga att Storbritannien varken skulle vara med i EU eller Europeiska ekonomiska samarbetsområdet (EES).[23] I denna bemärkelse är inte Norge ett tredjeland, eftersom man via European Free Trade Association (EFTA) är en del av EES. Genom sitt utträde ur EU träder också Storbritannien ur EES,[24] och skulle inte bli medlem i

[14] GDPR, artikel 49.1 a.
[15] I-scoop, u.d., https://www.i-scoop.eu/gdpr/consent-gdpr/, använd den 12 december 2018.
[16] Angående individens benägenhet att studera villkoren se Larsson, Stefan, *Den kvantifierade konsumenten: Om behovet av tillit och transparens på datadrivna marknader*, 2018, sidan 4, samt nedan i avsnitt 2.3.
[17] GDPR, artikel 6.1 a. För min redogörelse av detta, se nedan avsnitt 2.3.
[18] Se kapitel 6.
[19] Europeiska kommissionen, 2018, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en, använd den 14 december 2018; Europeiska kommissionen, 2017, sidan 7.
[20] Europeiska kommissionen, 2017, sidan 7.
[21] Wintour, Patrick, *Norwegian politicians reject UK's Norway-plus Brexit plan*, The Guardian, den 7 december 2018, https://www.theguardian.com/politics/2018/dec/07/norwegian-politicians-reject-uks-norway-plus-brexit-plan, använd den 10 december 2018.
[22] Jämför vitboken, sidan 74; om EFTA:s inställning se EFTA, 2018, http://www.efta.int/Advisory-Bodies/news/EFTA-Parliamentary-Committee-members-discuss-Brexit-counterparts-UK-507866, använd den 10 december 2018.
[23] Jonsson, Maria, med flera, Förordning 679/2016, 2018, artikel 44, Karnov 2018-07-01.
[24] Agreement on the European Economic Area (OJ No L 1, 3.1.1994 p. 3; and EFTA States' official gazettes) (EES-avtalet), artikel 126.1.

EFTA på annat sätt än genom förhandling.[25] I ljuset av att förhandlingar kan ta tid är det inte troligt att Storbritannien skulle bli medlem inom en snar framtid. Ytterligare en anledning att välja bort detta alternativ till förmån för de jag valt är att GDPR är tillämplig i EES.[26] Således vore inte en utredning av överföringen av personuppgifter inom EES särskilt intressant, även om *vägen till* en sådan lösning i och för sig skulle vara det.

Inom ramen för mina val finns heller inte det utträdesavtal[27] som förhandlats mellan EU och Storbritannien. Istället behandlar jag den situation som uppstår när Storbritannien väl utträder. I mitt arbete används alltså *brexit* för att beskriva den situation som uppstår efter att Storbritannien lämnat EU och efter det att en eventuell övergångsperiod mellan parterna löpt ut.[28] Anledningen till att jag väljer denna tidsram är först och främst att utträdesavtalet av den 14 november 2018 mellan EU och Storbritannien är mycket svårhanterlig materia. Eftersom förhandlingarna har pågått löpande under hösten 2018 hade en analys utifrån lösningen för personuppgiftsflöden inom ramen för utträdesavtalet varit mycket sårbar. Osäkerheten i förhandlingen kring utträdesavtalet mellan Storbritannien och EU har också varit den största svårigheten för mig eftersom det löpande har påverkat mitt arbete. Till exempel har EU:s indikationer på rörelse i riktning mot ett adekvansbeslut,[29] i kombination med en analys av vitboken och EU:s regelverk, visat att en lösning i enlighet med vitboken framstår som oerhört avlägsen.[30] De uppgifter som publicerats om hur personuppgiftsflöden skulle hanteras under en övergångsperiod har dessutom pekat på att man kommer att behandla uppgifterna som om Storbritannien fortfarande var medlem i EU.[31] En sådan situation bjuder inte till lika mycket diskussion som den man ännu inte hunnit förhandla klart – det vill säga perioden *efter* övergångsperioden. Den infallsvinkel jag har valt kan tänkas bli svår att hantera eftersom den i viss mån innebär spekulation om vad som kommer att ske. Även om så är fallet behandlar jag dock just denna genom mina utvalda alternativ, för att det på grund av osäkerheten finns all anledning att försöka få klarhet i de framtida omständigheterna.

1.2 Utformning av frågeställningar, material och metod – ett konkret exempel

I utformningen av mina frågeställningar har jag konstruerat ett exempel med hjälp av vilket jag kommer att dra slutsatser och genomföra analysen i kommande kapitel. Exemplet är hämtat ur ett dokument som den internetbaserade betaltjänsten PayPal publicerade i samband med ikraftträdandet av GDPR.[32] Man redovisar där alla potentiella situationer där personuppgifter

[25] Convention Establishing the European Free Trade Association (EFTA-konventionen), artikel 56.
[26] EFTA, 2018, http://www.efta.int/eea-lex/32016R0679, använd den 10 december 2018.
[27] Europeiska kommissionen, TF50 (2018) 55 Draft Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, as agreed at negotiators' level on 14 November 2018 (Utträdesavtalet av den 14 november 2018).
[28] Utträdesavtalet av den 14 november 2018, artikel 126; Europaportalen, *May vill förlänga övergångstid*, Europaportalen, den 19 oktober 2018, https://www.europaportalen.se/content/may-vill-forlanga-overgangstid, använd den 23 oktober 2018.
[29] Europeiska unionens råd, *Political declaration setting out the framework for the future relationship between the European Union and the United Kingdom* (politiska deklarationen), 2018, sidan 4.
[30] Se mer om detta i avsnitt 4.3.
[31] Utträdesavtalet av den 14 november 2018, artikel 70 – 71. Dock med undantag för samarbetsmekanismen i GDPR, se utträdesavtalet av den 14 november 2018, artikel 70 a.
[32] PayPal, 2018, https://www.paypal.com/ie/webapps/mpp/ua/third-parties-list-prev, använd den 20 september 2018.

skulle kunna tänkas delas med en utomstående part och vilka uppgifter som i sådant fall skulle delas med just denna.[33]

Situationen jag tänker mig gäller en privatperson[34] som har ett konto hos en betaltjänst via nätet.[35] Betaltjänsten har sitt säte i en medlemsstat i EU,[36] och är ett större privat företag, likt PayPal.[37] Denna samlar på digital väg in till exempel namn, adress, telefonnummer, mejladress et cetera till privatpersonen via det konto som hen skapat.[38] Eftersom betaltjänsten samlar in uppgifterna samt bestämmer vad ändamålet med detta är liksom hur dessa ska behandlas så är betaltjänsten personuppgiftsansvarig.[39] Betaltjänsten är som sagt ett privat företag och därför omfattas inte dess insamling av användarens personuppgifter av undantagen för tillämpning i GDPR.[40]

Betaltjänsten delar med sig av personuppgifter som samlas in via kontot till ett privat företag som befinner sig i Storbritannien. Detta gör man för att det senare företaget ska lagra uppgifterna och sedermera kunna utforma reklamkampanjer[41] för betaltjänstens räkning. Eftersom man delar med sig av uppgifterna för att företaget ska behandla uppgifterna för betaltjänstens[42] räkning, så är företaget i Storbritannien personuppgiftsbiträde som behandlar uppgifterna i tredjeland.[43] De personuppgifter man delar med sig av är till exempel namn, adress, telefonnummer och mejladress till kontoinnehavaren.[44] Liksom för betaltjänsten faller inte heller företagets behandling inom undantagen för tillämplighet av GDPR.[45] En del av ändamålet med den första insamlingen av uppgifterna är att dessa ska lämnas ut till den ytterligare mottagaren[46]. Således används uppgifterna

---

[33] Paypal, 2018; Schwab, Katharine, *How Widely Do Companies Share User Data? Here's A Chilling Glimpse*, Fast Company, den 19 januari 2018, https://www.fastcompany.com/90157501/how-widely-do-companies-share-user-data-heres-a-chilling-glimpse, använd den 20 september 2018.

[34] En fysisk person och inte en juridisk sådan, GDPR, artikel 1.1 och skäl 14.

[35] Betaltjänster via internet kategoriseras som informationssamhällets tjänster, Europaparlamentets och rådets direktiv 2000/31 av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (EGT L 178, 17.7.2000, s. 1–16) skäl 17; Europaparlamentets och rådets direktiv 98/84/EG av den 20 november 1998 om det rättsliga skyddet för tjänster som bygger på eller utgörs av villkorad tillgång (EGT L 320, 28.11.1998, s. 54–57); Europaparlamentets och Rådets direktiv 98/48/EG av den 20 juli 1998 om ändring av direktiv 98/34/EG om ett informationsförfarande beträffande tekniska standarder och föreskrifter (EGT L 217, 5.8.1998, s. 18–26), bilaga V; Europaparlamentets och rådets direktiv 98/34/EG av den 22 juni 1998 om ett informationsförfarande beträffande tekniska standarder och föreskrifter (EGT L 204, 21.7.1998, s. 37–48). Detta påverkar emellertid inte GDPR:s tillämplighet i typfallet, även om GDPR ej heller ska påverka den reglering som finns för dessa tjänster, jämför direktiv 2000/31 och GDPR, artikel 2.4.

[36] Det ligger således inom det territoriella tillämpningsområdet för förordningen, GDPR, artikel 3.1.

[37] Reuters, 2018, https://www.reuters.com/finance/stocks/company-profile/PYPL.O, använd den 29 november 2018.

[38] Just dessa uppgifter är typiska personuppgifter eftersom de identifierar, alternativt gör det möjligt att identifiera en fysisk person, GDPR, artikel 4.1. Eftersom man samlar in och lagrar personuppgifterna digitalt så behandlas dessa automatiskt, GDPR, artikel 2.1 och 4.2; Jonsson, med flera, Jonsson, med flera, Förordning 679/2016, 2018, artikel 2.1, Karnov 2018-07-01.

[39] GDPR, artikel 4.7.

[40] GDPR, artikel 2.2 a – d e contrario.

[41] Här ska tilläggas att det inte rör sig om direktmarknadsföring, som i uppsökande verksamhet specifikt riktad mot en privatperson, utan jag tänker mig en övergripande kampanj. För definition av direktmarknadsföring se International Chamber of Commerce Sweden, ICC:s Regler för Reklam och Marknadskommunikation, 2011, sidan 27.

[42] För den personuppgiftsansvariges räkning.

[43] GDPR, artikel 4.8 och 3.1.

[44] PayPal, 2018.

[45] GDPR, artikel 2.2 a – d e contrario.

[46] GDPR, artikel 4.9.

endast inom ramen för de ändamål man deklarerat från början. Själva utlämnandet är därför förenligt med principen om laglig behandling av personuppgifter enligt GDPR.[47]

Skälen till att jag vill använda mig av ett exempel i min utredning och analys, liksom skälen till att det blev just detta exempel, är flera. Först och främst handlar det om att konkretisera. Genom att använda ett exempel blir de abstrakta termer som annars i mångt och mycket präglar personuppgiftsskyddsreglerna mer konkreta och därmed, tror jag, enklare att ta till sig. Dessutom är ett konto hos en betaltjänst en välkänd företeelse, vilket också bidrar till konkretisering. För det andra illustrerar exemplet vad som typiskt sett avses med personuppgifter. Jag kommer att återkomma till detta närmare i avsnitt 2.1 om definitioner, så långt kan dock sägas att de uppgifter betaltjänsten här delar med sig av inte utgör särskilda sådana, som till exempel etniskt ursprung.[48] För det tredje vill jag se till hur aktörerna påverkas av Storbritanniens utträde, och inte fokusera på personuppgiftsskyddet i sig, även om det handlar om reglering av detta. Man ska emellertid komma ihåg att GDPR har två syften – skydd för individen, men också fria flöden av personuppgifter.[49] Genom att välja just detta exempel, med två privata företag når jag i min redogörelse och analys företagsperspektivet med fokus på de fria flödena, snarare än skyddet för individen. För det fjärde och sista, är detta ett metodologiskt val. Jag väljer detta exempel och detta perspektiv för att effektivt nå fram till de skillnader som potentiellt kan bli resultatet av de olika alternativen som finns för personuppgiftsflödena efter brexit. Skillnaderna jag är intresserad av är de som uppstår för de aktörer som vill verka över EU:s gräns mot Storbritannien. Företagsperspektivet är ett verktyg för att i analysen lyfta fram de praktiska skillnader som uppstår. Det är nämligen så att det kan uppstå många skillnader, till exempel i relationen mellan EU och Storbritannien, eller på lagteknisk nivå. Det är emellertid inte givet att dessa faktiskt leder till en skillnad på aktörsnivå, och det är denna senare skillnad jag vill finna. På så sätt kan exemplet metodologiskt effektivisera min utredning och analys, framför en mer abstrakt, eller om man så vill traditionell, metod.

För tydlighetens skull ska här nämnas att i fortsättningen av texten kallas de två aktörerna var för sig just *betaltjänsten* och *företaget*. Samlat benämner jag dem *aktörerna*. Samlingsnamnet för den särskilda situation jag valt att exemplifiera med kallar jag *typfallet*. Jag väljer att kalla exemplet typfallet just eftersom man behandlar typiska personuppgifter.

Redogörelsen för de olika stegen i typfallet ovan syftar till att, förutom att sätta ramarna för det, konstatera GDPR:s generella tillämplighet på typfallet. Typfallet faller inom GDPR:s materiella och territoriella tillämpningsområde.[50] Utifrån redogörelsen ovan är de frågeställningar jag ska behandla de följande:

1. Hur skulle överföringen av betaltjänstens insamlade personuppgifter från EU till Storbritannien se ut enligt reglerna om adekvansbeslut i artikel 45 GDPR?
2. Hur skulle överföringen av betaltjänstens insamlade personuppgifter från EU till Storbritannien se ut enligt Storbritanniens vitbok och är denna lösning ett reellt alternativ?

[47] GDPR, artikel 6. Se mer om detta nedan i avsnitt 2.3.
[48] GDPR, artikel 4.1 och artikel 9.
[49] GDPR, artikel 1.1.
[50] GDPR, artikel 2.1 och 3.1.

3. Utblick USA och Kanada – hur skulle överföringen av betaltjänstens insamlade personuppgifter från EU till Storbritannien se ut enligt dessa modeller?
4. Hur skulle överföringen av betaltjänstens insamlade personuppgifter från EU till Storbritannien se ut om inget adekvansbeslut kommer till stånd?

Avslutningsvis för att uppnå mitt syfte, ställer jag mig sedan i analysen frågan:

5. Utifrån de möjliga alternativen – blir det någon skillnad för betaltjänsten och företaget i förhållande till situationen inom unionen och betyder det i sådant fall ett sämre flöde?

Förutom typfallet har metoden för mitt arbete framför allt bestått i att läsa, tolka och analysera texter. Texterna kommer främst från EU:s institutioner, liksom från statliga organ i Storbritannien. De mest centrala dokumenten har varit GDPR, och Storbritanniens vitbok om den framtida relationen till unionen. Även andra dokument har emellertid haft stor betydelse för mitt arbete, till exempel tidigare adekvansbeslut från kommissionen, meddelanden från densamma, den politiska deklarationen EU antagit inför det framtida samarbetet med Storbritannien et cetera. Genom texterna har jag kunnat dra slutsatser kring mina alternativ och sedermera satt dessa i relation till varandra. Framförallt i mitt kapitel om adekvansbeslutet[51] har jag dessutom satt texter aktuella för den förevarande situationen i relation till tidigare dokument och praxis från liknande situationer. Med praxis åsyftas att det finns avgöranden på utflöde av personuppgifter till andra tredjeländer, avseende *tidigare* lagstiftning,[52] om än inte från en exakt likadan situation som vi nu står inför med brexit. Eftersom kombinationen GDPR och brexit aldrig uppstått förr så finns endast ett begränsat material skrivet om kombinationen av dessa två. Jag har därför varit tvungen att läsa äldre material för att närma mig förevarande situation. Det äldre materialet har inte bara bestått i praxis från tidigare lagstiftning, utan också den tidigare lagstiftningen i sig, liksom adekvansbeslut baserade på denna. Detta är naturligtvis förenat med faror som kan generera brister i mitt resultat. Förr och nu är inte detsamma och därför kan en utredning av dagens situation, både vad gäller brexit och GDPR, på basis av material från en annan period behäftas med sådant som sedan visar sig vara fel. För att minimera risken för att förfela min utredning har jag i kommande avsnitt noggrant identifierat de parametrar som låter sig jämföras mellan dagens situation och tidigare lagstiftning.

Att situationen är ny och det därmed egentligen inte finns någon litteratur på området gör att de texter jag tolkat, jämfört och kontextualiserat via typfallet, i stort sett enkom bestått av offentliga publikationer från EU och Storbritannien. Detta material som bas minskar risken för att min produkt blir spekulativ och vriden efter åsikter som kanske annars uttrycks i media med en viss agenda. Det har emellertid också inneburit att det emellanåt varit svårt att tolka och få klarhet i materialet, när de officiella texterna inte varit tydliga. För att bringa klarhet i detta har också en del av min metod varit att kontakta dels Storbritanniens dataskyddsmyndighet[53], dels den brittiska

[51] Se kapitel 3.
[52] Europaparlamentets och 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 (EGT L 281, 23.11.1995, s. 31–50) (direktiv 95/46); samt till exempel Domstolens dom (stora avdelningen) av den 6 oktober 2015. Maximillian Schrems mot Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650 (Schrems-målet).
[53] Information Commissioner's Office (ICO).

regeringens brexit-departement[54] för att ställa frågor. Dessa åtgärder genererade dessvärre inget annat resultat än vad som redan stod att finna i de publikationer som är offentliga.

Sammanfattningsvis kan således min metod sägas bestå i *texttolkning*, delvis med hjälp av frågor direkt ställda till texternas källor, *jämförelser* mellan olika texter och alternativ, liksom att *sätta utfallen i sammanhang* med hjälp av typfallet. Innan jag börjar tillämpa min metod och går in på de utredande delarna vill jag presentera några teoretiska utgångspunkter, som språngbräda till utredningen.

2 Grundläggande teoretiska utgångspunkter

2.1 Definitioner – personuppgifter, tillsynsmyndighet, privatperson och behandling

För förståelsen av GDPR, liksom en stor del av utredningen i min uppsats ska jag i denna del kort redogöra för några viktiga termer. Det rör sig dels om vad jag avser med personuppgifter och behandling, dels om hur tillsynsmyndigheters ansvar ser ut inom unionen och vem som skyddas av GDPR. När jag talar om vad *jag avser* med de två första termerna menas att jag har skalat ner dessa i viss mån i förhållande till den övergripande definitionen i GDPR.

I utredningen redogör jag för behandlingen av personuppgifter i ordinär mening. Således lämnar jag de särskilda kategorierna personuppgifter, inklusive barns och personuppgifter rörande brottmål, rättskipning och dylikt, därhän.[55] Denna avgränsning gör jag eftersom dessa typer av personuppgifter inte är de vanligaste,[56] och därför inte tjänar som ett i vidare mån generellt exempel för utflödet av personuppgifter från EU till tredjeland. En ytterligare anledning är naturligtvis att alla personuppgifter inte låter sig redogöras för inom ramen för mitt arbete. De personuppgifter som valts ut är emellertid, som sagt till exempel namn, mejladress, telefonnummer et cetera. Dessa är, enligt definitionen i GDPR typiskt sett sådana uppgifter som identifierar, alternativt gör det möjligt att identifiera en fysisk person, alltså *typexempel* på personuppgifter.[57]

Tillsynsmyndigheter nämns något i min text varför också en förklaring till hur dessa fungerar i EU är på sin plats. Tillsynsmyndigheterna finns för att kontrollera GDPR:s efterlevnad i medlemsstaterna.[58] Dessa är del av något som kallas för ”One Stop Shop”-mekanismen (OSS). OSS innebär att man som aktör bara ska behöva vända sig till en myndighet i den mån sådan kontakt behövs i relation till personuppgiftsbehandling.[59] Varje tillsynsmyndighet är behörig i ärenden inom det egna territoriet.[60] Dock, vid behandling som sker i flera medlemsstater, så kallad *gränsöverskridande behandling*, är den tillsynsmyndighet som finns där den personuppgiftsansvarige har sitt huvudsakliga verksamhetsställe ansvarig trots det gränsöverskridande momentet.[61] Dock kan man alltid vända sig till en lokal tillsynsmyndighet i lokala fall, när man har ett ärende som inte

[54] Department for Exiting the European Union.
[55] För regler kring nämnda personuppgifter, se GDPR, artikel 8, 9, 10 och 48.
[56] Jämför GDPR skäl 38 och 52, artikel 4.1, 8 och 9; Jonsson, med flera, Förordning 679/2016 artikel 9.1, Karnov 2018-07-01; Tillväxtverket, 2018, https://www.verksamt.se/driva/gdpr-dataskyddsregler/vad-ar-en-personuppgift, använd sen 21 september 2018.
[57] GDPR, artikel 4.1.
[58] GDPR, artikel 51.1.
[59] GDPR, artikel 56.1 – 2.
[60] GDPR, artikel 55.1.
[61] GDPR, artikel 56.1.

rör landet för det huvudsakliga verksamhetsstället.[62] En privatperson har dessutom privilegiet att kunna vända sig till vilken tillsynsmyndighet som helst inom hela unionen för att få hjälp med ett klagomål rörande personuppgifter.[63]

Begreppet privatperson innebär i sammanhanget att det är just fysiska personer som GDPR skyddar – det är individer som skyddas och inte juridiska personer.[64] Min begreppsanvändning kan komma att variera mellan fysisk person, privatperson eller individ genom texten – för omväxlings skull. Vad som avses är emellertid de som skyddas enligt GDPR, det vill säga *fysiska personer*, vilka i förordningen kallas *registrerade*.[65] Anledningen till att jag inte vill använda begreppet registrerad är att jag uppfattar det som abstrakt och att det för tankarna till ett register. Medveten om att det kan tyckas onödigt att använda andra benämningar än de som finns, gör jag ändå detta för att markera att det handlar om en konkret, fysisk person och inte något abstrakt.

När jag talar om *behandling* av personuppgifter avser jag de förfararanden som räknas upp i artikel 4.2 GDPR. Det kan således röra sig om till exempel insamling och lagring, som sagts ovan. I det typfall jag valt skulle det alltså handla om insamling och lagring av till exempel namn, adress, mejladress, telefonnummer, och så vidare.[66] Det ska emellertid påpekas att en typ av behandling kan vara just *överföring* av personuppgifter.[67] Överföring till tredjeland i den mening som jag avser utreda, och som regleras i artiklarna 44 – 50 GDPR, kommer jag dock att benämna i andra termer än behandling, företrädesvis *överföring* till tredjeland. Denna benämning använder jag för att det inte ska råda någon tvekan kring vilken behandling som avses.

2.2 Analysen – inom vilka ramar kommer eventuella skillnader för personuppgiftsflödena att bedömas?

Som redan antytts kommer resultatet av mina studier avslutningsvis att analyseras utifrån vilka skillnader som eventuellt uppstår i förhållande till hur personuppgiftsflödena regleras och fungerar i EU. Ett verktyg jag har för att genomföra analysen och komma till slutsats kan sägas vara den liberala grund som EU-samarbetet bygger på.[68] Tanken är inte att genom uppsatsen idogt propagera emot brexit. Det är emellertid så att jag vill skriva utifrån ett EU-perspektiv och en del av EU:s grundtanke är just att underlätta rörlighet inom unionen – det vill säga de fyra friheterna: fri rörlighet för varor, tjänster, personer och kapital.[69] På senare tid har dessutom röster höjts, såväl nationellt i Sverige som i övriga EU, för att även fri rörlighet för data bör vara att betrakta som en frihet i detta avseende.[70] De lagstiftningsinitiativ som kommit från EU de senaste åren vittnar om att fritt flöde av såväl personuppgifter som ickepersonuppgifter inom unionen är något man

[62] GDPR, artikel 56.2.
[63] GDPR, artikel 77.1.
[64] GDPR, artikel 1.1 och skäl 14.
[65] GDPR, artikel 4.1.
[66] PayPal, 2018.
[67] GDPR artikel 4.2.
[68] Fördraget om Europeiska unionens funktionssätt (EUT C 202, 7.6.2016, s. 1–388) (FEUF), artikel 26.2.
[69] FEUF, artikel 26.2.
[70] Se exempelvis Kommerskollegium, *Data Flows A Fifth Freedom for the Internal Market,* 2016, sidan 2; Nadkarni, Teixeira, Isabel, 2018, www.europarl.europa.eu/news/en/press-room/20180926IPR14403/free-flow-of-non-personal-data-parliament-approves-eu-s-fifth-freedom, använd den 12 december 2018; Kala, Kaspar, *Free movement of data as the 5th fundamental freedom of the European Union*, 2017, https://e-estonia.com/free-movement-of-data-as-the-5th-fundamental-freedom-of-the-european-union/, använd den 24 september 2018.

eftersträvar.[71] Samtidigt slår EU på fördragsnivå fast att personuppgifter ska vara skyddade.[72] Man kan sammanfatta fördragstexterna som att ett så fritt flöde av personuppgifter som möjligt, med bibehållen säkerhet för individen, är det som stadgas inom unionen. Mot bakgrund av det är utgångspunkten för mitt arbete just detta; ett så fritt flöde som möjligt av personuppgifter, med hänsyn tagen till individens säkerhet är *bättre*, sådant som begränsar ett dylikt flöde är *sämre*.

Så fritt flöde som möjligt inom unionen, med tillfredsställande hänsyn tagen till individens skyddsintressen är således bra och det som har bäst förankring i fördragen. Detta gäller emellertid som sagt *inom* unionen. Angående EU:s yttre relationer säger förvisso fördragen att man ska främja internationell handel och på sikt stävja internationella handelshinder.[73] Samtidigt ska emellertid EU också skydda bland annat sina värden och sin självständighet liksom de mänskliga rättigheterna,[74] det vill säga exempelvis skydd för personuppgifter.[75] Det blir en motsägelse vilken dock synliggör GDPR:s förankring i fördragen och förklarar det sätt på vilket GDPR är uppbyggd. Det vill säga att fritt flöde av personuppgifter ska gälla i EU, men skyddsmekanismer ska finnas för individen.[76] Samtidigt gäller ett *förbud* som utgångspunkt för överföring av uppgifterna till tredjeland.[77]

Utredningen tar således avstamp i att fritt flöde av data är bra. Motsatsvis är hinder som ställs upp mot det fria flödet problematiska, så länge inte dessa trumfas av något annat viktigare intresse som behöver tillgodoses. Ett sådant kan till exempel vara individens skydd för personuppgifter, som i fallet med GDPR.[78] Låt vara att detta fortfarande är ett problem ur det perspektivet att det fria flödet inte längre står fritt, men det ”ofria” flödet kan, som i detta fall, ha ett högre syfte. Analysen av de utredande delarna ska därför göras i ljuset av huruvida flödena blir mindre fria efter brexit i förhållande till rådande situation inom EU. Alltså, om aktörerna genom alternativen för tredjelandsöverföring behöver ta sig igenom fler hinder, till exempel mer administration som kan fördröja flödena, än i unionen. I sådant fall är det *sämre* än enligt GDPR i unionen, som representerar det *bättre* alternativet. Inbegripet i detta angreppssätt ligger att det är utifrån aktörerna jag kommer att utgå. Jag riktar således inte in mig på det primära av GDPR:s syften – *skyddet* för personuppgifter,[79] utan snarare det andra – *fritt flöde* av personuppgifter.[80] Som introduktion, för att skapa en bild av hur personuppgiftsflödena fungerar inom EU och för att ställa upp min måttstock, ska jag i det följande göra en redogörelse för vad jag kallar ”situation noll”.

2.3 ”Situation noll” – en introduktion till hur GDPR fungerar i EU

Situation noll representerar de omständigheter som gäller under hösten 2018, det vill säga att Storbritannien fortfarande är medlemsstat i EU. Betaltjänsten och företaget verkar här således

[71] GDPR, artikel 1.1; Europaparlamentets och rådets förordning (EU) 2018/1807 av den 14 november 2018 om en ram för det fria flödet av andra data än personuppgifter i Europeiska unionen (EUT L 303, 28.11.2018, s. 59–68), artikel 1.
[72] FEUF, artikel 16.1; Europeiska unionens stadga om de grundläggande rättigheterna (EUT C 326, 26.10.2012, s. 391–407) (stadgan), artikel 8.
[73] Fördraget om Europeiska unionen (EUT C 202, 7.6.2016, s. 1–388) (FEU), artikel 21.2 e; FEUF, artikel 206.
[74] FEU, artikel 21.2 a – b.
[75] Stadgan, artikel 8; EKMR, artikel 8.1.
[76] GDPR, artikel 1.
[77] GDPR, artikel 44.
[78] GDPR, skäl 4 och artikel 1.2.
[79] GDPR, artikel 1.2.
[80] GDPR, artikel 1.3.

inom unionen. I övrigt är omständigheterna desamma som de jag redogjort för ovan under 1.2, varför denna situation också är inom GDPR:s tillämplighet. [81]

GDPR har två syften, att skydda fysiska personer vad gäller behandlingen av deras personuppgifter, liksom att säkerställa ett fritt flöde av personuppgifter i unionen.[82] För betaltjänstens överföring innebär detta att man för att få föra över kontohavares namn, mejladresser et cetera till företaget i Storbritannien måste följa principerna som ställs upp i artikel 5 GDPR. Artikeln stipulerar i sex punkter vad den personuppgiftsansvarige under ansvar måste följa vid behandling av personuppgifter.[83] I förhållande till individen vars uppgifter behandlas ska man vara öppen, behandlingen ska vara korrekt och laglig.[84] Ändamålen för vilka man samlar in uppgifterna ska anges, liksom begränsas i så måtto att de ska vara berättigade och uttömmande.[85] De uppgifter man behandlar ska inte vara för omfattande i proportion till syftet med behandlingen, och uppgifterna ska vara korrekta.[86] Uppgifterna ska vidare inte lagras längre än vad som är nödvändigt med hänsyn till syftet, liksom behandlas så att de inte riskerar att hamna hos någon obehörig eller till exempel förstöras.[87]

Så långt om de principer som ska följas enligt artikel 5. I artikel 6 stadgas sedan vad det innebär att behandla personuppgifter *lagligt*. Artikel 6 slår således fast de rättsliga grunder på vilka behandling ska ske, och är alltså kumulativ till artikel 5.[88] Grunderna är alternativa,[89] och den som enligt mina avvägningar är mest praktiskt användbar och som jag därför ska använda för att förklara GDPR:s funktion inom EU, är samtycke.[90] Samtycke enligt GDPR innebär:

> *"samtycke* av den registrerade: varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne"[91]

Så som de allra flesta känner samtycket, i vart fall enligt min föreställning, är genom den ruta vi kryssar i för att bekräfta att vi samtycker till att man på en hemsida använder cookies. Just detta, att aktivt kryssa i en ruta, används som exempel på hur en individ kan uttrycka sitt samtycke i GDPR.[92] Eftersom samtycke dessutom är ett otvetydigt agerande, som avser något specifikt, och som är fullständigt frivilligt och informerat,[93] så finns inget utrymme för till exempel konkludent handlande – det innebär inte samtycke. Det finns emellertid inga formkrav för hur samtycket kan

[81] GDPR, artikel 2 och 3.1.
[82] GDPR, artikel 1.
[83] Angående ansvar, se specifikt GDPR, artikel 5.2.
[84] GDPR, artikel 5.1 a.
[85] GDPR, artikel 5.1 b.
[86] GDPR, artikel 5.1 c – d.
[87] GDPR, artikel 5.1 e – f.
[88] Jonsson, med flera, Förordning 679/2016, 2018, artikel 5, Karnov 2018-07-01.
[89] GDPR, artikel 6.1.
[90] GDPR, artikel 6.1 a.
[91] GDPR, artikel 4.11.
[92] GDPR, skäl 32.
[93] GDPR, skäl 32.

lämnas.[94] Detta betyder att samtycket i princip skulle kunna vara muntligt,[95] men den personuppgiftsansvarige, alltså betaltjänsten, måste kunna *visa* att samtycke finns.[96] I praktiken kan man således ifrågasätta om samtycket egentligen över huvud taget skulle kunna vara muntligt. Det *informerade* samtycket inbegriper bland annat att man samtycker till just den behandling som avses och dess syfte.[97] I förhållande till typfallet har jag preciserat att man informerar om att både överföringen till Storbritannien och behandlingen som där ska ske är känd från början. I relation till ett *informerat samtycke* är detta således inte ett problem om betaltjänsten använder samtycke som rättslig grund. Dock måste betaltjänsten be om ett särskilt samtycke för den ytterligare behandlingen, eftersom det ska vara specifikt.[98] Dessutom får betaltjänsten i sig inte villkoras av samtycke till den senare behandlingen eftersom den primära tjänsten inte är beroende av den senare behandlingen för att fungera, i sådant fall skulle samtyckets frivillighet vara tveksam.[99] Vidare ligger i den fullständiga friheten att man inte får störas nämnvärt i sin användning av till exempel en hemsida för att man inte accepterar cookies. I ett sådant fall riskerar man att ”samtycka” bara för att få en bättre användarupplevelse.[100] Individen måste dessutom ovillkorligt kunna återkalla sitt samtycke och hänsyn ska tas till om samtycket verkligen är frivilligt i den mån det åtföljs av fullgörande av ett avtal.[101]

I relation till begreppet ”informerat samtycke” går det att starkt ifrågasätta om det ens ryms inom samtyckets natur i detta sammanhang. En kritik som ofta lyfts i relation till samtycket är att detta aldrig kan vara tillräckligt informerat för att man egentligen ska förstå vad man samtycker till. När man klickar för att samtycka till något på en hemsida, antingen cookies, eller kanske en personuppgiftspolicy, är det endast en liten andel som faktiskt läser de villkor man samtycker till.[102] Istället läser de allra flesta inte villkoren alls.[103] Sammanfattningsvis kan man säga att det kan ifrågasättas om *informerat* samtycke över huvud taget kan uppstå. Privatpersoner läser oftast inte villkoren, och många aktörer kan egentligen inte precisera hur de kommer att använda uppgifterna eftersom villkoren för den digitaliserade marknaden hela tiden förändras.[104]

Ifrågasättandena till trots finns samtycket i GDPR och för aktörerna fungerar det således som en rättslig grund. Det ska tilläggas att det i skäl till GDPR anges att samtycke inte *bör* användas som rättslig grund i fall där det råder skillnad i maktförhållandena mellan användare och den som samlar in personuppgifter.[105] Här kan man därför ställa frågan om det i sådant fall är en legitim grund över huvud taget mellan en konsument och en, i detta fall, betaltjänstleverantör. Konsumenter är typiskt sett en grupp som ska skyddas och för vilken man genom reglering behöver stadga rättigheter för

---

[94] Jämför GDPR, artikel 4.11.
[95] Article 29 Data Protection Working Party(WP29), 17/ EN WP259 rev. 01 Guidelines on consent under Regulation 2016/679, 2017, sidan 18.
[96] GDPR, artikel 7.1.
[97] GDPR, skäl 32, 42 och 43.
[98] GDPR, skäl 32, 43 och artikel 4.11.
[99] GDPR, skäl 32, 43, artikel 4.11; WP29, 2017, sidan 9.
[100] GDPR, skäl 32, 43 och 42.
[101] GDPR, artikel 7.3 – 4.
[102] Larsson, 2018, sidan 4.
[103] Bechmann, Anja, *Non-inforfmed Consent Cultures: Privacy Policies and App Contracts on Facebook*, Journal of Media Business Studies, 2014, sidan 22.
[104] Berinato, Scott, *Stop Thinking About Consent: It Isn't Possible and It Is'nt Right*, Harvard Business Review, 2018, sidan 4.
[105] GDPR, skäl 43.

en stärkt position i förhållande till de kommersiella aktörerna.[106] Dock anges det i skälet att man speciellt ser en skillnad i maktförhållandet när den personuppgiftsansvarige är en myndighet, vilket inte är fallet här.[107] Skälet anger vidare att samtycke inte *bör* användas, alltså är det en uppmaning, men ingen skarp gräns. Det är dessutom ett faktum att man tillämpar samtycke i vid mån i relationen mellan företag och konsumenter,[108] utan någon reaktion från EU-håll. Detta i kombination med skälets formulering tyder på att man inte ser detta som en relation där samtycke inte skulle vara legitimt.

Trots kritiken finns samtycket således ändå där som en rättslig grund. När betaltjänsten så följer principerna och privatpersonen har samtyckt till behandling hos denna, liksom till överföring till och behandling hos företaget, har man en rättslig grund. Därefter finns ytterligare åtaganden för betaltjänsten. Först ska individen informeras om bland annat syftet med och rättslig grund för behandlingen, liksom uppgifter om vem som är personuppgiftsansvarig, och vem som är mottagare vid en överföring.[109] Alltså ska betaltjänsten för privatpersonen uppge att företaget i Storbritannien är mottagare. Dessutom ska man upplysa om vilken period man tänker behandla uppgifterna under, individens rätt till rättelse och tillgång, radering eller begränsning, rätten att återkalla sitt samtycke, liksom rätten att klaga till en tillsynsmyndighet.[110] Detta ska alltså betaltjänsten informera individen om, det är emellertid även sådan information som individen har *rätt att få tillgång till* enligt artikel 15 GDPR.

I detta sammanhang, där det finns en mottagare i Storbritannien, ska betaltjänsten underrätta företaget i det fall privatpersonen väljer att utnyttja sin rätt till rättelse, radering eller begränsning.[111] Således, i den mån privatpersonen väljer att till exempel ta tillbaka sitt samtycke, vilket omfattas av radering, ska betaltjänsten anmäla detta till företaget.[112] Ovan i avsnitt 1.2, där ramarna för typfallet med betaltjänsten och företaget mejslades ut, noterades att betaltjänsten är personuppgiftsansvarig och företaget personuppgiftsbiträde, tillika mottagare. Det är således betaltjänsten som ansvarar för att kunna visa att man handlar i enlighet med GDPR vad gäller personuppgiftsbehandling.[113] I den mån företaget i Storbritannien i sin behandling på något sätt skulle överträda GDPR:s bestämmelser är företaget emellertid att betrakta som personuppgiftsansvarig för just denna del av behandlingen.[114] Här ska också något påpekas om det ansvar som följer med rollerna som personuppgiftsansvarig och personuppgiftsbiträde. Betaltjänsten och företaget skulle vara solidariskt ansvariga för att ersätta privatpersonen i den mån behandling skett i strid med GDPR.[115] För betaltjänsten sträcker sig i sådant fall ansvaret till all sådan behandling man medverkat vid, för företaget å sin sida sträcker det sig till ansvar i den mån man inte uppfyllt sina skyldigheter enligt

[106] Europeiska kommissionen, Insyn i EU-politiken: Konsumentskydd, 2016, sidan 3.
[107] GDPR, skäl 43.
[108] Till exempel samtycke till cookies.
[109] GDPR, artikel 13.1 a, c och e. För en fullständig redogörelse för angivna och ytterligare informationspunkter se GDPR, artikel 13.1 i sin helhet.
[110] GDPR, artikel 13.2 a – d, samt artikel 15 – 18 för de specifika reglerna för de olika delarna av informationen.
[111] GDPR, artikel 19.
[112] GDPR, artikel 17.1 b och artikel 19.
[113] GDPR, artikel 24.1.
[114] GDPR, artikel 28.10.
[115] GDPR, artikel 82; Jonsson, med flera, Förordning 679/2016, 2018, artikel 82.4, Karnov 2018-07-01.

GDPR, alternativt inte följt de instruktioner man fått från betaltjänsten.[116] Dessa instruktioner måste naturligtvis i sig vara i enlighet med lagen.[117]

Man är alltså skyldig under skadeståndsansvar gentemot individen att följa GDPR när man behandlar personuppgifter inom unionen. I den mån en överträdelse faktiskt skulle ske, och man måste ta kontakt med en tillsynsmyndighet finns den så kallade ”One Stop Shop”-mekanismen (OSS)[118] inom unionen. OSS innebär att man, dels som privatperson vars personuppgifter behandlas, dels som personuppgiftsansvarig eller -biträde, inte behöver vända sig till mer än *en* myndighet för att hantera sina gränsöverskridande[119] personuppgiftsärenden.[120] Således ska en verksamhet inte behöva kontakta dataskyddsmyndigheter i varje enskild medlemsstat till vilken man har gränsöverskridande behandling. Istället ska det räcka att ta kontakt med den myndighet som finns där man har sitt huvudsakliga verksamhetsställe, denna är behörig att hantera ärendet och är den så kallade *ansvariga* tillsynsmyndigheten.[121] En privatperson å sin sida, kan vända sig till vilken tillsynsmyndighet som helst i unionen för att få ett ärende hanterat och behöver inte leta upp den ansvariga tillsynsmyndigheten.[122] Det kan sägas att man istället för att låta de privata subjekten hantera administrationen lägger man över det administrativa arbetet på dataskyddsmyndigheterna i medlemsstaterna, som på så sätt måste samarbeta enligt kapitel VII GDPR. För att OSS ska fungera måste medlemsstaterna samarbeta mellan tillsynsmyndigheter. Det finns dels bestämmelser om samarbetet,[123] dels för vad man kallar *mekanism för enhetlighet*.[124] Denna går främst ut på att man med samarbete och Europeiska dataskyddsstyrelsen (styrelsen) som verktyg ska kunna nå enhetlig tillämpning av reglerna i GDPR i unionen.[125] Styrelsen ska bland annat avge yttranden och fungera som tvistlösningsorgan i förhållande till tillsynsmyndigheternas tillsyn. Man skulle kunna kalla denna mekanism för ett slags infrastruktur för samarbete.

Genomgående för det som gäller inom unionen är, i konsekvens med vad som ovan sagts, att betaltjänsten ska vara transparent och informativ om sin behandling av personuppgifter. Dessa principer gäller oavsett om man bygger sin behandling på grunden samtycke eller ej. Samtycket å sin sida har sedermera flera egna parametrar som måste uppfyllas för att detta ska anses ha status som rättslig grund. Det vill säga att samtycket ska vara: frivilligt, specifikt, informerat och otvetydigt. Samtyckets konstruktion och dess karaktär av informerat, liksom dess tillämpning i förhållande till konsumenter kan ifrågasättas. Likväl finns det ändå som en rättslig grund för aktörerna att tillämpa. Betaltjänsten och företaget är emellertid ansvariga för att behandlingen uppfyller kraven enligt GDPR och vid skada för individen bär dessa ett solidariskt ansvar att betala skadestånd.

---

116 GDPR, artikel 82.2.
117 GDPR, artikel 82.2.
118 På svenska kallas denna ”mekanismen för en enda kontaktpunkt”, den svenska översättningen av GDPR, skäl 127. Jag väljer emellertid för mitt arbete att förkorta denna OSS.
119 Gränsöverskridande behandling definieras som behandling vid verksamhetsställen i mer än en medlemsstat, eller behandling som påverkar eller sannolikt kommer att påverka, i väsentlig grad, registrerade i mer än en medlemsstat, GDPR, artikel 4.23.
120 GDPR, artikel 56.1 – 2.
121 GDPR, artikel 56.1 och 6.
122 GDPR, artikel 77.1.
123 GDPR, artikel 60 – 62.
124 GDPR, artikel 63.
125 GDPR, artikel 63 – 67.

Från situation noll och GDPR:s funktion inom EU ska jag nu gå vidare för att reda ut de olika alternativen för personuppgiftsflöden som finns i förhållande till tredjeland. Först och främst ska adekvansbeslutet enligt artikel 45 GDPR behandlas.

3 Hur skulle överföringen av betaltjänstens insamlade personuppgifter från EU till Storbritannien se ut enligt reglerna om adekvansbeslut i artikel 45 GDPR?

Utgångspunkten för överföring av personuppgifter till tredjeland från unionen är att det är förbjudet.[126] Denna position är alltså skild från vad som gäller inom EU, där fritt flöde gäller, under förutsättning att GDPR:s andra syfte om skydd för fysiska personer uppfylls.[127] Det kan i och för sig ifrågasättas huruvida dessa infallsvinklar verkligen är särskilt väsensskilda – båda stipulerar egentligen att uppgifterna inte får flöda om inte vissa villkor uppfylls.[128] Diskussionen om effekten av dessa två bestämmelser egentligen blir densamma lämnas emellertid därhän för tillfället eftersom den inte utgör fokus för mitt arbete. Istället noterar jag bara att man ser på dessa två situationer av flöden utifrån vad man kan kalla ett negativt och ett positivt perspektiv. För att trots förbudet få föra över personuppgifter till tredjelandet (Storbritannien) måste därför något av undantagen till förbudet kunna tillämpas. Det första av dessa är beslut från kommissionen om adekvat skyddsnivå enligt artikel 45 GDPR. Det rör sig alltså om ett undantag från förbudet att överföra uppgifter till tredjeland, förutsatt att tredjelandet uppfyller en *adekvat skyddsnivå* gällande personuppgifter. Det vill säga i princip om landet ifråga har ett tillräckligt högt skydd för att kunna tillgodose rättigheter i förhållande till individen.[129] Oaktat adekvansbeslutet som sådant innebär själva beslutet att ens inleda en prövning av skyddsnivån i ett land ett ställningstagande från kommissionen. Kommissionen kan precis lika gärna bestämma sig för att inte pröva frågan eftersom det är ett unilateralt beslut.[130] I detta fall har man emellertid, i den politiska deklaration rådet antagit inför den framtida relationen med Storbritannien i princip utfäst sig att pröva skyddsnivån i Storbritannien.[131] Detta innebär dock inte att man faktiskt kommer att fatta ett beslut om detta,[132] samt att en politisk deklaration inte är juridiskt bindande varför man i och för sig skulle kunna frångå denna.

Funktionen av adekvansbeslutet består i, förutsatt att det omfattar det territorium eller den sektor som en aktör verkar inom, att denna kan överföra sina uppgifter till Storbritannien utan något särskilt tillstånd.[133] Utan särskilt tillstånd betyder att överföringen skulle fungera i stort sett som om Storbritannien fortsatt var en del av unionen.[134] Detta inbegriper att man fortfarande måste följa

[126] GDPR, artikel 44.
[127] GDPR, artikel 1 och 5.
[128] Jämför GDPR artikel 5 och 44.
[129] Jämför GDPR, artikel 45.2.
[130] Kommerskollegium, *Efter brexit – en analys av svenska intressen inför kommande förhandlingar*, 2018, sidan 148.
[131] Politiska deklarationen, sidan 4.
[132] Politiska deklarationen, sidan 4.
[133] GDPR, artikel 45.1.
[134] Europeiska kommissionen, 2017, sidan 6.

det som gäller generellt för behandling av personuppgifter, det vill säga de skyldigheter som ställts upp i situation noll.[135]

Innan ett beslut om adekvat skyddsnivå kan vara på plats finns en omfattande process att gå igenom, dels från kommissionens sida,[136] dels potentiellt för Storbritannien avhängigt den nationella situationen. Det är dessutom så att flera parter antingen ska utvärdera förslaget till beslut, eller godkänna det, innan det slutligen kan antas av kommissionen.[137] I den politiska deklarationen inför det framtida samarbetet har EU dock uttryckt att man kommer att *anstränga* sig för att ha ett adekvansbeslut att anta i slutet av 2020, i den mån Storbritannien uppfyller kraven.[138] I deklarationen tar man således höjd för att undvika en period där man helt står utan lösning för personuppgiftsflödena. Dock, beroende på hur långt man når genom sina ansträngningar, behöver eventuellt processen ändå väntas ut innan betaltjänsten kan föra över personuppgifter till företaget i Storbritannien enligt artikel 45 GDPR. Även i utkastet till utträdesavtalet av den 14 november 2018 har adekvansbeslutet nämnts som en lösning framöver av kommissionen.[139]

EU har emellertid också sagt att man inte kommer att inleda en prövning förrän Storbritannien blir ett tredjeland, även om Storbritannien uttryckt att man redan nu är redo att inleda förhandlingar.[140] Detta får antas innebära den 29 mars 2019, mot bakgrund av att man vill ha beslutet klart i slutet av 2020. I information från kommissionen för det fall det inte blir något utträdesavtal med Storbritannien har man inte uteslutit någon av de övriga tredjelandslösningarna i GDPR.[141] Man lyfter således inte adekvansbeslut som något som nödvändigtvis är mer troligt än något annat. Istället påpekar kommissionen snarare att företag som påverkas av brexit måste förbereda sig för ett så kallat ”no deal-scenario”.[142] Det finns emellertid ytterligare ett dokument som kan ge en indikation om vartåt kommissionen lutar i frågan om ett adekvansbeslut. I ett meddelande kommissionen publicerade i januari 2017 tar man upp kriterier för att man ska inleda ett förfarande om adekvansbeslut.[143] För att påbörja ett sådant ska man enligt kommissionen beakta: affärsförbindelserna med tredjelandet, omfattningen av personuppgiftsflödet mellan EU och landet, hur framstående landet är inom dataskydd och generellt de politiska förbindelser man har med det.[144]

Utifrån de kriterier som räknas upp alldeles ovan är det svårt att se att kommissionen skulle undvika att inleda ett förfarande om ett eventuellt adekvansbeslut gentemot Storbritannien. Eftersom Storbritannien är och kommer att vara en före detta medlemsstat finns det nära affärsförbindelser

---

135 GDPR, artikel 44.
136 Europeiska kommissionen, 2018, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en, använd den 27 november 2018.
137 Europeiska kommissionen, 2018, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en, använd den 27 november 2018.
138 Politiska deklarationen, sidan 4.
139 Utträdesavtalet av den 14 november 2018, artikel 71.1 b.
140 Department for Digital, Culture, Media & Sport, 2018, https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal/data-protection-if-theres-no-brexit-deal, använd den 27 november 2018.
141 Europeiska kommissionen, Withdrawal of the United Kingdom from the Union and the EU Rules in the Field of Data Protection, 2018.
142 Europeiska kommissionen, Withdrawal of the United Kingdom from the Union and the EU Rules in the Field of Data Protection, 2018.
143 Europeiska kommissionen, 2017, sidan 8.
144 Europeiska kommissionen, 2017, sidan 8.

med EU. I och med GDPR flödar personuppgifter i nuläget fritt mellan Storbritannien och övriga EU, liksom att Storbritannien också har en skyddsnivå för personuppgifter som står i överensstämmelse med EU:s. Politiskt kan knappast något annat sägas än att Storbritannien varit väl insatt och delaktigt i EU-arbetet i egenskap av medlemsstat. Storbritannien uppfyller således alla kriterier som kommissionen själv ställer upp för att *inleda* förfarandet för adekvansbeslut. Detta, liksom vad som uttrycks i den politiska deklarationen, tyder på att man kommer att inleda en adekvansprövning i förhållande till Storbritannien.

För att visa hur processen går till går jag i följande avsnitt igenom de parametrar kommissionen har att bedöma för ett adekvansbeslut liksom hur den nationella situationen i Storbritannien ser ut. Kapitlet avslutas sedermera med att jag drar slutsatser och gå in på den mer specifika betydelse ett adekvansbeslut och dess process kan ha för betaltjänsten och företaget.

3.1 Delar för kommissionen att bedöma för ett beslut om adekvat skyddsnivå för personuppgifter i Storbritannien

Artikel 45 GDPR stadgar en rad omständigheter som kommissionen särskilt ska ta hänsyn till vid bedömningen av om adekvat skyddsnivå föreligger eller ej. Kommissionen ska därför bland annat särskilt se till Storbritanniens position för: rättsstatsprinciper, mänskliga rättigheter, säkerhet, försvar, myndigheters tillgång till personuppgifter, dataskydd, möjlighet till prövning och verkställbara rättigheter.[145] Även en genomlysning av lagstiftningen i Storbritannien på de uppräknade områdena ska göras.[146] Vidare ska kommissionen granska om Storbritannien har en tillfredsställande organisation kring tillsynsmyndigheten för dataskyddsfrågor, dess verkställighetsbefogenheter och samarbete med motsvarande myndigheter i medlemsstaterna.[147] Till sist i artikelns andra punkt nämns att kommissionen också särskilt ska se till Storbritanniens internationella åtaganden i sin bedömning,[148] det vill säga vilka internationella konventioner och liknande Storbritannien är part i.

En motsvarande bestämmelse fanns i GDPR:s föregångare direktiv 95/46. Denna var emellertid inte lika explicit i sin ordalydelse kring vad kommissionen särskilt bör ta hänsyn till, utan pekade endast ut att adekvat skyddsnivå kan uppnås genom nationell lagstiftning och internationella åtaganden.[149] Situationen var inte densamma före GDPR som den vi nu befinner oss i och direktiv 95/46 och GDPR är inte helt likalydande. Först och främst var GDPR:s föregångare ett direktiv, och GDPR är en förordning. Direktiv är reglering medlemsstaterna införlivar i sin egen, nationella lagstiftning, medan förordningar är direkt tillämpliga.[150] Något man kan skönja som motivering bakom valet att utforma den nya regleringen som förordning är att införlivandet av det tidigare direktivet i medlemsstaternas lagstiftning gett upphov till *olika* skydd och personuppgiftsflöde inom EU.[151] Utöver de varierande omständigheterna innehåller GDPR dessutom materiellt några viktiga

[145] GDPR, artikel 45.2 a; stadgan, artikel 7, 8, 11, 47 och 52.1.
[146] GDPR, artikel 45.2 a.
[147] GDPR, artikel 45.2 b.
[148] GDPR, artikel 45.2 c.
[149] Direktiv 95/46, artikel 25.6.
[150] FEU, artikel 288; Europeiska unionen, https://europa.eu/european-union/eu-law/legal-acts_sv, använd den 21 oktober 2018.
[151] GDPR, skäl 9 och 10.

skillnader i förhållande till direktiv 95/46.[152] Till exempel gäller nu justerade konsekvenser vid överträdelser,[153] liksom hårdare krav för att samtycke ska anses föreligga.[154] Den personuppgiftsansvarige ska kunna visa att samtycke har lämnats.[155] Det ska tilläggas att uppräkningen av omständigheter för kommissionen att ta särskild hänsyn till i artikel 45 GDPR inte är uttömmande,[156] liksom, som nyss nämnts, att den tidigare regleringen inte var specifik.[157] Således utesluter, eller uteslöt, inte dessa att ytterligare omständigheter läggs, eller lades, till bedömningen av huruvida skyddsnivån är, eller var, adekvat.

Jag vill poängtera skillnaderna mellan regleringarna för att visa att det inte rakt av går att göra en jämförelse mellan de två, och därtill kopplad praxis. Just vad gäller adekvansbesluten visar emellertid en genomgång av dessa, trots regleringarnas skillnader, att en jämförelse potentiellt låter sig göras. Enligt den tidigare regleringen var de parametrar man främst tog hänsyn till vid bedömningen av skyddsnivån följande: hur tredjelandets nationella reglering såg ut, internationella åtaganden, oberoende tillsyn av en tillsynsmyndighet, liksom effektiva rättsmedel för enskilda.[158] Inom ramen för detta har kommissionen beaktat huruvida mänskliga rättigheter tillgodoses, rättsstatliga principer följs et cetera. Sammanfattningsvis kan sägas att adekvansbesluten visar att man analyserat situationen i tredjelandet för att se om regleringen och organisationen där motsvarar de principer som stadgas enligt EU-rätten. Uppnås denna nivå har också en adekvat skyddsnivå ansetts föreligga.[159] Även om det kan konstateras att regleringarna inte är helt desamma ur skyddshänseende, visar alltså en genomgång ändå att adekvansbesluten sedan tidigare tagit hänsyn till ungefär de parametrar som räknas upp i GDPR idag. Därför drar jag slutsatsen att adekvansbesluten från den tidigare regleringen kan tjäna som ledning för vad kommissionen ska ta hänsyn till vid en bedömning av Storbritannien efter brexit.

Det ska tilläggas här att EU-domstolen (EUD) i praxis gällande direktiv 95/46 uttalat att det skydd som garanteras av ett tredjeland inte kan krävas vara identiskt med det som föreskrivs i direktivet, men att ett likvärdigt skydd måste gälla och säkerställas enligt landets egen lagstiftning.[160] Som jag konstaterat i stycket ovan är detta således vad adekvansbeslutets olika parametrar kan sammanfattas resultera i. Principerna som finns i EU-rätten ska finnas representerade i tredjelandets lagstiftning, om än inte nödvändigtvis ett exakt *likalydande* skydd.

---

[152] Jonsson, med flera, Förordning 679/2016, 2018, artikel 13, Karnov 2018-07-01.
[153] GDPR, artikel 77 – 84 jämfört med direktiv 95/46, artikel 22 – 24.
[154] GDPR, artikel 4.11 och skäl 32 jämfört med direktiv 95/46, artikel 2 h.
[155] GDPR, artikel 7.1.
[156] Se formuleringen ”särskilt beakta” i artikel 45.2.
[157] Direktiv 95/46, artikel 25.6.
[158] Se till exempel Kommissionens beslut av den 8 maj 2008 i enlighet med Europaparlamentets och rådets direktiv 95/46/EG om adekvat skydd för personuppgifter på Jersey (2008/393/EG) (EUT L 138, 28.5.2008, s. 21–23) (adekvansbeslut för Jersey); Kommissionens beslut av den 28 april 2004 om skyddsnivån för personuppgifter på Isle of Man (2004/411/EG) (EUT L 151, 30.4.2004, s. 48–51) (adekvansbeslut för Isle of Man).
[159] Se till exempel Kommissionens beslut av den 21 november 2003 om skyddsnivån för personuppgifter på Guernsey (2003/821/EG) (EUT L 308, 25.11.2003, s. 27–28) (adekvansbeslut för Guernsey).
[160] Schrems-målet.

3.1.1 Storbritanniens nationella rätt

3.1.1.1 Data Protection Act 2018 och GDPR

I relation till Storbritannien finns det flera adekvansbeslut sedan tidigare för länder som ligger under den brittiska kronan, men som inte är en del av Storbritannien. Det rör sig om Isle of Man, Jersey och Guernsey. En omständighet som är gemensam för dessa länder är att deras personuppgiftslagstiftning ofta är baserad på EU-reglering, alltså sådan som redan gällt i Storbritannien. Dessutom har Storbritanniens ratificering av Europarådets konvention 108[161] sträckts ut för att också omfatta dessa länder. Där finns således dels exempel på inhemsk lag som baseras på EU-rätt liksom internationella åtaganden som är gemensamma med Storbritannien.[162]

När den inhemska rätten baseras direkt på EU-rätten är det rimligtvis så att de principer som finns i unionsrätten, och som kommissionen efterfrågar vid en adekvansbedömning, också finns representerade i tredjelandets lag. Poängen med detta resonemang och det i föregående stycke är att det här är omständigheter som i viss mån finns i Storbritannien idag, inför utträdet ur unionen. Part till konvention 108 är man oavsett sitt utträde, det är ett dokument av Europarådet. Vidare har man, eftersom GDPR trädde ikraft i maj 2018, redan anpassat sin nationella rätt efter denna reglering. GDPR är i och för sig en förordning och alltså direkt tillämplig nationellt. Vad Storbritannien gjort i den nationella lagstiftningen är emellertid att konsekvent hänvisa till GDPR:s lydelser samt kompletterat denna, så som medlemsstaterna får göra.[163] Det är således, genom hänvisningarna, den ursprungliga texten som är tillämplig. Man har alltså som utgångspunkt en inhemsk reglering som följer EU-rätten,[164] som sig förvisso bör när man är en medlemsstat, men inte nödvändigtvis behöver vara fallet när utträdet sedermera blir verklighet. Vad som går att utläsa från Storbritanniens ståndpunkt inför utträdet ur unionen är att man ser sig ha en fördelaktig startposition i förhållande till EU och GDPR:s regler om adekvansbeslut. Denna uppfattning är sprungen ur att man har just en lagstiftning som hänvisar till GDPR.[165] Mot bakgrund av det finns inget som tyder på att man skulle vilja reglera, så att säga *bort från* GDPR. Istället vill man fortsätta tillämpa den specifika rättsakten efter utträdet, i den mån ingen annan överenskommelse nås med EU.[166] Man påpekar också att ingen omedelbar skillnad kommer att uppstå i skyddet för flöden av persondata från EU till Storbritannien, eftersom man fortsatt stödjer sig på GDPR.[167] Man förefaller vilja utnyttja just att den nationella lagen tar avstamp i EU-rätten.

Kommissionen ska således göra en bedömning av Storbritanniens nationella lag ”Data Protection Act 2018” (DPA). Denna är förvisso i nuläget anpassad till GDPR i så måtto att den tar hänsyn till de principer och krav som GDPR ställer upp. Dock är själva designen sådan att reglerna ständigt refererar till GDPR. Till exempel hänvisar andra artikeln till att GDPR och förevarande akt skyddar individer mot missbruk av deras personuppgifter.[168] Frågan blir i detta sammanhang hur det ska

[161] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108) (konvention 108).
[162] Se till exempel adekvansbeslut för Jersey och adekvansbeslut för Isle of Man.
[163] Se till exempel artikel 6.2 GDPR om laglig behandling av personuppgifter; samt Information Commissioner's Office, 2018, https://ico.org.uk/for-organisations/data-protection-act-2018/, använd den 23 oktober 2018.
[164] Vitboken, sidan 75.
[165] Vitboken, sidorna 74 – 75.
[166] The Government of the United Kingdom, European Union (Withdrawal) Act 2018 (Withdrawal Act 2018), 2018, sektion 3; Department for Digital, Culture, Media & Sport, 2018.
[167] Department for Digital, Culture, Media & Sport, 2018.
[168] DPA, sektion 2.

läsas när Storbritannien väl trätt ur EU. Det är korrekt att GDPR som sådan delvis finns till för att skydda individen mot missbruk av personuppgifter,[169] men detta gäller *för unionen* enligt vad som anges om den territoriella tillämpningen.[170] Här vill jag dessutom påminna om att Storbritannien, som nämnts, inte längre kommer att vara medlem i EES, där GDPR är tillämplig.[171] För att kunna tala om en inhemsk reglering som fortsatt stödjer sig på GDPR kommer därför krävas att man på något sätt garanterar dess tillämplighet i det brittiska systemet.

Storbritannien har naturligtvis sett till att utforma en lösning för hur den EU-rätt som man vill behålla efter utträdet ska kunna överföras till nationell rätt. GDPR är gällande nationellt även efter brexit, eftersom den är direkt tillämplig i Storbritannien före utträdesdagen och ej heller undantagen enligt Storbritanniens Withdrawal Act 2018, som antagits för inkorporering av EU-rätt nationellt.[172] Man har således löst en del av problemet med tillämpligheten genom att så att säga erkänna viss reglering som nationell i den mån den uppfyller vissa krav. Den brist som uppstår i och med GDPR:s territoriella tillämpningsområde har man lagt in en mekanism i Withdrawal Act 2018 för att läka.[173] Till exempel kan man via denna justera EU-lagstiftning som annars varit beroende av Storbritanniens status som medlemsstat för att anpassa den till att enkom fungera som nationell rätt – man transformerar den.[174] Det vill säga att man ändrar akterna på nationell nivå, men inte på EU-nivå, tekniskt rör det sig alltså inte längre om EU-lagstiftning. Dessa ändringar kommer bara att kunna göras enligt den aktuella sektionen i Withdrawal Act 2018 i två år från och med utträdesdagen.[175]

För att fullt inkorporera en EU-rättsakt som är avhängig Storbritanniens status som medlemsstat nationellt behöver således översättningen ske i två led. Dels genom att uppfylla kraven för att vara tillämplig nationellt, dels genom textmässig justering.[176] Min bedömning är, eftersom man vill behålla GDPR, att man *behöver* göra denna typ av textuella ändring för att kunna tala om en personuppgiftsreglering baserad på EU-rätten och som lever upp till de principer som gäller enligt densamma. Än så länge har inte någon sådan textuell ändring gjorts.[177] Man har ej heller uttryckt att man *ska* justera GDPR enligt detta textmässiga förfarande, även om man sagt att i ett scenario där inget annat överenskommits kommer GDPR att inkorporeras via Withdrawal Act 2018.[178]

---

169 GDPR, artikel 1.
170 GDPR, artikel 3.
171 EES-avtalet, artikel 126.1; Vahl, Marius, 2018, http://www.efta.int/EEA/news/General-Data-Protection-Regulation-incorporated-EEA-Agreement-509291, använd den 20 september 2018.
172 Withdrawal Act 2018, sektion 3 (1 – 3).
173 Withdrawal Act 2018, sektion 8.
174 Withdrawal Act 2018, sektion 8 (1 – 2).
175 Withdrawal Act 2018, sektion 8 (8).
176 Withdrawal Act 2018, sektion 3 (1 – 2) och sektion 8 (1 – 2).
177 Den 22 december 2018. Se dock löpande uppdateringar i lista från Linklaters, https://www.linklaters.com/Brexit-SI-Tracker, använd den 22 december 2018.
178 Department for Digital, Culture, Media & Sport, 2018. På fråga till brittiska regeringens Department for Exiting the European Union i ärendet framkom inget annat än att en ändring av GDPR i detta avseende är avhängig hur brittiska parlamentet röstar dagen för omröstning av en eventuell ändring. Man svarade inget om när en sådan omröstning skulle kunna ske, och hänvisade i övrigt till adekvansbeslut och till de höga ambitioner Storbritannien uttryckt för persondataflöden i vitboken, Department for Exiting the European Union Correspondence Unit, den 30 november 2018.

Kommissionens bedömning i detta sammanhang skulle alltså behöva göras utifrån hur Storbritanniens lagstiftning faktiskt tar hänsyn till och tillämpar de principer som GDPR ställer upp. Dessa måste vara tillämpbara i Storbritannien även efter utträdet. Storbritannien måste således av allt att döma justera och formulera sin lagstiftning annorlunda för att garantera uppfyllandet av GDPR:s principer. GDPR är emellertid inte den enda rättsakt som behandlar ämnet personuppgifter i EU-rätten. För att adekvat skyddsnivå ska kunna anses föreligga måste också förenlighet med stadgan kunna konstateras.[179] Det är rent av så att EUD underkänt giltigheten av adekvansbeslut från kommissionen på den grunden att oförenlighet med stadgan varit fallet, i det så kallade Schrems-målet.

3.1.1.2 Förhållandet till stadgan

När Storbritannien lämnar unionen lämnar man också stadgan – tillämpningsområdet sträcker sig till medlemsstaterna och deras tillämpning av EU-rätten.[180] Detta faktum konstaterar också Storbritannien uttryckligen i Withdrawal Act 2018.[181] En fråga som väcks är varför man deklarerar detta så tydligt, när man samtidigt är benägen att behålla många EU-rättsakter genom att transformera dem till nationell rätt.[182] Dessutom är det så att till exempel GDPR hänvisar till stadgan som en grund på vilken akten har antagits.[183] Det är inte självklart ur ett lagtekniskt perspektiv att man kan tillämpa lagstiftning som grundar sig på och hänvisar till stadgan när man inte är part till denna själv eftersom stadgan endast är tillämplig i medlemsstater i EU.[184] Potentiellt skulle detta kunna vara en del av den ändring som behövs för GDPR på nationell nivå. Dock verkar det som att det inte är den lösning man tänkt sig. Istället har man, samtidigt som man tar avstånd från stadgan, sagt att hänvisningar till stadgan och dess rättigheter i tidigare EU-rätt kan behållas, så länge rättigheterna som stadgas däri är självständigt existerande, alltså oberoende av just stadgan.[185] Det är inte tydligt om man med skrivningen närmast menar på ett naturrättsligt plan, eller om man menar att rättigheterna existerar i andra rättsakter. En genomlysning av de rättigheter som finns i stadgan och de som finns enligt andra akter för mänskliga rättigheter som Storbritannien är bundet av visar emellertid att det finns en diskrepans mellan dokumenten.[186]

Det skydd som ställs upp i stadgan är enligt ordalydelsen i artikel 8:

> ”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

[179] Framförallt stadgan, artikel 7 och 8, men även artikel 11 om yttrandefrihet, artikel 47 om domstolsprövning och 52.1 om begränsning av rättigheterna, se Schrems-målet.
[180] Stadgan, artikel 51.1.
[181] Withdrawal Act 2018, sektion 5 (4).
[182] Jämför Linklaters, 2018.
[183] GDPR, skäl 1 och artikel 1.2.
[184] Stadgan, artikel 51.1.
[185] Withdrawal Act 2018, sektion 5 (5).
[186] Här åsyftas att stadgans rättigheter för privatpersoner gällande deras uppgifter skiljer sig från motsvarande skydd i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Rom, 4.XI.1950) (EKMR) och konvention 108.

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."

I förhållande till ordalydelsen i EKMR och konvention 108 finns flera viktiga skillnader i skyddet. För det första är rättsakterna tillkomna inom ramen för olika typer av samlingar av länder,[187] vilket gör att de skiljer sig åt redan där. Detta behöver dock inte betyda att skyddet för privatpersoner egentligen skiljer sig nämnvärt mellan akterna. Vad som emellertid visar sig vid en jämförelse mellan dem är att EKMR och konvention 108 saknar garanterad tillsyn av en oberoende myndighet.[188] I de två senare finns vidare inga uttryckliga legitima grunder att behandla personuppgifter på. Dessutom är rätten till rättelse av personuppgifter för en individ begränsad till att uppgifterna måste ha behandlats emot nationell lag som har bäring på de fundamentala principer som uttrycks i konvention 108. Endast i ett sådant fall kan individen begära rättelse.[189]

Storbritannien har så sent som 10 oktober 2018 signerat ett protokoll om ändring av konvention 108.[190] Protokollet innebär att konventionen närmar sig stadgan på flera sätt. Man exemplifierar med samtycke vad som är en legitim grund för behandling av personuppgifter,[191] samt inför tillsyn av oberoende tillsynsmyndighet.[192] Avslutningsvis justerar man rätten till rättelse på så sätt att personuppgifterna som utgångspunkt ska vara riktiga och att rättelse kan begäras i den mån uppgifter behandlas i strid med konventionens regler.[193] Det ska emellertid påpekas att det kommer att dröja innan ändringen träder ikraft med hänsyn till att ikraftträdandet är beroende av staternas ratifikation av protokollet. Inte ens hälften av parterna till konvention 108 har signerat detta ännu.[194]

Den skillnad som kvarstår mellan rättigheterna i den ändrade konvention 108 och stadgan är att rätten till rättelse i stadgan är ovillkorad.[195] Rätten till rättelse kan ställas i relation till vilken rättighet som blir utflödet av GDPR och dess hänvisning till stadgan. I skäl 65 till GDPR står att en individ *bör* ha rätt till rättelse om *lagring* sker i strid med GDPR, annan EU-rätt eller nationell rätt. I artikeln är emellertid inte rätten till rättelse begränsad till just lagring av uppgifter, eller till att denna ska ske

[187] Det vill säga inom ramen för EU respektive Europarådet med 47 medlemsstater, Europarådet, utan dag, https://www.coe.int/en/web/portal/47-members-states, använd den 15 december 2018.
[188] EKMR, artikel 8; konvention 108, artikel 5, 7 – 9.
[189] EKMR, artikel 8; konvention 108, artikel 5, 7 – 9.
[190] Europarådet, 2018 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/country/UK?p_auth=qaopIGxq, använd den 11 oktober 2018.
[191] Europarådet, 2018, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2018, artikel 7.2.
[192] Europarådet, 2018, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2018, artikel 19.
[193] Europarådet, 2018, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2018, artikel 7 och 11.2.
[194] Europarådet, 2018, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2018, artikel 37.1; Europarådet, 2018, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures?p_auth=9tiU0QIN, använd den 10 oktober 2018.
[195] Stadgan, artikel 8.2.

i strid med nämnd rätt.[196] Även i GDPR är alltså rätten till rättelse ovillkorad. Dock finns ett krav i GDPR på att uppgifterna ska vara riktiga, varför man i och för sig kan hävda att det strider mot förordningen att behandla oriktiga uppgifter och att sådan behandling är katalysator för rätten till rättelse.[197] Eftersom rättigheten i GDPR härstammar från stadgan och genom GDPR:s konstruktion bara blir aktuell när man bryter mot GDPR, så skulle man kunna hävda att rätten till rättelse i GDPR och stadgan inte är unik. Effekten av GDPR och stadgan blir densamma som den i ändringen av konvention 108. Dock vill jag ändå argumentera för att rättigheten är unik i det avseendet att dess ordalydelse är ovillkorlig i såväl stadgan som GDPR, vilket inte är fallet i ändringen av konvention 108.

Med utgångspunkt i de rättigheter som finns i de olika rättsakterna innebär min utredning att övriga akter saknar den *ovillkorliga* rätten till rättelse i förhållande till stadgan. Man kan emellertid argumentera för att effekten av rättigheten i den ändrade konvention 108 är densamma som den inom EU-rätten och att det därför inte finns någon skillnad. Samtidigt finns det dock utrymme för att hävda att den ovillkorliga rätten till rättelse har ett värde i sig, oaktat att dess utlösande effekt är att man bryter mot GDPR:s krav på att uppgifterna ska vara riktiga – så som rätten slås fast i stadgan är den ju ovillkorad. I den mån man utgår från det senare kan inte stadgans rättighet anses existera oberoende av densamma, som Storbritannien annars hänvisar till i Withdrawal Act 2018,[198] förutsatt att Storbritannien inte är bundet av någon ytterligare rättsakt som stipulerar motsvarande rättighet. Det går inte att utesluta att man med sin formulering i Withdrawal Act 2018 också hänvisar till något slags naturrättsligt resonemang,[199] eller något likt det som i unionsrätten benämns allmänna principer.[200] Till de allmänna principerna i EU hör till exempel de grundläggande rättigheterna i EKMR.[201] Som tredjeland är just dessa emellertid knappast något Storbritannien kan hänvisa till, när man inte längre är medlemsstat och bunden av EU-rätten.

En fråga i anslutning till detta är om man skulle kunna bygga en hållbar argumentation på att den ovillkorliga rätten till rättelse existerar oskriven som en del av folkrätten. Man kan hävda att så är fallet eftersom stadgan är ett dokument som sammanställer grundläggande rättigheter i skrift.[202] Här hamnar man emellertid lätt i ett cirkelresonemang, eftersom det i sådant fall är svårt att förstå varför Storbritannien så uttryckligt anger att man ska lämna stadgan och inte inkorporera denna i sin nationella rätt. Vad har det för betydelse att transformera stadgan nationellt om den ändå inte gör annat än sammanställer sådant som redan gäller? Eller också behövs ingen inkorporering av just samma skäl. Dock är det i sådant fall svårt att se varför Storbritannien ändå fortsättningsvis skulle låta vissa hänvisningar till denna vara kvar. Det blir som sagt ett cirkelresonemang och jag kan inte nå en annan lösning på detta än att den skrivning som Storbritannien har i sin Withdrawal Act 2018 kan vara problematisk att förena med GDPR:s hänvisning till stadgan. Det ska här tilläggas att det också blir svårt att hävda att rättigheterna som stadgan slår fast är sådana som gäller oberoende genom ett slags konsensus, när ändringen av konvention 108 inte inbegriper alla dessa.

196 GDPR, artikel 16.
197 GDPR, artikel 5.1 d.
198 Withdrawal Act 2018, sektion 5 (4 – 5).
199 Carlsson, Bo, *En rationell diskurs; "Tillbaka till Rousseau"*, Tidskrift för rättssociologi, 1985, sidorna 163 – 175.
200 FEU, artikel 6.3.
201 FEU, artikel 6.3.
202 Ingressen till stadgan.

Var man landar i frågan från ovanstående stycke kan vara avhängigt den syn man har på rätten.[203] Sluter man sig emellertid till att rättigheten inte existerar *alldeles oberoende* av stadgan eller något som bekräftar dess existens, eller att det i vart fall är svårt att argumentera juridisk utifrån perspektivet att den skulle vara helt oberoende, syns ett problem med Storbritanniens bibehållande av GDPR. När man transformerar GDPR till nationell rätt innebär det i sådant fall att en del av den grund man bygger sin nationella lag på inte är tillämplig i den kontext den ska verka. Det blir måhända något av ett metaresonemang, men en akt vars grund inte är tillämplig på den rättsordning akten ska fungera inom tycks i bästa fall vara byggd på ett ostadigt fundament. I värsta fall innebär det att hela rättsaktens tillämplighet faller. Som nämnts ovan är detta något som skulle kunna bli föremål för den ändring som kan göras i tidigare EU-rätt enligt Withdrawal Act 2018, även om sektion 5 i samma akt antyder att man inte tänkt sig just denna lösning för den här situationen. Enligt min analys är det emellertid, mot bakgrund av instabiliteten som annars kan genereras, något man onekligen bör göra eftersom man inte längre är bunden av stadgan som potentiellt erbjuder ett i viss mån unikt skydd. I den mån skrivningen i Withdrawal Act 2018 inte nödvändigtvis hänvisar till andra akter utan snarare till något slags allmän konsensus kan kanske bristerna i förhållande till stadgans eventuellt unika rättigheter anses läkta. Dock vill jag påpeka här att det kan bli svårt att argumentera för att det finns ett sådant övergripande samförstånd när ändringen av konvention 108 inte för konventionen närmare stadgan än den gör.

Storbritannien har sedan tidigare visat sig ha problem med stadgan i förhållande till sin nationella lagstiftning om lagring av personuppgifter hos telekomoperatörer. Enligt den så kallade Tele2-domen,[204] har EUD konstaterat att den brittiska lag[205] som stipulerar att inrikesministern kan begära att aktörer som levererar telekommunikationstjänster generellt och odifferentierat ska lagra personuppgifter inte överensstämmer med stadgan.[206] Storbritannien grundar denna befogenhet på artikel 15.1 direktiv 2002/58/EG,[207] vilken genom en uttömmande lista, stadgar att lagring av personuppgifter i en dylik situation undantagsvis kan vara tillåten att lagstadga om. Man har förändrat den nationella lagen på senare tid, och är i färd med att förändra den ytterligare med anledning av domen. I förhållande till de krav som listas i Tele2-domen, liksom i den artikel man hänvisar till i direktiv 2002/58/EG har man den senaste tiden i stort sett justerat allt för att följa stadgan.[208] Dock, enligt min bedömning finns fortfarande vissa problem i den senaste versionen av den brittiska lagen i förhållande till att listan rörande undantag i direktivet är uttömmande.[209] Det ska påpekas att denna lag inte finns till för att införliva GDPR i brittisk rätt.[210] Det finns heller inget uttalande från kommissionen som talar för att man kommer att ta hänsyn till detta när man fattar ett eventuellt adekvansbeslut gentemot Storbritannien. Det finns emellertid potentiellt ändå

[203] Jämför till exempel naturrätten med rättspositivismen, Carlsson, 1985, sidorna 163 – 175; Stenhammar, Fredrik, *Hård rättspositivism i folkrätten*, Svensk juristtidning, 2008, sidorna 4 – 5.
[204] Domstolens dom (stora avdelningen) av den 21 december 2016, C-203/15 och C-698/15, EUT C 53, 20.2.2017, s. 11–12 (Tele2-målet), 2016. Det första av de två förenade målen rörde svenska Post- och Telestyrelsen mot Tele2.
[205] Regulation of Investigatory Powers Act 2000 (RIPA), 2018.
[206] Tele2-målet rörande stadgan, artikel 7, 8, 11 och 52.1.
[207] 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) (EGT L 201, 31.7.2002, s. 37–47).
[208] Jämför den brittiska lagen Investigatory Powers Act 2016 (IPA), sektion 87 – 89; RIPA, sektion 22; Tele2-målet; direktiv 2002/58/EG, artikel 15.1.
[209] Jämför RIPA, sektion 22.2 (h); direktiv 2002/58/EG, artikel 15.1; Tele2-domen stycke 90.
[210] Istället rör det sig om ett utnyttjande av den möjlighet till undantag för skydd av fysiska personer rättigheter gällande deras personuppgifter som ges enligt direktiv 2002/58/EG, artikel 15.1.

anledning att anpassa även förevarande lag efter stadgans principer med hänsyn till en framtida adekvansbedömning.

Först och främst ska konstateras att inom ramen för tillämpningsområdet för den lag genom vilken Storbritannien genomför direktiv 2002/58/EG kommer operatörerna över personuppgifter från unionen, till exempel genom telefonnummer.[211] Bara på den grunden skulle anledning kunna finnas att överväga att rätta sig efter stadgan och Tele2-domen även efter brexit. Som nämnts ovan är dessutom två av parametrarna kommissionen ska ta särskild hänsyn till i fattandet av ett adekvansbeslut tredjelandets inhemska lagstiftning och dess hänsyn till mänskliga rättigheter.[212] Man är således inte begränsad till GDPR:s område. Vad gäller GDPR och dess relation till direktiv 2002/58/EG, ska tillämpningsområdet för de båda vara skilda från varandra, men det föreligger i nuläget inte någon skarp gräns dem emellan.[213] Områdena går alltså in i varandra i viss mån än så länge, även om man i GDPR uttrycker att direktivet behöver ses över.[214] I GDPR stadgas förvisso att densamma inte ska betyda någon ytterligare skyldighet för de som behandlar personuppgifter inom ramen för direktiv 2002/58/EG.[215] Denna bestämmelse tar emellertid sikte på att inte ytterligare betunga aktörerna inom de områden som redan är reglerade genom direktivet och således inte på hur medlemsstaterna får reglera lagring enligt artikel 15.1 direktivet.

Enligt det ovan nämnda Schrems-målet underkände EUD ett adekvansbeslut på den grunden att de amerikanska reglerna inte följde stadgan. Stadgan är alltså i allra högsta grad aktuell för ett adekvansbeslut, men frågan är om lagring av personuppgifter hos telekomoperatörer skulle falla inom detta område. Det går inte att avgöra hur kommissionen kommer att se på detta, men det ska nämnas att alla adekvansbeslut som tidigare fattats håller på att ses över i nuläget.[216] Det vill säga *efter* att såväl Schrems-målet som Tele2-målet prövats, liksom efter GDPR:s ikraftträdande. Vidare finns en antydan i det adekvansbeslut där man senast påbörjat antagningsförfarandet, i relationen till Japan, om att även den sektor som omfattas av direktiv 2002/58/EG och de personuppgifter som behandlas där omfattas av beslutet.[217] Således skulle även detta eventuellt bedömas mot stadgan. Vill man vara säker på att nå upp till den skyddsnivå ett adekvansbeslut kräver kan det således vara av värde att se till att den reglering man har som berör personuppgifter generellt uppfyller skyddet i stadgan.

3.1.2 Storbritanniens internationella åtaganden

En del har redan nämnts om Storbritanniens internationella åtaganden, några fler kommentarer är emellertid på sin plats. Storbritannien är som sagt part dels i EKMR, dels i konvention 108.[218] Man

---

[211] Vodafone, 2018, https://www.vodafone.co.uk/privacy, använd den 5 november 2018.
[212] GDPR, artikel 45.2.
[213] GDPR, skäl 173.
[214] GDPR, skäl 173.
[215] GDPR, artikel 95.
[216] Stupp, Catherine, Euractiv, *Commission conducting review of all foreign data transfer deals*, den 9 november 2017, https://www.euractiv.com/section/data-protection/news/commission-conducting-review-of-all-foreign-data-transfer-deals/, använd den 6 november 2018.
[217] Europeiska kommissionen, Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan, 2018, sidorna 8 – 9, https://ec.europa.eu/info/sites/info/files/draft_adequacy_decision.pdf, använd den 22 november 2018.
[218] Europarådet, 2018, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/country/UK?p_auth=qaopIGxq, använd den 11 oktober 2018.

har dessutom signerat ett tillägg till konvention 108, vilket syftar till att modernisera den senare.[219] Det ska emellertid tilläggas att en signatur inte är bindande för en stat, om än en indikation i riktning mot en ratifikation och således också bundenhet.[220] De reservationer som Storbritannien gjort i förhållande till EKMR rör inte rätten till privatliv i artikel 8.1. Således är rätten till skydd för privatliv fredad i detta avseende.[221] Gällande konvention 108 har Storbritannien ett flertal deklarationer, dock är ingen sådan att man inskränker skyddet enligt konventionen i förhållande till skyddet för personuppgifter.[222] Situationen gällande de internationella åtagandena är därför liknande den som gäller i de länder som omfattas av de tidigare adekvansbeslut som nämnts.[223]

Här ska erinras om att EU, till skillnad från Storbritannien, inte är part till EKMR.[224] Medlemsstaterna är dock parter och konventionen finns som del av EU-rätten på principiell nivå.[225] EU har vidare uttryckt att man ska ansluta sig till den.[226] EKMR är emellertid varken signerad eller ratificerad av EU – man har inte slutfört anslutningsprocessen.[227] Som kunnat konstateras ovan är stadgans rättigheter mycket mer långtgående för personuppgiftsskydd än EKMR:s och i viss mån unika även i förhållande till konvention 108.[228] I konsekvens med detta är det i ljuset av de rättigheter som stadgan stipulerar en bedömning av skyddsnivån ska göras, inte i förhållande till EKMR och konvention 108.[229] Detta blir än tydligare i och med att EUD förklarade adekvansbeslutet för USA ogiltigt på grund av dess oförenlighet med stadgan.[230] USA är förvisso inte part till EKMR, men av resonemanget i Tele2-målet att döma,[231] liksom det faktum att skyddet i stadgan, EKMR och konvention 108 skiljer sig åt,[232] bör slutsatsen kunna översättas till denna situation. Utifrån detta resonemang blir slutsatsen att, oberoende av de problem Storbritannien potentiellt har med stadgan i förhållande till ett adekvansbeslut, är det stadgans skyddsnivå som ska uppnås inom området för personuppgifter generellt. Det ligger i linje med vad som sagts om att det är ett likvärdigt, men inte nödvändigtvis likalydande skydd som det inom EU som ska finnas för att ett adekvansbeslut ska meddelas. I kombination med stadgans eventuellt unika skydd blir resultatet som *utgångspunkt* att Storbritannien inte skulle kunna uppnå en adekvat skyddsnivå genom

---

[219] Europarådet, 2018 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/country/UK?p_auth=qaopIGxq, använd den 11 oktober 2018.
[220] No. 18232 Vienna Convention on the law of treaties (with annex). Concluded at Vienna on 23 May 1969 (Wienkonventionen), 1969, artikel 1.b och artikel 18.
[221] Europarådet, 2018, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures?p_auth=DdNsMbLo, använd den 11 oktober 2018.
[222] Europarådet, 2018, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/declarations?p_auth=DdNsMbLo, använd den 11 oktober 2018.
[223] Bland andra adekvansbeslut för Guernsey och adekvansbeslut för Jersey.
[224] Europarådet, 2018, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures?p_auth=Q4OaIJ6M, använd den 12 december 2018.
[225] FEU, 6.3.
[226] Europaparlamentet, 2010, http://www.europarl.europa.eu/sides/getDoc.do?language=SV&type=IM-PRESS&reference=20100507STO74260, använd den 12 december 2018.
[227] Europarådet, 2018, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures?p_auth=Q4OaIJ6M, använd den 12 december 2018.
[228] Jämför EKMR, artikel 8; stadgan artikel 7 – 8; samt konvention 108, artikel 5, 7 – 9.
[229] Jämför slutsatserna i Tele2-målet och Schrems-målet.
[230] Schrems-målet, framförallt stycke 98.
[231] Framförallt styckena 127 – 128 i domen.
[232] Jämför EKMR, artikel 8; stadgan artikel 7 – 8; samt konvention 108, artikel 5, 7 – 9.

att *enbart* följa EKMR och konvention 108. Det ska dessutom lyftas att det uttryckligen slås fast i stadgan att denna kan ha mer långtgående rättigheter än EKMR.[233]

En dom från Europadomstolen från september 2018 i det så kallade Big Brother-målet[234] nyanserar emellertid potentiellt denna bild något. Inom ramen för målet behandlade man samma lagstiftning som prövades i Tele2-målet. Här konstaterade man att den reglering Storbritannien tillämpat var i strid med den som skulle genomföras enligt EU-rätten, således stred också detta mot laglighetskravet i artikel 8.2 EKMR. Resonemanget från domstolen går ut på att Storbritannien inte genomförde direktivet korrekt genom att säkerställa vissa skyddsåtgärder till förmån för individen i relation till myndigheters tillgång till personuppgifter. Genom detta bröt Storbritannien mot sin nationella rätt så som den skulle genomföras i ljuset av EU-rätten, således fanns där också ett brott mot artikel 8.2 EKMR som stadgar att myndigheters inskränkning av skyddet för personuppgifter måste vara lagstadgad.[235]

Med avstamp i Big Brother-målet kan konstateras att Europadomstolen betraktar artikel 8 EKMR som bruten mot genom att EU-rätten inte följts av en EU-medlemsstat. På den grunden kan man därför hävda att artikel 8 EKMR således omfattar även det skydd som slås fast i stadgan. Det är dock tveksamt om den teknik domstolen använder skulle fungera på samma sätt när Storbritannien inte längre är medlemsstat i EU. Som tredjeland behöver man inte följa EU-rätten och det sätt på vilket myndigheters tillgång till telekomoperatörers uppgifter regleras är endast avhängigt nationell rätt. Därför skulle det bli svårt att argumentera för ett brott mot lagkravet i artikel 8.2 EKMR när man följer sin nationella rätt, om än inte EU-rätten.

Genom Big Brother-målet nyanseras bilden något. Lagkravet i EKMR öppnar för att EKMR kan omfatta andra rättigheter som finns i stadgan och således skulle bristen på den ovillkorliga rätten till rättelse utanför EU-rätten eventuellt kunna läkas. Det är dock svårt att se hur detta skulle gå till när Storbritannien efter brexit blivit ett tredjeland som inte är bundet av EU-rätten. I förhållande till Storbritanniens eventuella problem med stadgan innebär således inte Big Brother-målet någon garanti och den utgångspunkt som konstaterats ovan står fast. Man kan inte vara helt säker på att följa stadgans standard genom att endast stödja sig på konvention 108 och EKMR, även om domen i Big Brother-målet genom lagkravet förvisso utgör ett slags garanti i förhållande till EU:s medlemsstater.

3.1.3 Storbritanniens tillsynsmyndighet och dess samarbete med EU:s medlemsstaters motsvarigheter

Så långt om Storbritanniens nationella lagstiftning och internationella åtaganden. Nästa parameter för kommissionen att utreda rör oberoende tillsynsmyndighet. I Storbritannien utgörs denna av ”The Information Commissioner”(ICO), som man i den brittiska lagen hänvisar till är för att

[233] Stadgan, artikel 52.3. Jämför också med resonemanget i Kommerskollegium, *Efter brexit – en analys av svenska intressen inför kommande förhandlingar*, 2018, sidan 153, där man kommer till en något annorlunda slutsats.
[234] Big Brother Watch and Others v. the United Kingdom (applications nos. 58170/13, 62322/14 and 24960/15), dom meddelad den 13 september 2018.
[235] Se pressrelease rörande Big Brother-målet, The Register of the Court, Some aspects of UK surveillance violate Convention, 2018.

uppfylla syftet enligt GDPR.[236] Det är dock ett organ som kan dateras ända tillbaka till 1984,[237] varför tillsynsmyndigheten knappast kan anses finnas enkom för att uppfylla syftet enligt GDPR och därmed heller inte bör förlora sin roll nationellt i och med brexit. Här, liksom ovan, finns emellertid problemet att man kommer att behöva grunda och säkra ICO:s befogenhet på något annat än en direkt hänvisning till GDPR när man träder ur EU. Man måste transformera befogenheterna till nationell rätt. För kommissionen gäller bedömningen tillsynsmyndighetens verkliga befogenheter i förhållande till hur man agerat i fall av missbruk av personuppgifter. Angående denna fråga ska nämnas att det finns många exempel på hur ICO dömt ut ekonomiska påföljder för företag som inte följt reglerna.[238] Mot bakgrund av detta förefaller ICO vara organiserad på ett sådant sätt att man faktiskt har makt att agera för att genomdriva de principer som skyddet för personuppgifter grundar sig på. Ur detta perspektiv är det således i linje med vad som kan krävas för att få ett beslut om adekvat skyddsnivå.

En ytterligare parameter för kommissionen att ta hänsyn till är samarbetet mellan tredjelandets tillsynsmyndighet och de motsvarade myndigheterna i EU:s medlemsstater. Enligt Storbritanniens ståndpunkt inför utträdet har man deklarerat att man vill att ICO ska behålla vissa delar av sina befogenheter inom ramen för EU-samarbetet, man vill vara kvar i OSS.[239] Jag kommer att få anledning att återkomma till detta i kommande avsnitt.[240] Här ska bara kort nämnas att man, utifrån vad som står i GDPR och vad som finns att tillgå angående EU:s position i frågan, kommer att behöva söka samarbeta på annat sätt, sedan man inte längre är medlemsstat.[241] Mot bakgrund av att man förlorar möjligheten att utnyttja de samarbetsmekanismer som ställs upp i kapitel VII GDPR tappar man potentiellt infrastrukturen för samarbetet med andra tillsynsmyndigheter.[242] Dock har man förmodligen ändå möjlighet till goda relationer till medlemsstaternas tillsynsmyndigheter i egenskap av tidigare medlemsstat. På så sätt behöver man inte upprätta ett helt nytt förhållande till dessa, utan kan bygga på det som redan finns, om än utanför ramen för EU-samarbetet.

3.1.4 Effektiva rättsmedel i Storbritannien

Den sista identifierade parametern för kommissionen att bedöma för ett eventuellt adekvansbeslut är effektiva rättsmedel. Det vill säga att få sin sak prövad i domstol i Storbritannien för det fall man anser att ens personuppgifter blivit missbrukade. I DPA erkänns dessa möjligheter till prövning för individen i sektion 165 – 169. Sektionerna hänvisar upprepade gånger till GDPR, denna del är således behäftad med samma problem som generellt gäller för den nationella tillämpningen. För att kunna uppfylla de principer som EU-rätten ställer upp för effektiva rättsmedel krävs därför att man transformerar GDPR:s garantier för prövning till nationell rätt.

---

[236] DPA, sektion 115.
[237] Information Commissioner's Office, 2018, https://ico.org.uk/about-the-ico/our-information/history-of-the-ico/, använd den 11 oktober 2018.
[238] Information Commissioner's Office, 2018, https://ico.org.uk/action-weve-taken/enforcement/, använd den 12 oktober 2018; se till exempel angående böter mot Boost Finance Limited, https://ico.org.uk/action-weve-taken/enforcement/boost-finance-limited/, använd den 12 oktober 2018; Oaklands Assist UK Limited, https://ico.org.uk/action-weve-taken/enforcement/oaklands-assist-uk-limited/, använd den 12 oktober 2018.
[239] Vitboken, sidorna 75 – 76.
[240] Avsnitt 4.2.2.
[241] GDPR, kapitel VII; Utträdesavtalet av den 14 november 2018, artikel 70 a; Barnier, Michel, Speech by Michel Barnier at the 28th Congress of the International Federation for European Law, 26 maj 2018.
[242] Se mekanismen för enhetlighet, GDPR, artikel 63 – 67.

Till detta kommer att man förlorar möjligheten till förhandsavgörande av EUD. En begäran om förhandsavgörande kan endast göras av medlemsstat,[243] något Storbritannien också lyfter fram i sin Withdrawal Act 2018.[244] Det blir emellertid en logisk slutsats av att adekvansbeslut meddelas till tredjeländer att möjlighet till prövning av EUD inte är nödvändig för att anses ha effektiva rättsmedel. Dock, eftersom man vill behålla GDPR, om än som en inhemsk version, är det en möjlighet till tolkning av den rätt man baserat sin lagstiftning på som går förlorad. Detta innebär att man är begränsad till tolkning inom den nationella ordningen. Potentiellt kan det innebära att man rör sig bort från den tolkning som är avsikten med EU-rätten och därmed också förlorar det som adekvansbeslutet från början byggde på. Faktum är att brittiska domstolar redan, sedan folkomröstningen gällande brexit 2016, börjat begära färre förhandsavgöranden från EUD.[245] Kanske är det en naturlig reaktion eftersom EUD:s avgöranden snart inte kommer att vara bindande för Storbritannien.[246] Det ger emellertid en fingervisning om att man redan börjar avvika från den tolkning som görs av EU:s rättsakter av EU självt. Storbritannien har dessutom uttryckt att man kanske rent av vill röra sig bort från EU:s standarder.[247] Här vill jag nämna att det naturligtvis inte är nödvändigt att kunna få sin nationella rätt bedömd av EUD för att få ett adekvansbeslut – tvärtom är det till tredjeländer adekvansbesluten meddelas. Vad jag menar är emellertid att man, i och med att man vill behålla *samma* akt som EU, löper en större risk att frångå den tolkning som avses i EU-rätten, och därmed också äventyra adekvansbeslutet.

På sikt skulle det kunna betyda att man skapar ett avstånd mellan de principer som stadgas i EU-rätten och den nationella lagstiftningen. På så sätt skulle man också eventuellt tappa det som adekvansbeslutet grundar sig på som utgångspunkt. I den mån de principer som adekvansbeslutet grundar sig på går om intet genom de tolkningar man gör nationellt, kan kommissionen återkalla beslutet.[248] Denna återkallningsmöjlighet finns som en inneboende osäkerhet i adekvansbeslutets konstruktion, för såväl aktörer som medlemsstater och tredjeland.

3.2 Slutsatser och funktionen för betaltjänsten och företaget av adekvansbeslutet

Sammanfattningsvis kan följande sägas. De parametrar som kommissionen tittat på i tidigare adekvansbeslut har främst varit tredjelandets nationella lagstiftning, internationella åtaganden, oberoende tillsynsmyndighet och effektiva rättsmedel. Via dessa har man bedömt uppfyllelsen av bland annat mänskliga rättigheter och rättsstatsprinciper, det vill säga de principer som stadgas enligt EU-rätten. Skyddet i tredjelandet måste inte vara identiskt, men det ska vara likvärdigt med det som råder i unionen. En jämförelse mellan de nuvarande reglerna och de tidigare besluten vittnar om att man rimligen bör titta på samma parametrar efter införandet av GDPR.

---

[243] FEUF, artikel 267.
[244] Withdrawal Act 2018, sektion 6 (1).
[245] Dyevre, Arthur, *Have British judges already left the EU? The impact of the Brexit vote on EU law in the UK*, 2018, http://blogs.lse.ac.uk/europpblog/2018/11/13/have-british-judges-already-left-the-eu-the-impact-of-the-brexit-vote-on-eu-law-in-the-uk/, använd den 27 november 2018.
[246] Dyevre, 2018; Withdrawal Act 2018, sektion 6 (1).
[247] Hill, Rebecca, *Data flows post-Brexit: 'Leave it to government to make sure you've got a smooth run in.' Er, OK*, The Register, den 8 november 2018, https://www.theregister.co.uk/2018/11/08/dominic_raab_data_protection/, använd den 12 november 2018. Det ska dock tilläggas att uttalandet kom från Dominic Raab, som avgått som brexitminister i Theresa Mays regering.
[248] GDPR, artikel 45.5.

För Storbritannien innebär detta att man i och för sig har många delar på plats, som därmed talar för att man ska kunna få ett beslut om adekvat skyddsnivå från kommissionen. Man har en oberoende tillsynsmyndighet med befogenheter att vidta åtgärder, denna har dessutom etablerade relationer till andra medlemsstaters motsvarande myndigheter, även om man inte får vara kvar i OSS som tredjeland. Det finns effektiva rättsmedel i så måtto att individen har möjlighet att få sin sak prövad. Man har ett nationellt regelverk som är baserat på EU-rätten, vilket man ser från tidigare adekvansbeslut är en fördel. Till sist har man relevanta internationella åtaganden. Till detta kan adderas att EU uttryckt att det är ett adekvansbeslut vi rör oss mot, eller i vart fall en prövning av om Storbritanniens skyddsnivå är adekvat.[249] Så långt ser det positivt ut för Storbritannien angående att kunna få ett beslut om adekvat skyddsnivå.

Det finns emellertid flera parametrar som pekar i motsatt riktning. Det är ett lagtekniskt problem i sammanhanget för Storbritannien att man byggt sin reglering på direkta hänvisningar till GDPR. Den nationella regleringen måste justeras textmässigt för att man ska kunna tala om en reglering som når upp till samma skydd som det i unionen. Någon sådan ändring har inte gjorts ännu, även om man tala om ett genomförande nationellt av GDPR via Withdrawal Act 2018. Enligt vad jag kommit fram till i detta avsnitt kan man dock inte nöja sig med att DPA är baserad på GDPR så som den ser ut nu.[250] En liknande problematik uppstår med stadgan och dess potentiellt unika skydd i förhållande till andra rättsakter som slår vakt om mänskliga rättigheter. Det är, utifrån vad Storbritannien uttrycker i sin Withdrawal Act 2018, osäkert om man kan inkorporera GDPR på nationell nivå utan att göra en justering även gällande förordningens hänvisning till stadgan, något man egentligen inte verkar ha för avsikt att göra att döma av Withdrawal Act 2018. Det gäller emellertid under förutsättning att rättigheterna inte kan anses finnas oskrivna i det brittiska rättssystemet, naturrättsligt eller anses motsvara EU-rättens skydd baserat på den *effekt* som nås i EU-rätten. Den naturrättsliga bedömningen är något som enligt min redogörelse ovan kan vara svår att sluta sig till. Mot bakgrund av detta och utfallet av Big Brother-målet är det heller inte garanterat att Storbritannien uppfyller stadgans nivå av skydd genom att vara part till EKMR och konvention 108. Man ska också komma ihåg att Storbritannien potentiellt fortfarande har problem med sin efterlevnad av stadgan, utifrån den lydelse i RIPA som finns kvar trots Tele2-domen, även om det förvisso inte är helt klart om det område denna behandlar kommer att vara av betydelse för ett adekvansbeslut.

Den infrastruktur som finns för myndighetssamarbete mellan medlemsstaterna raseras för Storbritannien när man utträder. Man står därför, om än med befintliga kontakter, inför att skapa nya kanaler för samarbete. Sist men inte minst finns så problematiken med effektiva rättsmedel. Eftersom Storbritannien vill behålla GDPR som en nationell variant är det ett problem att man inte längre kommer att stå under EU-domstolens jurisdiktion. Man rör sig genom sin prövning i nationella domstolar potentiellt bort från den tolkning som var avsedd för EU-rättsakten och därigenom också kanske bort från den adekvata skyddsnivån. En tendens man redan ser är att Storbritanniens domstolar är mindre benägna att be om förhandsavgörande nu, än före folkomröstningen. Mot bakgrund av denna sammanställning finns det viss osäkerhet kring

[249] Politiska deklarationen, sidan 4; General Secretariat of the Council, European Council (Art. 50) (23 March 2018) – Guidelines, 2018, sidan 6.
[250] Jämför vitboken, sidorna 74 – 75.

huruvida ett adekvansbeslut kommer att kunna fattas i relation till Storbritannien. Detta trots att EU i princip utfäst sig att inleda en prövning i den politiska deklarationen.

Slutsatsvis kan sägas att det inte går att avgöra mer än att det är osäkert huruvida Storbritannien uppfyller en adekvat skyddsnivå. Oaktat vad som talar för och emot detta skulle ett adekvansbeslut, *om det väl finns på plats*, innebära att betaltjänsten kan överföra personuppgifterna till företaget i Storbritannien utan hinder. Det vill säga lika fritt som om det inte vore ett tredjeland, eftersom inga hinder i sådant fall skulle finnas för betaltjänstens flöde över gränsen mellan Storbritannien och EU.[251] Överföringen till tredjeland skulle således kunna ske utan något särskilt förfarande från betaltjänstens sida. På så sätt är ett adekvansbeslut en förhållandevis friktionsfri lösning för de aktörer som vill fortsätta att överföra personuppgifter till Storbritannien efter brexit. Här ska dock påminnas om att adekvansbeslutsprocessen kan vara något som tar tid, även om EU har sagt att man ska anstränga sig för att det inte ska uppstå en period där vi inte har någon reglering av personuppgiftsflödena på plats. Denna eventuellt segdragna process är något som tar oerhört lång tid i jämförelse med hur snabbt personuppgifter kan flöda från betaltjänsten till företaget. Som exempel kan adekvansbeslutet i förhållande till Japan nämnas. Kommissionen inledde diskussioner med Japan om ett eventuellt adekvansbeslut i januari 2017. Först i september 2018 lanserade man utkastet till beslut, som sedan ska genomgå granskning av olika parter.[252]

Till detta hör, vilket i och för sig är något positivt i förhållande till skyddet för fysiska personer, att kommissionen ska utvärdera utvecklingen av skyddet för personuppgifter i tredjeländer löpande, minst vart fjärde år.[253] Problematiskt för Storbritannien i detta hänseende och hotet mot ett eventuellt adekvansbeslut, liksom flödet för betaltjänsten till företaget, är tolkningen av den rättsakt man antar. Som nämnts ligger ett problem i att Storbritannien potentiellt skulle röra sig bort från den tolkning av GDPR, inbegripet stadgan, som EU-rätten avsett. Inom ramen för kommissionens utvärdering bör sådana tendenser knappast kunna flyga under radarn. Om kommissionen i ett sådant fall ser att den adekvata skyddsnivån gått förlorad kan beslutet återkallas, upphävas eller ändras.[254] Således innebär det en ständig underliggande osäkerhet för betaltjänsten om och hur länge man kommer att kunna skicka användarnas namn, mejladress, telefonnummer et cetera till företaget i Storbritannien. Finns inget adekvansbeslut strider betaltjänstens överföring till företaget istället mot förbudet i artikel 44 GDPR, under förutsättning att man inte tillämpar något av de andra undantagen. Adekvansbeslutet är emellertid en smidig lösning när det är på plats och fungerar och det krävs ingenting av betaltjänsten och företaget för att beslutet ska fattas.

Avslutningsvis kan följande sägas utifrån adekvansbesluten, betaltjänsten och företaget. Det är på intet sätt säkert att Storbritannien når upp till de krav som ställs på personuppgiftsskydd enligt EU-rätten. Detta kombinerat med den långa process som kan föregå adekvansbeslutet, trots EU:s ansträngningar att få det klart före slutet av 2020, inte minst med hänsyn till det arbete Storbritannien måste göra nationellt, innebär att ett dylikt beslut skulle kunna dröja. Utifrån detta

[251] Europeiska kommissionen, 2018, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en, använd den 27 november 2018.
[252] Europeiska kommissionen, 2018, http://europa.eu/rapid/press-release_IP-18-5433_en.htm, använd den 13 december 2018.
[253] GDPR, artikel 45.3 – 4.
[254] GDPR, artikel 45.5.

är det högst troligt att betaltjänsten skulle behöva överföra personuppgifter till företaget i Storbritannien redan innan ett beslut finns på plats. Även om ett beslut om adekvat skyddsnivå i Storbritannien skulle innebära att betaltjänstens överföring till företaget skulle ske som om det fortfarande befann sig i unionen, innehåller lösningen ändå osäkerhetsmoment. Tillsynen från kommissionen liksom att Storbritannien potentiellt skulle röra sig bort från EU-rättens principer innebär att risken finns att beslutet justeras eller undanröjs. Det är något som vore problematiskt för betaltjänsten som då inte skulle kunna föra över personuppgifter till företaget utan att bryta mot förbudet i artikel 44 GDPR, innan man själv lyckats lösa överföringen på andra sätt. Dessa andra sätt kommer jag att få anledning att återkomma till i kommande kapitel.[255]

4 Hur skulle överföringen av betaltjänstens insamlade personuppgifter från EU till Storbritannien se ut enligt Storbritanniens vitbok och är denna lösning ett reellt alternativ?

I juli 2018 publicerade Storbritannien en så kallad vitbok där man deklarerar sin ståndpunkt gällande den framtida relationen med EU. Dokumentet togs emot med skepsis från EU, även om man också uttryckte att detta kunde tjäna som grund för det fortsatta förhandlingsarbetet.[256] Generellt kan sägas att tonen i vitboken vad gäller just dataflöden, är satt efter att Storbritannien anser sig ha en hög skyddsnivå.[257] Genom detta och genom att använda sig av kommissionens egna uttalanden om dataflöden till tredjeländer argumenterar man för en lösning som tar avstamp i reglerna om adekvansbeslut, men som går längre.[258] Med utgångspunkt i GDPR finns utöver detta flera intressanta parametrar som uttrycks i Storbritanniens dokument. I de följande avsnitten kommer jag att försöka bringa klarhet i hur Storbritannien föreslår att regleringen av persondataflöden bör se ut. Det vill säga vad de egentligen menar med sin inställning till ett adekvansbeslut, den tvistlösningsmekanism man föreslår, liksom vad det är för avtal som avses. Sedan ska jag, liksom ovan, sätta det i en kontext där betaltjänstens överföring till företaget i Storbritannien står i fokus.

4.1 Den nationella regleringen och inställningen till ett adekvansbeslut

Utgångspunkten för Storbritannien, i det avsnitt i vitboken som behandlar persondataöverföring från EU till Storbritannien är att man har en hög skyddsnivå i och med sin nationella lagstiftning och att man därför är redo att inleda diskussioner för att kommissionen ska fatta ett adekvansbeslut.[259] Kommissionen har dock meddelat att man inte kan inleda några sådana diskussioner innan Storbritannien de facto blivit ett tredjeland.[260] Som diskuterats i avsnitt 3.1.1 finns dock en problematik kring Storbritanniens nationella lagstiftning, dess grund i EU-rätten och frågetecken kring om man skulle uppfylla en adekvat skyddsnivå.

---

[255] Kapitel 6.
[256] Herszenhorn, David M. och de La Baume, Maïa, *Barnier dismantles UK's Brexit white paper*, Politico, den 26 juli 2018, https://www.politico.eu/article/michel-barnier-brexit-white-paper-analysis/, använd den 30 november 2018.
[257] Vitboken, till exempel sidan 74.
[258] Vitboken, till exempel sidan 74.
[259] Vitboken, sidan 75.
[260] Department for Digital, Culture, Media & Sport, 2018.

Oaktat detta argumenterar Storbritannien för att man ska omfattas av ett adekvansbeslut eftersom man genom den nationella varianten av GDPR säkerställer en likvärdig skyddsnivå med den i EU.[261] Frågan är emellertid om man faktiskt förstått vilken karaktär ett adekvansbeslut har.[262] Kommissionen bestämmer ensidigt om ett sådant beslut ska fattas, liksom om ett förfarande i riktning mot ett dylikt beslut över huvud taget ska påbörjas.[263] I vitboken talas emellertid om adekvansbeslutet som en utgångsposition, utifrån vilken man sedan ska kunna komma *överens* om en mer långtgående lösning.[264] Storbritannien vill alltså ha ett avtal med EU på området för persondataskydd, men man vill också, vad det verkar, ha ett adekvansbeslut.[265] Det kan emellertid ifrågasättas om ett adekvansbeslut är möjligt i den mån man också vill ha en överenskommelse för samma område, eller om det senare tar ut det förra. I den mån man skulle vilja ha ett adekvansbeslut som en del av avtalet innebär adekvansbeslutets unilaterala natur att en del av avtalet i sådant fall inte skulle vara ömsesidig. Jag har svårt att se att detta är vad Storbritannien skulle vilja ha ut av avtalet, kanske är det således inte så att man egentligen vill ha ett *renodlat* adekvansbeslut som grund att bygga ett avtal på, som man anger i vitboken.[266]

Inställningen till adekvansbeslutet från Storbritanniens sida, trots de frågor som väcks kring huruvida ett avtal och ett beslut över huvud taget är möjliga att förena, får ändå anses som positiv. Man tycks inte se några problem med sin nationella lagstiftning. Istället ser man snarare en fördel i att den tillkommit i anslutning till GDPR. Jag drar slutsatsen att det har att göra med hur tidigare adekvansbeslut för de länder som ligger under den brittiska kronan sett ut – den nationella rättens grund i EU-rätten tyder på att EU-rättens principer gäller nationellt.[267] Storbritannien förefaller alltså ändå ha en positiv syn på adekvansbeslutet, och vill ha detta som grund för sitt avtal. Därför drar jag slutsatsen att tanken enligt vitboken är att personuppgiftsflödena i och för sig skulle fungera som vid ett adekvansbeslut även enligt Storbritanniens modell. Därför bör också betaltjänsten behöva följa GDPR i övrigt enligt artikel 44 GDPR, fastän Storbritannien tycks söka gå längre än ett adekvansbeslut från EU. Frågan är emellertid vad det faktiskt är för överenskommelse man vill träffa med EU och om det ens är genomförbart.

4.2 Storbritanniens avtal för flöde av persondata – vad avses med dess två delar?

Storbritannien vill ta lösningen för flödet av persondata längre än vad adekvansbeslutet tillåter. Utöver ett adekvansbeslut uttrycker man att man vill ha ett avtal, dels avseende ett ramverk för att främja stabilitet och insyn i systemet för dataskydd, dels gällande samarbete mellan den nationella tillsynsmyndigheten och EU:s motsvarande myndigheter.[268] Det finns flera intressanta parametrar gällande den argumentation Storbritannien använder för att motivera sin ståndpunkt. Framförallt det faktum att man genom kommissionens egna uttalanden verkar vilja stadga en ny ordning som GDPR egentligen inte medger.

---

[261] Vitboken, sidorna 74 – 75.
[262] Kommerskollegium, *Storbritanniens vitbok om den framtida relationen med EU, en analys av förslagen*, 2018, sidorna 22 – 23.
[263] Kommerskollegium, *Storbritanniens vitbok om den framtida relationen med EU, en analys av förslagen*, 2018, sidorna 22 – 23; Kommerskollegium, *Efter brexit – en analys av svenska intressen inför kommande förhandlingar*, 2018, sidan 148.
[264] Vitboken, sidorna 73 – 75.
[265] Vitboken, till exempel sidan 74.
[266] Vitboken, sidan 75.
[267] Bland andra adekvansbeslut för Guernsey och adekvansbeslut för Jersey.
[268] Vitboken, till exempel sidan 74.

De möjligheter GDPR tillåter för överföring av persondata till tredjeländer är de som återfinns i artiklarna 45 – 49 GDPR. Man kan därför säga att GDPR är ett solitt regelverk i den bemärkelsen. De sätt på vilka personuppgifter får överföras är de i kapitel fem, det skulle alltså röra sig om en uttömmande uppräkning.[269] Här kan man ställa sig frågan varifrån Storbritannien över huvud taget fått idén att en *överenskommelse* med EU vad gäller persondataflöden skulle vara möjlig. Mot bakgrund av GDPR är det helt och hållet en fråga som avgörs på unionens villkor och hänsyn tas inte till vad en potentiell motpart skulle ha för intressen. Man kan förvisso säga att bestämmelserna, bortsett från artikel 45 GDPR, inbegriper överenskommelser med motparten.[270] Dock innebär inte dessa artiklar att man på ett övergripande plan får en överenskommelse med *unionen*. Istället handlar det om avtal på basis av bedömningar av och mellan aktörer på varsin sida EU:s yttre gräns.[271] Den överenskommelse Storbritannien talar om med unionen som motpart verkar alltså inte rymmas inom ramen för GDPR:s undantag från förbudet att föra över personuppgifter till tredjeland.

Den ordning man från Storbritanniens sida skulle vilja införa är emellertid inte helt lösryckt – det är inte något man kommit på helt självständigt utan har grund i EU-rätten. Först och främst stadgar fördragen möjlighet för unionen att ingå avtal med tredjeland. Artikel 217 FEUF ger EU befogenhet att ingå avtal om:

> ”en associering med ömsesidiga rättigheter och förpliktelser, gemensamt uppträdande och särskilda förfaranden”

Här ska emellertid erinras om att ett dylikt avtal inte nödvändigtvis är beständigt bara för att parterna är överens – EUD har mandat att upphäva ett sådant i den mån det inte är lagenligt.[272]

I skälen till GDPR anges vidare att förordningen inte hindrar att medlemsstaterna ingår avtal med tredjeländer för överföring av personuppgifter förutsatt att det inte påverkar EU-rätten och en skälig skyddsnivå finns.[273] Likaså ska inte GDPR påverka avtal mellan unionen och tredjeländer.[274] Det är emellertid inte helt klart utifrån formuleringen i skälet om man avseende avtalen som omfattar unionen som helhet bara inbegriper sådana avtal som redan finns eller om även *nya* avtal kan ingås. Dock markerar ordalydelsen i skäl 102 att ingående av avtal för medlemsstater är tillåtet under vissa förutsättningar, men markerar inte motsvarande befogenhet för unionen som sådan. Det indikerar att nya avtal endast är aktuellt på medlemsstatsnivå och inte för EU i stort. Skäl 102 lyder som följer:

> ”Denna förordning påverkar inte internationella avtal mellan unionen och tredjeländer som reglerar överföring av personuppgifter, däribland lämpliga skyddsåtgärder för de registrerade. Medlemsstaterna får ingå internationella avtal som innefattar överföring av personuppgifter till tredjeländer eller internationella

[269] Jämför formuleringen i GDPR, artikel 44.
[270] GDPR, artikel 46 – 49.
[271] Se till exempel GDPR, artikel 46.
[272] FEUF, artikel 263 – 266.
[273] GDPR, skäl 102.
[274] GDPR, skäl 102.

> organisationer i den mån sådana avtal inte påverkar denna förordning eller andra bestämmelser i unionsrätten och innehåller en skälig nivå av skydd för de registrerades grundläggande rättigheter."

Mot bakgrund av detta sällar jag mig till slutsatsen att de avtal som avses i förhållande till unionen i stort rör sådana som redan var ingångna före GDPR. Storbritannien verkar följaktligen inte kunna härleda sin tanke om ett avtal till skälet.

Det finns emellertid ytterligare omständigheter som ligger i linje med vad Storbritannien framför. Artikel 50 GDPR stadgar att kommissionen ska främja internationellt samarbete för personuppgiftsflöden på olika sätt. Man ska bland annat i relation till tredjeland utveckla rutiner för tillämpning av lagstiftning gällande skydd för personuppgifter, involvera berörda i diskussioner för att öka samarbetet, liksom verka för utbyte av lagstiftning på området.[275] Trots GDPR:s gedigna stadgande finns det alltså ändå en rörelse åt mer internationellt samarbete utöver adekvansbeslut, direkt i lagstiftningen. Dock, vad gäller just adekvansbesluten innebär dessa de facto att man från EU:s sida sprider den reglering som gäller inom EU. Detta sker förvisso inte nödvändigtvis genom exakt likalydande regler, men icke desto mindre på ett principiellt plan; som förklarats meddelas inte adekvansbeslut annars. Även om adekvansbesluten inte inbjuder till dialog och samarbete på samma sätt som man kan skönja i artikel 50, vill jag ändå hävda att adekvansbesluten bidrar till utbyte av lagstiftning för personuppgiftsflöden internationellt. Man uppnår således en del av tanken med artikel 50 GDPR genom adekvansbeslutet, även om det förvisso kanske sker i en mer "kolonial" anda än vad som verkar vara tanken bakom artikel 50. Kanske går därför adekvansbeslut och artikel 50 i någon mån ihop, även om det sker på EU:s villkor.

Mötet mellan artikel 50 och adekvansbeslutet ger upphov till en tvetydighet som både bekräftar GDPR som ett tätt sammansatt regelverk samtidigt som det öppnar för en möjlighet till mer dialog mellan berörda parter. Möjligheten för Storbritannien att härleda sin idé om ett avtal med EU tar emellertid inte slut där. Istället lyfter man i samband med sitt förslag om avtal gällande samarbete mellan myndigheter fram ett meddelande från kommissionen där internationellt samarbete på personuppgiftsområdet betonas.[276] Man hänvisar särskilt till ett uttalande där kommissionen säger att man tillsammans med berörda aktörer ska arbeta fram särskilda lösningar för särskilda situationer rörande överföring av personuppgifter till tredjeland.[277] En del av meddelandet hänvisar vidare till artikel 50 GDPR. Denna senare del har inte Storbritannien hänvisat till i sitt förslag till avtal i vitboken, men den är enligt min bedömning av största vikt för att förstå hur artikel 50 ska tolkas. Skrivelsen från kommissionen lyder:

> "Genom denna reform får kommissionen slutligen befogenheter att utarbeta mekanismer för internationellt samarbete i syfte att underlätta efterlevnaden av dataskyddsbestämmelserna, inklusive genom överenskommelser om ömsesidigt bistånd."[278]

[275] GDPR, artikel 50 a, c och d.
[276] Europeiska kommissionen, 2017.
[277] Europeiska kommissionen, 2017, sidan 12; vitboken, till exempel sidan 76.
[278] Europeiska kommissionen, 2017, sidan 6.

Kommissionen hänvisar sedan sitt uttalande till artikel 50 GDPR.[279] Så som jag läser detta begränsar kommissionen utrymmet för att enbart hänvisa till adekvansbeslutet som lösning på överföring av personuppgifter till Storbritannien efter brexit. Man öppnar, genom sitt eget meddelande och lydelsen av artikel 50 GDPR, istället för att andra lösningar *kan vara möjliga* – särskilda situationer kräver särskilda lösningar. I konsekvens med detta innebär det att uppräkningen i GDPR kanske inte är så uttömmande som den kan verka vid en första anblick och att utrymme *kan* finnas för förhandling om ett avtal mellan Storbritannien och kommissionen.

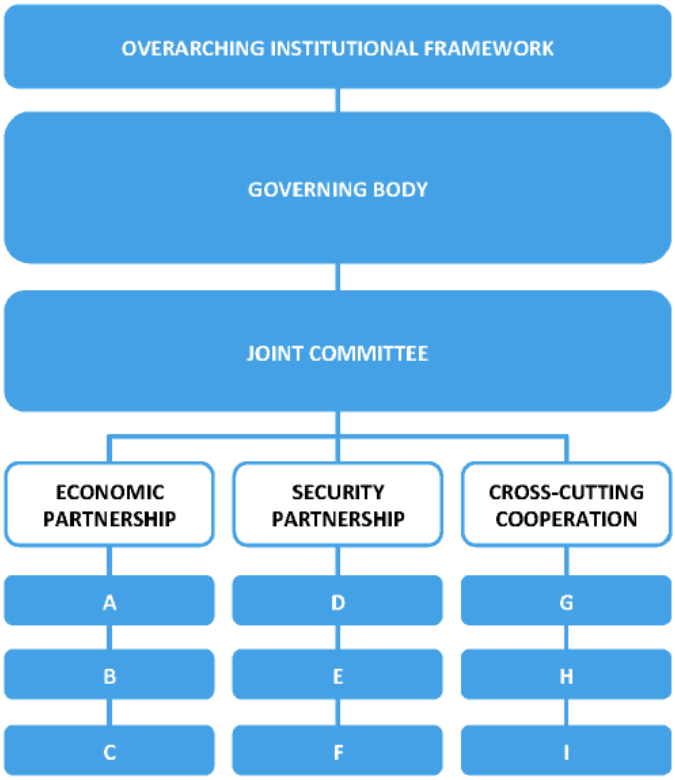
Vad är det då för lösning som Storbritannien vill få till genom ett avtal? Ovan nämnde jag att det dels rör ett ramverk för personuppgiftsflöden för att säkerställa transparens och stabilitet, dels samarbete mellan EU:s myndigheter för dataskydd och Storbritanniens ICO.[280] Det rör sig alltså om ett avtal i två delar, inledningsvis ska ramverket utredas, följt av myndighetssamarbetet.

4.2.1 Storbritanniens ramverk – uppbyggnad och tvistlösning

Innan jag går in på det ramverk man hänvisar till vad gäller just personuppgifter ska jag nämna något om den övergripande konstruktion man tänker sig. Potentiellt avser Storbritannien lägga avtalet för överföring av personuppgifter under den övergripande institutionella konstruktion man föreslår.[281] För det framtida samarbetet med EU vill Storbritannien, i konsekvens med föregående mening, alltså ha ett övergripande institutionellt ramverk. Konstruktionen för detta skulle se ut som följer. Först och främst skulle det övergripande ramverket för samarbetet fungera som ett paraply över de organ som inryms därunder. Ramverket skulle bestå av olika juridiskt bindande avtal och åtaganden på politisk nivå som inte har juridisk bindande verkan.[282] Därunder skulle ”Governing Body”(GB) och ”Joint Committee”(JC) ligga.[283] GB skulle vara ett politiskt organ för att mejsla ut den politiska riktningen för samarbetet på ministernivå.[284] JC å sin sida skulle fungera som ett exekutivt organ, man skulle se till att den riktning som beslutats av GB genomförs och man skulle också ha kompetens att lösa tvister mellan Storbritannien och EU.[285] Under bevakning av dessa organ skulle sedan samarbeten inom olika områden finnas genom avtal mellan parterna.[286] En bild av hur konstruktionen ser ut som följer:

[279] Europeiska kommissionen, 2017, sidan 6.
[280] Vitboken, till exempel sidan 74.
[281] Vitboken, sidan 84.
[282] Vitboken, sidorna 84 – 88.
[283] Vitboken, sidorna 84 – 88.
[284] Vitboken, sidorna 84 – 88.
[285] Vitboken, sidorna 84 – 88.
[286] Vitboken, sidorna 84 – 88.

Figur 1.[287]



Figur 1 visar hur Storbritannien konstruerar mekanismen inför ett framtida samarbete.

Man anger att vissa avtal skulle kunna komma att ligga utanför samarbetsmekanismen i den mån det bedöms att någon form av särreglering för detta skulle vara påkallad.[288] Det är inte tydligt utifrån vitboken om man redan nu har en uppfattning om vilka avtal som skulle falla inom den övergripande konstruktionen och vilka som skulle hanteras separat. Det är således svårt att avgöra vad som skulle vara fallet med just regleringen för flöden av personuppgifter. En tanke är emellertid att denna skulle kunna falla under såväl det ekonomiska som det säkerhetsmässiga partnerskapet i figur 1. Ekonomiskt skulle det avse rörlighet för data på ett näringsplan, och säkerhetsmässigt skulle det röra skyddet för personuppgifter.[289]

Man härleder konstruktionen av det institutionella ramverket ur andra överenskommelser om samarbete som EU har med tredjeländer, liksom ur avtal som gäller mellan internationella parter. Till exempel hänvisar man den övergripande institutionella strukturen till CETA[290], liksom att det finns ett internationellt tvistlösningsförfarande i NAFTA[291].[292] Potentiellt skulle alltså avtalet för flödet av personuppgifter kunna falla inom den övergripande mekanismen. Det som gör detta till en viktig fråga är att personuppgiftsflöden av allt att döma *inte* skulle falla inom området där

[287] Vitboken, sidan 86.
[288] Vitboken, sidan 86.
[289] Jämför Kommerskollegium, 2016, sidan 2; samt vitboken, sidorna 73 – 76.
[290] Comprehensive Economic and Trade Agreement, mellan EU och Kanada.
[291] North American Free Trade Agreement, mellan Kanada, USA och Mexiko.
[292] Vitboken, sidan 85. Man hänvisar i vitboken företrädelsevis till NAFTA i dess lydelse av juli 2018 och inte dess omförhandlade lydelse, se Elliott, Kimberly Ann, *Who Won in the NAFTA Renegotiation? A Preliminary Assessment*, World Politics Review, den 2 oktober 2018, https://www.worldpoliticsreview.com/articles/26188/who-won-in-the-nafta-renegotiation-a-preliminary-assessment, använd den 12 december 2018.

Storbritannien har en så kallad ”common rulebook”[293] med EU. Det skulle dessutom innebära att skyddet av personuppgifter i sådant fall skulle bli föremål för den prövningsmekanism man föreslår i vitboken.

Det är inte alldeles klart vad man menar med en common rulebook. Klart är emellertid att det är en konstruktion som ska finnas under det övergripande ramverket och att man tänker sig en sådan för till exempel varor och statsstöd.[294] Den gemensamma lösning som Storbritannien föreslår tycks bestå i att man ska ha samma regler som EU för till exempel varuflöden, för att varor ska kunna röra sig fritt över gränsen mellan EU och Storbritannien.[295] Common rulebook ska vara fallet där Storbritannien gör ett aktivt val att följa vissa EU-regler.[296] För dessa regler föreligger sedan ett särskilt förfarande där man bland annat vill säkerställa gemensam tolkning av reglerna, liksom kunna hänvisa till EUD.[297] Eftersom man uttryckligen anger att man avser ha en common rulebook för exempelvis varor, men inte gällande flödet av personuppgifter, drar jag slutsatsen att man inte tänker sig en sådan lösning på det senare området.[298] Det finns flera parametrar att ta upp inom ramen för detta eftersom common rulebook får konsekvenser för de regler som omfattas och därmed indirekt för de som inte omfattas.

Först och främst framgår en polemik rörande common rulebook i Storbritanniens ståndpunkt i förhållande till EU-rätten och EUD. När man talar om flödet av personuppgifter är man tydlig med att man vill ha *mer än* ett adekvansbeslut, man vill ha ett samarbete.[299] Man påpekar vilken unik startposition man har med GDPR som grund för sitt nationella personuppgiftsskydd.[300] Samtidigt, vad gäller det övergripande ramverket man vill tillämpa, är man mycket noga med att påpeka att man inte längre kommer att vara medlemsstat.[301] Av detta faktum följer att EU-rätten inte längre kommer att få företräde framför brittisk rätt. EU-rätten kommer helt enkelt inte längre att vara tillämplig i Storbritannien. Dessutom kommer förhandsavgöranden av EUD inte längre att vara möjliga, men ej heller lämpligt eller nödvändigt enligt Storbritannien.[302] Trots att man hävdar att det varken vore nödvändigt eller lämpligt med förhandsavgöranden från EUD, vill man inom ramen för tvistlösningsförfarandet för common rulebook kunna hänvisa till EUD för tolkning av EU-rätten.[303] Hänvisningen skulle i sådant fall göras antingen av JC eller en skiljenämnd.[304] Detta är visserligen generellt möjligt – under förutsättning att man lyckas sluta ett avtal med unionen med hänvisning till EUD i en skiljedomsklausul.[305] Dock markerar man här sitt avståndstagande från EU, samtidigt som man ändå vill hålla fast vid vissa utvalda delar. Dessa delar är dessutom sådana som man aktivt distanserar sig från i andra delar av vitboken.

---

293 Vitboken, sidan 89.
294 Vitboken, sidorna 8, 14 och 89 – 92.
295 Vitboken, sidorna 19 och 14.
296 Vitboken, sidan 89.
297 Vitboken, sidan 93.
298 Jämför vitboken, sidan 8 och till exempel sidan 73.
299 Vitboken, sidan 73.
300 Vitboken, sidan 75.
301 Vitboken, sidan 84.
302 Vitboken, sidorna 84 och 92.
303 Vitboken, sidan 93. Här ska nämnas att EUD fortsatt skulle ha jurisdiktion över Storbritannien under den övergångsperiod som ställs upp i utträdesavtalet om avtalet skulle röstas igenom, utträdesavtalet av den 14 november 2018, artikel 86.
304 Vitboken, sidan 93.
305 FEUF, artikel 272.

Samtidigt som man, i konsekvens med föregående stycke, markerar ett avstånd till EU-rätten i vissa bemärkelser vill man, utöver fortsatt möjlighet till avgörande av EUD i vissa fall, också vara med och påverka förändringar i common rulebook-lagstiftningen.[306] Möjligheten att påverka är förvisso något, vilket man också hänvisar till,[307] som finns i andra avtal för EU:s relationer till tredjeländer.[308] I dessa handlar det dels om ett informativt förfarande, dels om att man ska ha möjlighet att diskutera och inkomma med synpunkter innan en förändring görs av regelverk med bäring på avtalet mellan EU och landet.[309] En dylik lösning verkar höra till det normala i tredjelandsrelationer. Det är också ungefär så man vill lösa det för common rulebook-fallen.[310] Detta går i viss mån emot vad Storbritannien anför i andra delar avseende relationen till EU-rätten, även om det mot bakgrund av den normala lösningen mellan EU och tredjeländer inte är särskilt kontroversiellt. Något som emellertid blir av större intresse i denna del är hur Storbritannien tänker sig att man ska vidmakthålla en överensstämmande tolkning av reglerna inom ramen för common rulebook.

För att säkra en gemensam tolkning för common rulebook föreslår Storbritannien att de egna nationella domstolarna och EUD, ska ta hänsyn till praxis som utvecklats inom det relevanta området hos båda parter, i den mån ett mål angår innehållet i ett avtal dem emellan.[311] Skulle sådan diskrepans föreligga mellan de olika domstolarnas tolkning att man inte kan mötas skulle JC ha sista ordet för vad som vore en ändamålsenlig tolkning.[312] Storbritannien konstaterar samtidigt att EU-domstolen är det enda organ som kan binda EU gällande tolkningen av EU-rätten.[313] Man noterar också, i anslutning till detta, att man som tredjeland inte längre kommer att ha möjlighet att begära förhandsavgöranden hos EUD enligt artikel 267 FEUF. Något man, som sagt, i och för sig uttrycker varken vore lämpligt eller nödvändigt.[314] Storbritannien menar emellertid att det faktum att man inte längre kommer att kunna begära förhandsavgörande inte är något som kommer att påverka den gemensamma tolkningen – eftersom man ska ta hänsyn till varandras praxis.[315] Man avser bara utnyttja common rulebook-konstruktionen i de fall det finns omfattande mängder av praxis.[316] Det är riktigt att man som tredjeland förvisso inte kommer att kunna begära förhandsavgöranden av EUD.[317] Uttalandet går dock stick i stäv med att man ändå via JC eller skiljenämnd vill ha möjlighet att hänvisa till EUD i common rulebook-fallen. Dessutom säger man att även om JC skulle avgöra vad som är den rätta tolkningen av något i avtalet mellan parterna, skulle JC vid en tvist, efter hänvisning till och tolkning av EUD, avgöra i enlighet med EUD:s uppfattning om EU-rätten.[318] Det är således onekligen otydligt vad Storbritannien egentligen vill åstadkomma.

---

306 Vitboken, sidan 89.
307 Vitboken, sidan 89.
308 Se exempelvis kapitel 21 CETA; samt Economic Partnership Agreement between the European Union and Japan, 2017, kapitel 18.
309 CETA, artikel 21.4.
310 Vitboken, sidan 95, jämförd med CETA, artikel 21.4.
311 Vitboken, sidan 91.
312 Vitboken, sidan 91.
313 Vitboken, sidan 93.
314 Vitboken, sidan 92.
315 Vitboken, sidan 92.
316 Vitboken, sidan 92.
317 FEUF, artikel 267.
318 Vitboken, sidan 93.

I anslutning till ovanstående stycke är några noteringar på sin plats. Först och främst finns det ett problem i att säga att den överensstämmande tolkningen kommer att uppstå och slås vakt om genom att ta hänsyn till varandras praxis, det även om praxisen är omfattande. Redan inom ett och samma rättssystem finns problem med objektivitet och gemensam tolkning av samma regler. Även inom det svenska rättssystemet är detta ett problem, till exempel på grund av strukturell diskriminering.[319] Mot bakgrund av detta framstår *analys av varandras praxis* som ett något enkelt svar på frågan hur man ska lösa problemet med risken för diskrepans i tolkningen inom EU och Storbritannien. Även om den gemensamma rättsakten i detta fall skulle härröra från *ett* rättssystem skulle den tolkas i två olika, vilket knappast skulle minska risken för skilda tolkningar. Storbritanniens kommentar om att en tolkning från EUD inte vore nödvändig är utifrån detta ifrågasättbar. En lösning man föreslår är dock att JC ska få sista ordet, vilket förvisso skulle kunna lösa problemet med skilda tolkningar. Det skulle emellertid innebära att det tolkningsföreträde som EUD har i förhållande till EU-rätten och dess bindande verkan på EU, vilket Storbritannien vitsordar,[320] naggas i kanten.

Anledningen till att en genomlysning av konstruktionen för common rulebook är relevant i relation till personuppgiftsflöden är att, även om man inte verkar avse att ha en regelrätt gemensam reglering motsvarande den i varufallet, har man ändå angett att man tänker behålla GDPR i brittisk rätt.[321] Eftersom man placerar flödena av personuppgifter utanför common rulebook innebär det att man tänker sig tillämpa i stort sett samma regler, men utan att ha ett ramverk för tolkning som i fallet med common rulebook. Dessutom har man angett common rulebook som ett verktyg där det redan finns omfattande praxis. För personuppgiftsflöden vill man ha samma regler, men på ett område där det än så länge inte finns någon praxis för den senaste lagstiftningen. Även om det, som jag gjort i stycket ovan, kan pekas ut brister i ramarna för tolkningen av common rulebook, finns där ändå en uttalad vilja att för det framtida samarbetet röra sig åt samma håll som EU. Där finns också praxis att luta sig mot för att i alla fall sträva efter en överensstämmande tolkning. Någon sådant finns inte på samma sätt för personuppgiftsflöden.[322] Det ska påpekas att man i och för sig vill ha en avtalslösning för personuppgiftsflödena med avstamp i ett adekvansbeslut, på så sätt kan man säga att lösningen skiljer sig från hur common rulebook ser ut. Detta eftersom en avtalslösning bjuder till ytterligare överenskommelser mellan parterna än att Storbritannien enkom uttryckligen ska följa EU-reglerna. Icke desto mindre verkar Storbritannien ha för avsikt att behålla GDPR nationellt för att säkert nå skyddsnivån för ett adekvansbeslut.[323] Det faktiska resultatet av det blir att man har samma regler som EU, men inte enligt en common rulebook och därmed också utan de verktyg konstruktionen utrustar parterna med för gemensam tolkning och prövning.

Utanför området för common rulebook finns en annan tvistlösningsmekanism inom det övergripande ramverket för när tolkningarna går isär än den där hänvisning till EUD skulle vara möjlig. Istället ska man enligt denna lyfta tvisten för JC.[324] Kan frågan inte lösas genom förhandling ska den istället hänvisas till en oberoende skiljenämnd.[325] Av detta följer att det faktum att man

[319] Bladini, Moa, *Objektivitet i dömandet – på gott och på ont?,* Svensk juristtidning, 2016, sidan 304.
[320] Vitboken, sidan 93.
[321] Department for Digital, Culture, Media & Sport, 2018.
[322] Jämför vitboken, sidan 73 – 76.
[323] Vitboken, sidan 75; Department for Digital, Culture, Media & Sport, 2018.
[324] Vitboken, sidan 93.
[325] Vitboken, sidan 93.

väljer att hålla flödena av personuppgifter utanför konstruktionen för common rulebook kan innebära konsekvenser för det adekvansbeslut man vill ta avstamp i för sitt avtal med unionen. Utan någon möjlighet till hänvisning till EUD och med förlorad möjlighet till förhandsavgörande blir risken större att man rör sig bort från GDPR:s principer och därmed den adekvata skyddsnivån. Valet att placera överföringen av personuppgifter utanför common rulebook innebär inte bara att lösningen kommer att bli föremål för de problem som finns avseende skilda tolkningar i olika rättssystem som också finns *inom* common rulebook. Dessutom finns inte den uttalade ambitionen att söka sig åt samma håll i tolkningen som finns i common rulebook-fallet. Lägg därtill problematiken med förenlighet med stadgan som nämnts ovan och avståndet till EU-rätten blir än större och än mer problematiskt.

Så långt kan sägas att den första delen av avtalet Storbritannien vill sluta med EU på personuppgiftsområdet eventuellt skulle ligga under det övergripande ramverket för det framtida samarbetet. Klart är att man i sådant fall inte tänker sig att personuppgiftsflödena ska höra till en common rulebook, även om man vill fortsätta att tillämpa samma regler som EU. Detta kan potentiellt ställa till *mer problem* än om man lagt detta under en common rulebook. Den slutsatsen kommer av att man genom konstruktionen för common rulebook ställer upp en möjlighet att hänvisa till EU-domstolen, men inte genom den *allmänna tvistlösningsmekanismen* i vitboken. Lösningen genom common rulebook är förvisso behäftad med flera identifierade svagheter och motsättningar, men visar ändå på en vilja att röra sig åt ett och samma håll som unionen. Utan tolkningsmekanismerna enligt common rulebook-konstruktionen är personuppgiftsflödena hänvisade till att hanteras inom det generella tvistlösningsförfarandet i vitboken, vilket står längre ifrån EU-rätten.

Frågan är då hur man egentligen tänker sig med dataflödena. Jag läser Storbritanniens skrivning som ett aktivt uteslutande av common rulebook i fallet med personuppgiftsflöden, ändå vill man behålla samma, eller i vart fall i stort sett samma, regler. Detta innebär att man skulle stå helt bortom EUD:s kontroll eftersom dess tillsyn inte inbegrips på något sätt utanför common rulebook och eftersom man inte längre är medlemsstat.[326] Eftersom man säger sig vilja ha ett adekvansbeslut som grund för sitt avtal så framstår placeringen av den inhemska regleringen helt bortom EUD:s inflytande dock som något märklig. Risken blir därmed större att man rör sig bort från EU-rätten och grunden för beslutet. Dock har adekvansbeslutets kombination med ett avtal ifrågasatts ovan och kanske är det på grund av att dessa två svårligen förenas som detta är ett icke-problem för Storbritannien. Det vill säga att när man har ett avtal förlorar adekvansbeslutet sin unilaterala karaktär. Även om Storbritanniens skydd för personuppgifter då skulle börja avvika från EU:s standard på grund av brist på inflytande från EUD gör det ingenting när adekvansbeslutet inte kan dras tillbaka ensidigt. Förklaringen till att man håller personuppgifterna utanför common rulebook skulle emellertid också kunna vara, med de konsekvenser det innebär, att man de facto inte vill hålla sig till *exakt* samma regler, utan vill konstruera ett avtal som går utöver reglerna.

I vitboken finns inte många detaljer om vad den första delen av avtalet man vill ingå faktiskt skulle bestå i. Oaktat om detta skulle falla inom det övergripande ramverket eller ej, verkar den första beståndsdelen oavsett vara ett *eget ramverk* för flöden av personuppgifter. Faller detta utanför det

[326] Jämför FEUF, artikel 260.1 – 2.

övergripande ramverket bör detta andra ramverk vara behäftat med samma problem som det första. Hur ska gemensam tolkning kunna säkras, hur ska tvister lösas et cetera? Bortsett från dessa mer formella frågor verkar poängen man vill göra, även om det inte är tydligt i vitboken,[327] vara att man vill *komma runt de osäkerhetsmoment* som ett adekvansbeslut för med sig.[328] I ovanstående stycke nämner jag att ett adekvansbeslut kan dras tillbaka ensidigt av kommissionen i den mån skyddsnivån inte längre bedöms vara adekvat.[329] Detta innebär en osäkerhet för de som vill föra uppgifter mellan EU och Storbritannien. Från brittiskt håll argumenterar man därför för att ett avtal vore att föredra framför ett adekvansbeslut för att undvika avbrott i dataöverföringen,[330] genom ett ömsesidigt bindande avtal. Detta ligger i linje med att adekvansbeslutet som grund kanske inte är en faktisk möjlighet när man vill ha ett avtal. Med avseende på avbrott i flödena drar Storbritannien paralleller till vad som hände angående överföringen av personuppgifter när EU-domstolen ogiltigförklarade kommissionens adekvansbeslut i förhållande till USA i Schrems-målet.[331] Man hänvisar till avbrutna flöden och att vikten av dataflödena för handeln innebär att man inte ska riskera att samma sak händer igen.[332]

Utifrån denna argumentation kan man se att det skulle finnas ett intresse även för EU att inte vilja att flödena stoppas. Vad man emellertid inte lyfter, är varför Schrems-målet fick det utfall det faktiskt fick. Det var för att den amerikanska hanteringen av personuppgifter inte hade en likvärdig standard som det skydd som gällde i EU, då med betoning på skyddet enligt stadgan.[333] De eventuella problem Storbritannien har avseende stadgan enligt Tele2-domen bjuder visserligen inte in till att lyfta denna problematik i det egna dokumentet. Frågan väcks emellertid om det avtal man söker kanske rent av eftersträvas för att kunna ha ett avvikande skydd från det inom EU. Det är måhända en konspiratorisk tanke. Icke desto mindre öppnar en avtalslösning för en möjlighet till detta, mot bakgrund av att det i sådant fall skulle handla om en *överenskommelse* mellan två parter och inte ett unilateralt beslut från unionen.

Sammanfattningsvis kan konstateras att den första delen av avtalet Storbritannien vill ha med EU avseende persondataflöden egentligen föreslagits för att man inte vill bygga allt på ett ensidigt beslut, vilket kan dras tillbaka av kommissionen och därmed skapa besvär för aktörer. Istället vill man skapa ett ömsesidigt förhållande för att komma runt ensidigheten. Det är inte klart om man vill att avtalet ska existera inom det övergripande ramverket man vill bygga upp, eller vid sidan av detta. Oavsett vilken lösning man tänker sig finns problem med hur man ska säkra bland annat enhetlig tolkning av de i stort sett gemensamma reglerna och tvistlösning. Oaktat detta verkar man inte vilja hantera personuppgiftsflöden inom ramen för common rulebook. Detta innebär risker i

---

[327] Jämför vitboken, sidan 74.
[328] Exiting the European Union Committee, The progress of the UK's negotiations on EU withdrawal: Data, 2018, https://publications.parliament.uk/pa/cm201719/cmselect/cmexeu/1317/131706.htm#_idTextAnchor011, använd den 28 november 2018; The Government of the United Kingdom, Technical Note: Benefits of a New Data Protection Agreement, 2018.
[329] GDPR, artikel 45.5.
[330] Exiting the European Union Committee, 2018; The Government of the United Kingdom, Technical Note: Benefits of a New Data Protection Agreement, 2018.
[331] Exiting the European Union Committee, 2018; The Government of the United Kingdom, Technical Note: Benefits of a New Data Protection Agreement, 2018.
[332] Exiting the European Union Committee, 2018; The Government of the United Kingdom, Technical Note: Benefits of a New Data Protection Agreement, 2018.
[333] Schrems-målet.

förhållande till det adekvansbeslut man vill ha som utgångspunkt för avtalet, mot bakgrund av vilket avstånd som skapas till EU-rätten med en sådan lösning. Dock skulle ett sådant adekvansbeslut ändå kunna sättas ur spel just på grund av att man sluter ett avtal istället för att kommissionen fattar ett unilateralt beslut, på basis av EUD:s befogenhet att ogiltigförklara dylika avtal.

4.2.2 Samarbetet mellan Information Commissioner och EU:s myndigheter för skydd av personuppgifter

Som påpekats flertalet gånger vill Storbritannien grunda sitt personuppgiftssamarbete med EU på ett adekvansbeslut. Inom ramen för bedömningen av adekvat skyddsnivå har kommissionen som ett av kriterierna att tredjelandets dataskyddsmyndighet ska samarbeta med medlemsstaternas motsvarigheter.[334] Angående denna parameter, se ovan i kapitel tre. Storbritannien vill emellertid gå längre än var adekvansbeslutet medger även när det kommer till samarbete mellan myndigheter. Här vill man komma överens med unionen, i den andra delen av det tilltänkta avtalet. Man skulle förvisso kunna tänka sig att det faktum att samarbete mellan dataskyddsmyndigheter som kriterium för adekvat skyddsnivå är något som talar *för* Storbritanniens ambition om ett avtalat samarbete med EU. Det är emellertid inte givet mot bakgrund av vad Storbritannien föreslår i vitboken och hur reaktionerna blivit från unionen på dessa förslag.

För att samarbeta, och fortsätta det samarbete som redan finns, vill Storbritannien att deras dataskyddsmyndighet ICO, ska fortsätta att vara en del av den så kallade ”One Stop Shop”-mekanismen (OSS). Vad OSS innebär har förklarats i avsnitt 2.3. Här ska dock erinras om att bestämmelserna i GDPR markerar att det rör sig om gränsöverskridande behandling, det vill säga överföring sker *mellan medlemsstater, inte till tredjeländer*. Dessutom ska påminnas om den mekanism som finns för enhetlighet i tillämpningen av GDPR av tillsynsmyndigheterna där styrelsen ingår.[335] Denna konstruktion är inte helt olik den som Storbritannien föreslår för att nå en enhetlig tolkning i relation till sin common rulebook-konstruktion, om än med några viktiga skillnader. För det första fungerar styrelsen och de ramar man satt upp för samarbete och enhetlighet i unionen inom ett system. För det andra finns styrelsen inom systemet som tvistlösningsmekanism och för det tredje finns EU-domstolen som kan agera i den mån en medlemsstat inte skulle följa förordningen.[336]

Det är inte heller här helt tydligt vad Storbritannien menar med att man fortsatt vill delta i OSS. Man vill med all säkerhet fortfarande kunna vara behörig att ta emot ärenden från verksamheter och privatpersoner i enlighet med artikel 56.1 – 2 GDPR. Storbritannien har emellertid ändrat sin position avseende samarbetet något sedan i maj 2018. Tidigare ville man inte bara vara en fortsatt del av OSS, man ville också fortsatt låta sig representeras i styrelsen för tolkning och tvistlösning.[337] I vitboken finns detta inte längre med. Kanske är det ett resultat av den reaktion som kom från EU i samband med att Storbritannien publicerade sin ambition. Från EU reagerade man med att det varken var aktuellt för Storbritannien att sitta kvar i styrelsen eller, om än inte helt tydligt, fortsatt

[334] GDPR, artikel 45.2 b.
[335] GDPR, artikel 63 – 67. Se ovan i avsnitt 2.3 för en närmare beskrivning av mekanismen.
[336] FEUF, artikel 260.
[337] The Government of the United Kingdom, Framework for the UK-EU partnership Data Protection, 2018, sidan 17.

vara en del av OSS.[338] Det är emellertid ändå inte klart i vilken grad man vill fortsätta samarbeta med andra medlemsstater. Detta mot bakgrund av att det vore märkligt att separera OSS från mekanismen för enhetlighet – OSS och dess funktion bör vara beroende av denna. Detta konstaterar jag utifrån att i den mån man ska kunna vända sig till endast en tillsynsmyndighet i ett ärende kräver detta samarbete mellan myndigheterna och samarbete kräver enhetlighet i tillämpningen av GDPR.[339]

Unionen uttrycker att det är otänkbart att ha med ett tredjeland i det system som är avsett att fungera inom unionen, eftersom det skulle underminera EU:s självständighet.[340] Dessutom påpekar man att i den mån man inte är medlemsstat finns ingen som tillser att man följer regelverket, ej heller någon som kontrollerar att man uppdaterar det efter ändringar från EU.[341] Detta vill säga att Storbritannien inte längre skulle befinna sig under bevakning av EUD. Oaktat om Storbritannien bara tänker sig att man skulle vara del av OSS eller också en del av enhetlighetsmekanismen, blir det utifrån EU:s argumentation svårt att se att det skulle fungera att vara en del av OSS och enhetligheten när man inte längre är medlemsstat.[342]

Intressant med Storbritanniens argumentation är emellertid hur man använder sig av kommissionens egna uttalanden, liksom GDPR som sådan för att argumentera för att ett fortsatt deltagande i OSS vore en bra lösning. Jag har ovan[343] berört artikel 50 GDPR om internationellt samarbete och kommissionens meddelande om utbyte av personuppgifter globalt. I vitboken använder Storbritannien dessa verktyg för att driva sina argument för att kunna avtala med EU om att stanna i OSS. Storbritannien understryker, genom artikel 50 och kommissionens meddelande, EU:s egen rörelse mot mer samarbete med tredjeländer, och ett potentiellt avtal om OSS. I kommissionens meddelande påpekas att artikel 50 GDPR öppnar för att utöka möjligheterna till internationellt samarbete.[344] Dessutom säger kommissionen att man ska ”utveckla mekanismer för internationellt samarbete med viktiga internationella partner för att underlätta en effektiv tillämpning.”[345] I vitboken citerar Storbritannien det senare uttalandet och budskapet verkar vara att man vill agera startskott för kommissionens arbete med detta.[346] Man använder kommissionens egen ambition för att peka på att man borde skapa ny praxis och röra sig mot den nya ordning man kan skönja i kommissionens meddelande och GDPR.

Trots problemen som finns med ett fortsatt deltagande i OSS som tredjeland, förefaller således Storbritannien vilja påverka unionen i en viss riktning med hjälp av EU:s egen argumentation. På det sättet blir det svårare för EU att värja sig, eftersom man genom det också visar att även EU skulle kunna gynnas av att ha ett avtal om persondataflöden med tredjeland och då kanske just med Storbritannien. Samtidigt antyder inget i kommissionens meddelande att det samarbete man avser

338 Barnier, 2018.
339 Se ordalydelsen i GDPR, artikel 63.
340 Barnier, 2018.
341 Barnier, 2018.
342 Jämför också Kommerskollegium, *Storbritanniens vitbok om den framtida relationen med EU, en analys av förslagen*, 2018, sidan 23.
343 Avsnitt 4.2.
344 Europeiska kommissionen, 2017, sidan 6.
345 Europeiska kommissionen, 2017, sidan 14.
346 Vitboken, sidan 76.

skulle sträcka sig så långt som att bjuda in tredjeländer i EU:s egna mekanismer, inte ens om det rör sig om en före detta medlemsstat.[347] Vad Storbritannien utelämnar om kommissionens meddelande är att man pekar ut adekvansbeslutet som den bästa lösningen för personuppgiftsflöden till tredjeland, liksom att personuppgiftsflöden generellt, såväl som adekvansbeslutet specifikt inte kan förhandlas.[348] Michel Barnier[349] kommenterar dessutom Storbritanniens uttalande om att det skulle ligga i EU:s intresse att Storbritannien är kvar i OSS och styrelsen med att brexit aldrig kommer att ligga i unionens aktörers intresse.[350] Barniers svar i detta fall kan tyckas missa målet. Det kan förvisso hävdas att brexit inte ligger i EU:s intresse, men nu när det ändå verkar bli verklighet – skulle det inte ligga även i unionens intresse att avtala om dataflöden och därmed låta Storbritannien vara fortsatt del av OSS?

Ett Storbritannien som del av OSS skulle innebära ett underlättat förfarande för privatpersoner och företag som skulle kunna fortsätta att vända sig till ICO vid gränsöverskridande behandling, även om den ansvariga myndigheten egentligen skulle befinna sig någonstans inom unionen. Istället för att behöva söka upp myndigheten själv skulle det alltså vara enklare för privatpersoner och företag som skulle slippa den administrativa bördan som istället skulle ligga på myndigheterna.[351] På så sätt skulle Storbritanniens föreslagna lösning minst sagt ligga i unionens aktörers intresse. Däremot skulle en lösning där ett tredjeland är med i en mekanism inom ramen för EU-samarbetet men inte behöver underkasta sig EU-domstolen urholka EU:s självständighet, precis som Barnier påpekar.[352] Hur ska man då vara säker på att man kan lita på att Storbritannien följer och uppdaterar efter GDPR?[353] Här vill jag påminna om att Storbritannien, som nämnts, varit mycket tydligt med att EUD inte skulle ha något inflytande över Storbritannien efter utträdet, med undantag för den eventuella common rulebook-konstruktionen, vilken i och för sig inte skulle omfatta personuppgiftsflöden.[354]

Sammanfattningsvis vill Storbritannien att deras dataskyddsmyndighet, ICO, ska vara en fortsatt del av OSS. Det är oklart hur man tänker kring att också vara del av konstruktionen för enhetlighet främst mot bakgrund av att OSS och denna inte helt lätt låter sig separeras. EU har tydligt deklarerat att man inte vill ha ett avtal där ICO skulle vara en fortsatt del av OSS. Det är emellertid inte helt självklart att unionens aktörer, och unionen i sig, inte skulle kunna dra nytta av en sådan lösning. Det skulle bli enklare för privatpersoner och företag att kontakta myndigheter i unionen och Storbritannien vid gränsöverskridande behandling mellan EU och Storbritannien. För att nå en sådan lösning använder Storbritannien delar av EU:s egna argument för ett starkare samarbete med tredjeländer angående persondataflöden. Från EU har man emellertid påpekat att ett dylikt samarbete på intet sätt är möjligt. Detta med hänsyn till att det skulle underminera unionens självbestämmande att inviga ett tredjeland i en unionsmekanism utan att EUD skulle ha jurisdiktion över detsamma.

---

347 Jämför Barnier, 2018, som istället explicit säger precis tvärtom.
348 Europeiska kommissionen, 2017, sidan 9.
349 EU:s chefsförhandlare i brexit-förhandlingarna med Storbritannien.
350 Barnier, 2018.
351 GDPR, artikel 56.1 – 2.
352 Barnier, 2018.
353 Jämför Kommerskollegium, *Storbritanniens vitbok om den framtida relationen med EU, en analys av förslagen*, 2018, sidan 23.
354 Vitboken, sidorna 84 och 93.

4.3 Slutsatser och funktionen för betaltjänsten och företaget av presenterade lösningar sprungna ur Storbritanniens vitbok

En lösning i enlighet med Storbritanniens förslag skulle ha konsekvenser för betaltjänsten och företaget. Först och främst skulle det ramverk man föreslår, oaktat om detta skulle fungera inom det övergripande ramverket eller som ett separat avtal förmodligen bidra till mer säkerhet. I avsnitt 3.2 har jag nämnt att det finns en inneboende osäkerhet i adekvansbeslutet i egenskap av ett ensidigt beslut som kan dras tillbaka av kommissionen om skyddsnivån inte består. Storbritannien vill, med avtalet om ett ramverk för personuppgiftsflöden hantera denna risk. Att man anger att man vill ha adekvansbeslutet som utgångspunkt tolkar jag i relation till avtalets funktion som att utfallet för betaltjänsten blir som i adekvansbeslutsfallet. Det vill säga ett flöde av personuppgifter som inte kräver någon åtgärd från betaltjänsten och som fungerar som om Storbritannien fortfarande var en medlemsstat, om än inte behäftat med de orosmoment som adekvansbeslutet bjuder. I detta inbegrips då att betaltjänsten fortfarande måste uppfylla kraven enligt GDPR.[355]

Betaltjänsten skulle således kunna föra över personuppgifter till Storbritannien utan hinder, eftersom Storbritannien av kommissionen ansetts ha adekvat skyddsnivå. Dock får det antas som följd av avtalskonstruktionen att kommissionen inte skulle kunna dra tillbaka beslutet *ensidigt* utan konsekvenser, i den mån Storbritannien inte längre skulle uppfylla efterfrågad skyddsnivå. Detta skulle potentiellt vara negativt för privatpersoner eftersom det är deras personuppgifter som ska skyddas. För betaltjänsten och företaget skulle det emellertid bidra med mer säkerhet kring deras överföring av personuppgifter. Man skulle inte behöva oroa sig och ej heller behöva gardera sig för att ett ensidigt beslut plötsligt dras tillbaka med eventuella avbrott i flödena som följd. Inte heller skulle det innebära mer arbete för aktörerna, istället skulle den administrativa bördan fortsatt ligga på Storbritannien respektive EU.

Den andra delen av Storbritanniens avtal skulle också innebära mindre arbete för betaltjänsten och företaget än vid ett adekvansbeslut. De skulle kunna vända sig till den ansvariga myndigheten i sitt land, det vill säga ICO för företaget i Storbritannien inom ramen för OSS, i den mån man skulle behöva ta en myndighetskontakt i anslutning till den gränsöverskridande behandlingen. Det faktum att Storbritannien inte skulle ligga under EUD:s jurisdiktion ska emellertid inte underskattas och det är oklart hur man vill hantera enhetligheten för samarbetet inom OSS. Dessa parametrar skulle också påverka betaltjänsten och företaget. Utan tillsyn och möjlighet att påverka Storbritanniens utveckling regelmässigt innebär det också att en diskrepans kan uppstå mellan de regler betaltjänsten respektive företaget har att förhålla sig till. Här skulle jag vilja påpeka att ett ensidigt adekvansbeslut ur detta perspektiv rent av skulle kunna bidra med *mer säkerhet* för flödena av personuppgifter än enligt den modell Storbritannien föreslår. Gäller ett ensidigt adekvansbeslut vet man att man behöver följa samma skyddsnivå som i EU. Ett särskilt avtal där utvecklingen *kan* gå åt olika håll i jurisdiktionerna och där Storbritannien vill vara del av EU:s mekanismer, men utan att vara underkastad EUD, kan istället ge upphov till osäkerhet. En ovisshet om vilken standard som ska gälla skulle i sådant fall kunna börjar gro hos aktörerna. Det skulle alltså kunna leda till en osäkerhet om *standarden på skyddet* som sådan, och inte bara en osäkerhet kring om adekvansbeslutet skulle kvarstå.

[355] GDPR, artikel 44.

För betaltjänsten och företaget skulle Storbritanniens förslag alltså inte skilja sig i någon vidare utsträckning från adekvansbeslutet, mer än att flödenas bestånd inte skulle vara omgärdade av samma osäkerhetsmoment som i det rena adekvansbeslutsfallet. Det skulle underlätta för aktörerna om Storbritannien var del av OSS eftersom merparten av det administrativa arbetet vid myndighetskontakter skulle skötas av myndigheterna själva. Dock skulle en sådan ordning kunna leda till större osäkerhet kring vilka principer som ska följas, snarare än osäkerhet kring beslutet, på grund av olika tolkningar i de olika jurisdiktionerna.

Den återstående frågan är om det Storbritannien föreslår faktiskt är en möjlig lösning för personuppgiftsflödena. Vad Storbritannien inte tagit hänsyn till vad gäller avtalskonstruktionen är att denna egentligen inte ryms inom ramarna för GDPR. Man har från EU förvisso visat tendenser till att vilja röra sig i riktning mot mer samarbete med tredjeländer. Dock, vilket nämnts kort ovan, tar Storbritannien inte upp, när man försöker påverka unionen i en viss riktning med kommissionens eget uttalande, att kommissionen i samma meddelande konstaterar att:

> ”EU:s regler om dataskydd kan inte bli föremål för förhandlingar i ett frihandelsavtal. Medan dialoger om dataskydd och handelspolitiska förhandlingar med tredjeländer måste följa separata spår, är ett beslut om adekvat skyddsnivå, inbegripet ett partiellt eller sektorsspecifikt beslut, det bästa sättet för att skapa ömsesidigt förtroende.”[356]

Man markerar således från kommissionens sida att man ska främja någon form av samarbete med tredjeländer, men inte förhandla om reglerna för personuppgiftsskydd. Det finns inga andra tendenser från EU än att det är främst adekvansbeslutet åtföljt av andra lösningar i GDPR som är aktuellt mellan EU och Storbritannien.[357] Utöver detta ska påpekas att det är svårt att se, förutom att det skulle gynna aktörerna i viss mån genom stabila flöden och OSS, hur EU skulle gagnas av ett avtal istället för ett ensidigt beslut i förhållande till Storbritannien. EU:s autonomi skulle urholkas och man skulle vara bunden av något där risken finns att motparten börjar avvika från det skydd som stadgas i unionen, utan att man egentligen skulle kunna avbryta detta utan att ådra sig avtalsrättsliga konsekvenser. EU och Storbritannien skulle således gå från den effektiva tillämpningen i unionen under överinseende av EUD, till ett förhållandevis tandlöst avtal. Det är i och för sig troligt att avtalet skulle inrymma åtgärder att vidta vid avtalsbrott, men eftersom Storbritannien inte nämner något om detta går det inte säkert att veta eller uttala sig om.

Mot bakgrund av ovanstående, om än positivt för betaltjänsten och företaget i vissa bemärkelser, verkar inte ett avtal mellan Storbritannien och EU på området troligt. EU vill hålla fast vid det ensidiga adekvansbeslutet, och inte bjuda in ett tredjeland i vilket man inte kan bevaka efterlevnaden att delta i dess mekanismer för samarbete för personuppgiftsflöden. Inte heller verkar man vilja förhandla om adekvansbeslutets ensidiga karaktär till förmån för stabilare flöden utan samma risk för avbrott. Dessutom ska det påpekas att i den mån man ändå skulle kunna tänka sig att avtala med Storbritannien skulle EUD kunna förklara avtalet ogiltigt eftersom det går utöver

[356] Europeiska kommissionen, 2017, sidorna 9 – 10.
[357] Politiska deklarationen, sidan 4; Utträdesavtalet av den 14 november 2018, artikel 71; Europeiska kommissionen, Withdrawal of the United Kingdom from the Union and the EU Rules in the Field of Data Protection, 2018.

vad som medges i GDPR,[358] på samma sätt som gjordes i Schrems-målet. Utifrån en privatpersons perspektiv är det ett sätt för EU att slå vakt om att man måste kunna ta tillbaka beslutet om adekvat skyddsnivå i den mån man avviker från principerna i EU-rätten. För betaltjänsten och företaget är detta emellertid ett osäkerhetsmoment som adekvansbeslutet är behäftat med.

Utifrån min utredning ovan drar jag slutsatsen att det Storbritannien föreslår i vitboken över huvud taget inte är en lösning som skulle kunna vara möjlig. Kanske är det enda argument som Storbritannien för fram som egentligen håller att detta är en speciell situation och sådana kräver speciella lösningar.[359] Inte heller är EU-rätten helt isolerad mot speciallösningar, utan sådana finns i relation till USA och Kanada genom partiella adekvansbeslut. Dock, som kommer visas i nästa kapitel tenderar det speciella med dessa vara att man begränsar beslutet, snarare än låter det svälla utanför GDPR:s gränser.

5 Utblick USA och Kanada – hur skulle överföringen av betaltjänstens insamlade personuppgifter från EU till Storbritannien se ut enligt dessa modeller?

Man verkar som sagt från EU:s sida obenägen att vilja lösa situationen på annat sätt än genom ett adekvansbeslut. De exempel som finns där man kunnat tänka sig att avvika något från det traditionella adekvansbeslutet är det så kallade ”Privacy Shield”(PS)-ramverket man antagit i relation till USA liksom lösningen med Kanada.[360] Skillnaderna mellan dessa beslut och de traditionella adekvansbesluten är främst de följande. Ett adekvansbeslut riktar sig typiskt sett till ett land som sådant, ett specifikt territorium därinom, men kan också omfatta en eller flera specifika sektorer i landet.[361] Konstruktionen man byggt för personuppgiftsöverföring till USA handlar istället om ett självcertifieringssystem.[362] Det man har i relationen med Kanada omfattar endast aktörer i den privata sektorn som lyder under den kanadensiska lagen Personal Information Protection and Electronic Documents Act.[363] Vad som emellertid alltjämt gäller är att den som vill föra över uppgifter till USA eller Kanada måste följa GDPR i övrigt.[364]

Det amerikanska fallet innebär i första hand att det inte är de amerikanska förhållandena avseende lagstiftning och internationella åtaganden som sådana man bedömer för att adekvat skyddsnivå ska anses vara uppfylld. Istället bygger mekanismen på att företag som ska ta emot personuppgifter från EU uppfyller krav enligt EU-rätten i sin hantering av uppgifterna. Företagen registrerar sig för att sättas upp på PS-listan genom att de uppfyller kraven, alltså genom självcertifiering. USA:s handelsdepartement[365] verifierar att företagen de facto följer den standard som ställs upp enligt

[358] Det skulle därmed inte vara lagenligt, FEUF, artikel 263 – 266.
[359] The Government of the United Kingdom, Technical Note: Benefits of a New Data Protection Agreement, 2018.
[360] De är *partiella* adekvansbeslut, Europeiska kommissionen, 2017, sidan 7.
[361] GDPR, artikel 45.
[362] Europeiska kommissionen, EU-U.S. Privacy Shield: Frequently Asked Questions, 2016, http://europa.eu/rapid/press-release_MEMO-16-2462_en.htm, använd den 29 november 2018.
[363] Europeiska kommissionen, Kommissionens beslut av den 20 december 2001 i enlighet med Europaparlamentets och rådets direktiv 95/46/EG om adekvat skydd för personuppgifter genom den kanadensiska lagen om elektroniska handlingar och skydd för personuppgifter (2002/2/EG) (EGT L 2, 4.1.2002, s. 13–16) (adekvansbeslut för Kanada), 2001.
[364] GDPR, artikel 44.
[365] US Department of Commerce.

EU-rätten i PS-ramverket. Självcertifieringen är under kontroll av handelsdepartementet, som också ska samarbeta med dataskyddsmyndigheter i EU. Utöver detta har ramverket justerats efter den ovan nämnda Schrems-domen. Det förhindrar masslagring av data för att nationella myndigheter ska beredas obegränsad tillgång till personuppgifter från unionen.[366] Man har dessutom inrättat en särskild ombudsperson för att hantera klagomål från individer på nationella myndigheters tillgång till personuppgifter, liksom flera andra möjligheter till prövning.[367] Istället för att anpassa sin lagstiftning står amerikanska staten för vissa garantier, medan det är aktörerna som tillgodoser en adekvat skyddsnivå i störst utsträckning. Vad EU angår har kommissionen ändå tagit hänsyn till de parametrar man normalt sett gör vid ett adekvansbeslut.[368] Det är emellertid företagen istället för tredjelandets lagar et cetera som ska stå för att garantera skyddsnivån. Låt vara att man justerat de amerikanska lagarna för att begränsa och villkora tillgången till personuppgifter för nationella myndigheter. Även i relation till Kanada har kommissionen tagit hänsyn till de parametrar som normalt bedöms inom ramen för ett adekvansbeslut. Det kanadensiska fallet innebär inte ett självcertifieringssystem, utan är istället mer som ett traditionellt adekvansbeslut, med det undantaget att det endast riktar sig till den privata sektorn.[369] Kort sagt kan besluten sägas vara ett exempel på *speciallösningar i specialfall*, i och med att regleringen kring personuppgifter skiljer sig markant mellan EU och USA och Kanada.

I relation till vad Storbritannien vill uppnå är dessa faktiska exempel på hur EU har specialanpassat adekvansbeslutet. Det är således något som *kan ske*. Dock ska det tilläggas att dessa lösningar inte står utanför vad GDPR medger.[370] Det rör sig fortfarande om ensidiga beslut från kommissionen liksom att tredjelandet säkerställer adekvat skyddsnivå, om än på ett något okonventionellt sätt i sammanhanget. Man skulle kunna tala i termer av att man skalar ner adekvansbeslutet till att gälla något mycket specifikt – just det företag som är certifierat eller de i privat sektor – och inte hela landets skyddsnivå. Alternativt att det amerikanska beslutet kan ses som ett slags hybrid mellan adekvansbeslut och lämpliga skyddsåtgärder,[371] vilka jag ska återkomma till nedan. Utifrån att adekvansbeslutet kan rikta sig mot en specifik sektor bör dock den förra beskrivningen vara mest intuitiv. Fallen med USA och Kanada rör således *partiella adekvansbeslut*,[372] riktade mot en specifik sektor enligt artikel 45.1 GDPR.

Anledningen till att jag vill ta upp de amerikanska och kanadensiska lösningarna är att jag vill visa att det finns exempel på speciallösningar från kommissionen, vilka också bidrar till att förklara hur Storbritanniens förslag fungerar i relation till dessa. Jag kommer att återkomma till denna relation i diskussionen nedan.[373] Såhär långt kan emellertid sägas att Storbritanniens ambition om en speciallösning för ett specialfall, mot bakgrund av lösningarna med Kanada och USA, i viss mån är intuitiv, även om ett partiellt adekvansbeslut inte är vad Storbritannien föreslår. Vad som dock ska

366 Europeiska kommissionen, EU-U.S. Privacy Shield: Frequently Asked Questions, 2016, http://europa.eu/rapid/press-release_MEMO-16-2462_en.htm, använd den 29 november 2018.
367 Europeiska kommissionen, EU-U.S. Privacy Shield: Frequently Asked Questions, 2016, http://europa.eu/rapid/press-release_MEMO-16-2462_en.htm, använd den 29 november 2018.
368 Europeiska kommissionen, EU-U.S. Privacy Shield: Frequently Asked Questions, 2016, http://europa.eu/rapid/press-release_MEMO-16-2462_en.htm, använd den 29 november 2018.
369 Adekvansbeslut för Kanada.
370 Jämför ordalydelsen i GDPR, artikel 45.
371 GDPR artikel 46.
372 Europeiska kommissionen, 2017, sidan 7.
373 Kapitel 8.

påpekas är att man, i den mån man får ett adekvansbeslut, inte kan vara säker på att det inte är ett partiellt sådant. Är det påkallat enligt kommissionen skulle även Storbritannien kunna få ett adekvansbeslut riktat mot en specifik sektor, eftersom beslutet är ensidigt. Ett dylikt beslut skulle således inte ha något som helst att göra med vad Storbritannien föreslår som lösning. De partiella adekvansbesluten innebär att adekvansbeslutet avskalas och omfattar mindre än det gör i normalfallet. De indikationer man ser från unionen visar också att man har adekvansbeslutet som absolut gräns.[374]

5.1 Slutsatser och funktionen för betaltjänsten och företaget av ett speciellt (partiellt) adekvansbeslut i ett speciellt fall

För betaltjänsten och företaget vore speciallösningen med självcertifiering besvärligare än ett adekvansbeslut i traditionell mening. Adekvansbeslutet innebär, som tidigare påpekats, att personuppgifter kan föras över utan vidare åtgärd från aktörerna.[375] I detta fall skulle förvisso betaltjänsten, med säte i EU, kunna föra över utan vidare åtgärd, så länge företaget i Storbritannien skulle kvalificera sig för självcertifiering. Eftersom företagen i Storbritannien i stor utsträckning skulle bli ansvariga för att uppfylla adekvat skyddsnivå, istället för att enbart följa de aktuella lagarna för personuppgiftsskydd, skulle bördan flyttas från relationen mellan Storbritannien och EU till aktörerna. I förhållande till utfallet av ett vanligt adekvansbeslut ter sig detta närmast som ett slags hybrid mellan adekvansbeslut och andra lösningar för tredjelandsöverföring i GDPR, vilka jag ska komma in på nedan. Även om det här är ett sätt för personuppgifter att kunna flöda och vara fortsatt skyddade är en speciallösning av detta slag inget som skulle vara till fördel för aktörerna, jämfört med ett vanligt adekvansbeslut. Vad gäller den kanadensiska lösningen är denna mer lik ett ordinärt adekvansbeslut, om än ett begränsat sådant. Likheten med det traditionella adekvansbeslutet begränsar sig till företag i privat sektor som omfattas av en särskild lag. Därför, under förutsättning att företaget skulle omfattas av lagen i fråga, skulle denna lösning fungera som ett vanligt adekvansbeslut för betaltjänsten och företaget, alltså fria flöden från EU till Storbritannien enligt GDPR. Även om det gäller kanadensiska förhållanden och inte brittiska kan det påpekas att inget i den kanadensiska lag man som privat aktör ska lyda under tyder på att företaget i typfallet skulle vara undantaget.[376]

Utifrån denna utblick kan slutsatsen dras att de speciallösningar som ändå finns mellan EU och tredjeland för överföring av personuppgifter inte är något som skulle vara ändamålsenligt för Storbritannien. Dock kan det inte garanteras att det ändå skulle bli aktuellt med ett partiellt adekvansbeslut mot bakgrund av att detta som sagt är unilateralt. Det ska emellertid noteras att med utgångspunkt i en översatt GDPR till brittisk rätt skulle förmodligen inte detta vara nödvändigt. Förutsatt att det inte är påkallat utifrån de problem som konstaterats i förhållande till det traditionella adekvansbeslutet ovan. Vad Storbritannien skulle kunna göra är att använda den amerikanska och kanadensiska lösningen som argument för att speciallösningar är motiverade i speciella situationer. Dock, med hänsyn till EU:s upprepade konstateranden är det GDPR som gäller och inte något utöver detta. Överföringarna mellan EU och Storbritannien skulle således endast omfatta specifika sektorer i den mån man följde dessa modeller. Det skulle av allt att döma

[374] Europeiska kommissionen, 2017, sidorna 9 – 10.
[375] GDPR, artikel 45.1.
[376] Minister of Justice, Personal Information Protection and Electronic Documents Act, §§ 2 och 4, 2018.

innebära en sämre situation i förhållande till ett vanligt adekvansbeslut vad angår arbete för aktörerna, dels i fallet med självcertifiering, dels också i den mån företaget av någon anledning skulle hamna utanför den specifika sektorn. I det senare fallet vore man hänvisad till övriga tredjelandslösningar i GDPR, vilka ska behandlas i det följande.

6 Hur skulle överföringen av betaltjänstens insamlade personuppgifter från EU till Storbritannien se ut om ingen typ av adekvansbeslut kommer till stånd?

Ett adekvansbeslut verkar vara vad man har att vänta som resultat från förhandlingar mellan EU och Storbritannien i den mån Storbritannien anses uppnå adekvat skyddsnivå. Dock finns en risk att ett sådant inte kommer på plats, särskilt inte precis i tid för Storbritanniens utträde om det blir en övergångsperiod. Utan övergångsperiod kommer ett sådant beslut med all säkerhet inte ha hunnit tas. Mot bakgrund av detta är det sannolikt att aktörer i EU och Storbritannien kommer att behöva gardera sig och hitta andra lösningar för att föra över data till Storbritannien. De övriga lösningar som finns att tillgå i GDPR, bortom adekvansbeslutet, är lämpliga skyddsåtgärder och undantag i särskilda situationer.[377] Bindande företagsbestämmelser enligt artikel 47 är däremot inte tillämplig i typfallet eftersom företaget är en tredje part, således lämnas denna utanför min utredning.[378] I detta kapitel reds lämpliga skyddsåtgärder först ut översiktligt med standardavtalsklausuler som fokus, följt av en mer djupgående redogörelse för artikel 49 och samtycket. Samtycket väljs ut av skäl som redan nämnts.[379] Anledningen till att lämpliga skyddsåtgärder endast behandlas översiktligt är att artikel 46 innehåller många olika delar, vilka påverkar aktörerna på likartade sätt. På grund av detta går jag inte in på djupet i varje enskild del och kommenterar främst standardavtalsklausulerna.

6.1 Lämpliga skyddsåtgärder enligt artikel 46 GDPR

I den mån det inte finns något adekvansbeslut att luta sig mot för tredjelandsöverföring av personuppgifter är den därpå följande möjligheten till överföring lämpliga skyddsåtgärder. För att det ska vara tillåtet att överföra genom att vidta sådana åtgärder krävs också att det i tredjelandet finns rättigheter i lag för den individ vars uppgifter överförs, liksom effektiva rättsmedel.[380] Man behöver dessutom, liksom i alla andra fall följa GDPR i övrigt.[381] Artikel 46 i sig består av en uppräkning av vad som kan utgöra lämpliga skyddsåtgärder. Där nämns: rättsligt bindande och verkställbart instrument mellan offentliga myndigheter, bindande företagsbestämmelser i enligt artikel 47, standardavtalsklausuler från kommissionen, standardavtalsklausuler godkända av kommissionen framtagna av en nationell tillsynsmyndighet, godkänd uppförandekod enligt artikel 40, samt godkänd certifieringsmekanism enligt artikel 42.[382] Utöver det som räknas upp i andra punkten i artikeln noteras även i artikelns tredje punkt att, med reservation för att tillåtelse från

[377] GDPR, artikel 46 och 49.
[378] GDPR, artikel 47.1 a; Drooms Global, 2018, https://drooms.com/en/blog/gdpr-disadvantages-of-model-clauses-and-binding-corporate-rules, använd den 29 november 2018.
[379] Se avsnitt 1.1.
[380] GDPR, artikel 46.1.
[381] GDPR, artikel 44.
[382] GDPR, artikel 46.2 a – f.

tillsynsmyndighet krävs, skyddsåtgärder också får uttryckas genom: avtalsklausuler mellan privata aktörer och bestämmelser i administrativa överenskommelser mellan offentliga aktörer.[383]

Standardavtalsklausuler innebär att kommissionen, eller en tillsynsmyndighet efter godkännande, har antagit beslut om särskilda avtalsklausuler.[384] Dessa kan sedermera inkorporeras i avtal mellan en aktör som vill föra över personuppgifter och en annan som befinner sig i tredjeland. Genom att följa dessa uppfyller överföringsproceduren och behandlingen av personuppgifter de krav som ställs i unionen på skydd för privatpersoner.[385] Dock, under förutsättning att det finns lagstadgade rättigheter för individen och effektiva rättsmedel. Hittills har inte kommissionen antagit några dylika klausuler på grundval av GDPR, endast med direktiv 95/46 som bas.[386] Potentiellt skulle en tillsynsmyndighet i EU kunna anta standardavtalsklausuler, i brist på desamma direkt från kommissionen, för att säkra överföringen av personuppgifter till Storbritannien från EU efter brexit. Dock måste sådana standardavtalsklausuler godkännas av kommissionen,[387] liksom att styrelsen måste avge ett yttrande.[388] Även om standardavtalsklausuler skulle kunna framstå som en förhållandevis enkel lösning i det fall det inte finns något adekvansbeslut, måste alltså även dessa behandlas av en EU-instans innan aktörerna skulle kunna använda sig av dem. Med styrelsens yttrande avses att europeiska dataskyddsstyrelsen ger sin syn på det utkast som tillsynsmyndigheten tagit fram för standardavtalsklausuler och dess förenlighet med GDPR.[389] I den mån myndigheten sedan inte skulle rätta sig efter styrelsens yttrande ska denna istället anta ett bindande beslut, för att säkerställa förenlighet med GDPR.[390]

I anslutning till standardavtalsklausulerna ska också nämnas att dessa främst är anpassade efter mindre företag.[391] Därför är det också troligt, eftersom betaltjänsten i typfallet, i likhet med PayPal,[392] är ett större företag, att standardavtalsklausulerna skulle generera större men för detta än om det vore ett litet företag. Som liten aktör med förhållandevis få avtal blir inte förhandlingen av standardavtalsklausuler lika omfattande som i fallet med ett företag som har många fler avtal som behandlar personuppgiftsöverföringar. Avtalsförhandlingar och efterlevnaden av det man avtalar om medför kostnader, varför standardavtalsklausuler kan bli besvärliga för större aktörer.[393]

Även vad gäller övriga lämpliga skyddsåtgärder gäller att processen måste ske via styrelsen.[394] Alla de olika åtgärderna innebär således att aktörerna måste sköta en stor del av arbetet själva, genom

---

[383] GDPR, artikel 46.3 a – b.
[384] Europeiska kommissionen, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en, använd den 22 december 2018.
[385] Europeiska kommissionen, Kommissionens beslut av den 5 februari 2010 om standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredjeland i enlighet med Europaparlamentets och rådets direktiv 95/46/EG (EUT L 39, 12.2.2010, s. 5–18), 2010, artikel 1.
[386] Europeiska kommissionen, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en, använd den 22 december 2018.
[387] GDPR, artikel 46.2 d.
[388] GDPR, artikel 64.1 d.
[389] GDPR, artikel 63 och 64.
[390] GDPR, artikel 65.1 c.
[391] Drooms Global, 2018.
[392] Reuters, 2018.
[393] Drooms Global, 2018; Kommerskollegium, *No Transfer, No Trade - the Importance of Cross-Border Data Transfers for Companies Based in Sweden*, 2014, sidan 19.
[394] GDPR, artikel 42.1, 42.5, 46.2 d, 64.1 b – e, och 65.1 c.

att införa klausuler i sina avtal, tillämpa godkänd uppförandekod, godkänd certifiering et cetera. Samtidigt som denna administrativa börda läggs på aktörerna behöver dessa fortfarande invänta yttranden från styrelsen i samtliga fall, liksom godkännande i förekommande fall. Poängen jag vill göra är att det i mångt och mycket blir en dubbel förlust för aktörerna. De bär både en stor börda administrativt *och* är beroende av offentligt agerande på något sätt.

6.1.1 Slutsatser och funktionen för betaltjänsten och företaget av lämpliga skyddsåtgärder

Slutsatsvis kan sägas att lämpliga skyddsåtgärder är ett alternativ till adekvansbeslut i så måtto att det är ett sätt för betaltjänsten att föra över uppgifter till företaget, för vilket det dessutom inte krävs ett förfarande från kommissionen i förhållande till tredjelandet i fråga. Istället har en stor del av den administrativa bördan flyttats över till betaltjänsten och företaget. Detta innebär emellertid konsekvenser för betaltjänsten och företaget i Storbritannien. Först och främst riskerar i vart fall standardavtalsklausuler att medföra stora kostnader för betaltjänsten, i och med klausulernas anpassning till mindre företag. Här ska också anmärkas att de standardavtalsklausuler som kommissionen antagit ännu bara rör direktivet som föregick GDPR. Än så länge finns alltså inga dylika från kommissionen angående den gällande regleringen. Lämpliga skyddsåtgärder är således ett sätt för betaltjänsten och företaget att fortsätta att dela personuppgifter efter brexit, om än ett i viss mån trögt sådant eftersom det är beroende av beslut från myndigheter, eller kommissionen. Utöver det är lämpliga skyddsåtgärder en lösning som bjuder en del motstånd för betaltjänsten och företaget, eftersom de får bära den administrativa bördan – det blir i viss mån en dubbel förlust.

Här ska också erinras om varför beslutet i förhållande till USA kan kallas en hybrid mellan adekvansbeslut och lämpliga skyddsåtgärder. Den mekanism som ställs upp däri påminner om det förra, likväl som det senare eftersom den både innefattar beslut om skyddsnivån och certifiering där aktörerna bär bördan. Något som är till Storbritanniens fördel i relation till artikel 46 är att det krav på lagstadgade rättigheter och effektiva rättsmedel som ställs upp. Man bör kunna uppnå detta, dock med förbehåll för de justeringar som behövs i GDPR, liksom eventuellt i förhållande till stadgan, enligt vad som redovisats anslutning till adekvansbeslutet.

6.2 Undantag i särskilda situationer enligt artikel 49 GDPR

När inga andra medel finns att tillgå, när varken adekvansbeslut eller lämpliga skyddsåtgärder, kunnat fattas eller vidtas finns en sista möjlighet för överföring till tredjeland – undantag i särskilda situationer enligt artikel 49 GDPR. Existerar varken adekvansbeslut eller lämpliga skyddsåtgärder, och betaltjänsten inte kan uppfylla i vart fall ett av villkoren i artikel 49, faller man dock tillbaka på huvudregeln, det vill säga förbudet i artikel 44.[395] Artikeln stadgar att samtycke kan vara en legitim grund, liksom bland annat fullgörande av avtal mellan individen och den personuppgiftsansvarige och av nödvändigt samhällsintresse. Jag väljer här att fördjupa mig i samtycke, av skäl som redan lyfts i avsnitt 1.1. Här ska bara påminnas om att den främsta anledningen till detta är att samtycke förmodligen är det mest välkända undantaget och, med hänsyn till individens benägenhet att inte läsa villkoren, förmodligen det mest användbara.

[395] GDPR, artikel 49.1.

Som nämnts i genomgången av GDPR:s funktion inom EU är samtycke en av grunderna på vilken behandling av personuppgifter kan vara laglig,[396] under förutsättning att samtycket uppfyller kraven i artikel 4.11 GDPR.[397] Villkoren för att samtycket ska accepteras som grund är vidare att den personuppgiftsansvarige, betaltjänsten, ska kunna visa att samtycke lämnats och att det kan särskiljas från annan information vad samtycket avser.[398] Dessutom måste individen ovillkorligt kunna återkalla sitt samtycke och hänsyn tas till om samtycket verkligen är frivilligt i den mån det åtföljs av fullgörande av ett avtal.[399] I det senare fallet är det av särskild vikt om avtalets fullgörande villkorats av samtycket till behandling av personuppgifter som egentligen inte är nödvändig.[400]

I skälen till samtycke för behandling i *tredjeland* anges att undantagen i de särskilda situationerna främst bör vara legitima i fall som gör dem nödvändiga för allmänna intressen.[401] I förhållande till vad som gäller inom unionen är detta ställningstagande en skillnad. Dock, trots vad som anges i skälet, finns inget krav på att så ska vara fallet i själva artikeln. Även om det därför skulle vara önskvärt att varje överföring bortom adekvansbeslutet och lämpliga skyddsåtgärder hade ett högre syfte än ett rent kommersiellt är detta icke desto mindre inget krav. Man kan således använda sig av samtycke som undantag, även om det inte finns ett allmänt intresse bakom. Trots antydan till en annorlunda syn på detta i skälet, är samtycket här alltså inte skilt från det inom unionen. Vad som emellertid framhävs tydligt i de riktlinjer som finns för artikel 49 GDPR är att det rör sig om just *undantag* som inte får bli regel.[402] För att få använda sig av undantagen tar WP29 upp avsaknad av andra överföringssätt enligt kapitel V GDPR som motiv; samtycket i artikel 49.1 a GDPR är ett undantag tillämpligt i avsaknad av reglerna om adekvat skyddsnivå och lämpliga skyddsåtgärder.[403] Dock utesluter inte ordalydelsen i GDPR att man använder sig av samtycket i artikel 49.1 GDPR trots att andra möjligheter till överföring existerar.[404] WP29 understryker emellertid att undantagen i artikel 49 endast ska utnyttjas i den mån adekvansbeslut eller lämpliga skyddsåtgärder inte fattats eller vidtagits.[405] Av WP29:s riktlinjer att döma bör man därför, trots samtyckets undantagskaraktär, mer eller mindre regelmässigt kunna använda detta så länge lösningar enligt artikel 45 eller 46 GDPR inte existerar – man begränsar inte grunden i vidare mån än så.[406]

De unika delarna för tredjelandssamtycket är emellertid, utöver dess undantagskaraktär, dels att detta ska vara *uttryckligt* och dels den *ytterligare information* man måste lämna för att det ska vara giltigt.[407] När samtycket rör ett tredjeland vars skyddsnivå varken har blivit föremål för något beslut från kommissionen eller för lämpliga skyddsåtgärder måste man informera om vilka risker detta kan medföra för individen.[408] Likt den kritik som gäller generellt för informerat samtycke kan här

396 GDPR, artikel 6.1 a.
397 Samtycket ska vara frivilligt, specifikt, informerat och otvetydigt.
398 GDPR, artikel 7.1 – 2.
399 GDPR, artikel 7.3 – 4.
400 GDPR, artikel 7.4.
401 GDPR, skäl 112.
402 WP29, 18/EN WP 261 Guidelines on Article 49 of Regulation 2016/679, 2018, sidan 4.
403 WP29, 2018, sidorna 3 – 4. Se även riktlinjerna för hur samtycket skulle bedömas enligt motsvarande artikel i den tidigare regleringen, WP29, 2093/05/EN WP114 Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, 2005.
404 Jämför GDPR, artikel 45.7 och artikel 49.1.
405 WP29, 2018 sidorna 3 – 4.
406 WP29, 2018 sidorna 3 – 4.
407 GDPR, artikel 49.1 a.
408 GDPR, artikel 49.1 a.

ifrågasättas om det över huvud taget går att ha ett *informerat* samtycke när det gäller överföring till tredjeland, här antar dock frågan ytterligare en skepnad. I fallet med samtycke finns ingen kvalitetskontroll av tredjelandets reglering kring databehandling från EU. Beroende på vilken insyn det går att ha i landets reglering kring personuppgifter, till exempel regler om myndigheters tillgång till lagrade uppgifter,[409] går det att informera i olika grad om vad riskerna innebär. I den mån det inte går att veta vidden av vilken tillgång myndigheter har till lagrade personuppgifter, kan man då tala om ett informerat samtycke om samtycke ges?

Storbritannien kommer förvisso att ha en mycket EU-nära lagstiftning, åtminstone till en början, med reservation för de problem man potentiellt har med stadgan. Detta gör att problemet med insyn i de risker det kan innebära att föra över till Storbritannien efter utträdet inte går att avfärda alldeles enkelt. Dock är detta en ny nivå av samma problem som finns inneboende generellt i samtyckeskonstruktionen. Av den anledningen finns det egentligen inget som säger att tredjelandsdimensionen skulle ställa till *mer* problem än inom unionen – aktörerna vet förmodligen ändå inte fullt ut vilken behandling som kan bli aktuell.[410] Således är man knappast skyldig att informera om det man inte kan veta, även om man förvisso kanske borde informera om att man inte vet. Slutsatsen att detta inte bereder mer problem för betaltjänsten än vad som gäller för det informerade samtycket inom unionen ligger därför nära tillhands. Det måhända att det rent kvantitativt finns fler parametrar att informera om i detta senare fall än inom EU, det är emellertid ett marginellt problem, eftersom man ändå får överföra personuppgifterna när man fått samtycket.

Problemet med den andra unika delen i tredjelandssamtycket, det *uttryckliga* samtycket, är att det är svårt att avgöra på vilket sätt detta skiljer sig från samtycket som gäller inom EU. WP29 har i sin instruktion till tolkningen av samtycke enligt GDPR uttryckt det som att det handlar om hur den enskilda meddelar sitt samtycke – det måste vara uttryckligt.[411] Detta beskrivs som att man som aktör skulle kunna tillämpa tvåstegsautentisering, alltså till exempel skicka ett mejl till individen för samtycke för att detta sedan ska bekräftas med ytterligare en kod man får skickad till sin telefon.[412] Samtidigt konstaterar man emellertid att även om ett skriftligt samtycke är att föredra, särskilt för det uttryckliga samtycket, ställer GDPR inte upp några krav på hur detta ska lämnas, det kan alltså principiellt vara muntligt.[413] Ett annat exempel på hur det uttryckliga samtycket kan lämnas är genom att man kryssar i rutor, där det måste vara klart för individen att det är samtycke till behandling det avser.[414] Här är det svårt att se skillnaden mot samtycket inom EU, vilket också kan bestå i att kryssa i en ruta.[415]

Med utgångspunkt i att samtycket egentligen inte bereder så mycket problem för aktörerna skulle denna situation kunna inbjuda till att använda samtycket i artikeln mer regelmässigt än undantagsvis. Tilläggas ska att samtycket enligt artikel 49 GDPR inte påverkas av att ett adekvansbeslut skulle dras tillbaka, här finns således en hållbarhetsaspekt som kan vara attraktiv.[416]

[409] Jämför Schrems-målet.
[410] Berinato, 2018, sidan 4.
[411] WP29, 2017, sidan 18.
[412] WP29, 2017, sidan 19.
[413] WP29, 2017, sidan 18.
[414] WP29, 2017, sidan 19.
[415] GDPR, skäl 32.
[416] GDPR, artikel 45.7.

En reflektion från min sida är att aktörerna eventuellt på dessa grunder skulle kunna förvänta sig noggrannare tillsyn än i andra fall i GDPR. I den mån man fått ett samtycke till överföring när det inte finns någon annan lösning enligt GDPR tillgänglig vore det emellertid svårmotiverat att vid tillsyn hävda att överföringen är otillåten. Detta eftersom de särskilda situationer som motiverar undantagen i artikeln inte specificerats. En tillsynsmyndighet har emellertid befogenhet att förelägga om att överföring till tredjeland ska avbrytas,[417] något som skulle kunna öka osäkerheten i denna grunds stabilitet. Utöver potentiellt mer tillsyn ska också tilläggas att det största osäkerhetsmomentet i utnyttjande av samtycke är att den enskilda kan dra tillbaka detta när som helst,[418] alternativt att individen över huvud taget inte lämnar sitt samtycke.

6.3 Slutsatser och funktionen för betaltjänsten och företaget av samtycket enligt artikel 49.1 a GDPR

Även om det således ställs upp ytterligare krav på samtycket inom ramen för artikel 49.1 a GDPR än det gör inom unionen, är det inte klart huruvida dessa krav *egentligen* innebär något ytterligare för betaltjänsten. Man informerar om de risker som finns med samtycke till behandling i ett land vars skyddsnivå inte blivit föremål för granskning och man ber om samtycket genom rutor att kryssa i med tillhörande otvetydig text om att det rör sig om samtycke till behandling i detta land. Det verkar egentligen inte innebära mer än så. Den kritik som riktats mot samtyckeskonstruktionen handlar snarare om att det aldrig går att uppnå ett informerat samtycke, än på vilket sätt detta kan användas för att föra över uppgifter till tredjeland. Man ska som aktör förvisso fortfarande uppfylla övriga krav enligt GDPR och man behandlar personuppgifterna under skadeståndsansvar.[419] Att uppfylla övriga krav enligt GDPR i fallet med ett tredjeland kan vara problematiskt i sig; den enskilda har långtgående rättigheter vilka man naturligtvis inte får bryta mot som aktör.[420] Att föra över uppgifter till ett land som till exempel inte har en oberoende tillsynsmyndighet, förefaller emellertid inte vara ett problem så länge den personuppgiftsansvarige informerar om riskerna med detta.[421]

Slutsatsvis kan sägas att för att föra över personuppgifter till Storbritannien, i den mån varken adekvansbeslut eller andra mekanismer finns på plats för att garantera skyddsnivån, finns ändå samtycke som ett undantag för betaltjänsten och företaget. Även om det rör sig just om ett undantag och därför inte ska anta skepnad av regel, förefaller inte denna grund mot bakgrund av utredningen ovan vara förenad med mycket högre krav än vad som gäller inom unionen. Man ska uppfylla de övriga krav som ställs upp enligt GDPR, man ska informera om de ytterligare risker överföringen innebär och samtycket ska vara uttryckligt. Eftersom samtyckets karaktär av undantag inte är villkorat utifrån att det bara får ske i den mån överföringen är begränsad i sig,[422] är det dock inte klart hur undantagskaraktären tar sig uttryck för betaltjänsten. Något krasst kan man därför hävda att med ytterligare information och eventuellt ett i någon mån tydligare uttryckt samtycke, fungerar egentligen samtycket till behandling i tredjeland som samtycket inom unionen. Dessutom verkar aktörerna, av allt att döma, kunna tillämpa detta närmast regelmässigt så länge

[417] GDPR, artikel 58.2 j.
[418] GDPR, artikel 7.3.
[419] GDPR, artikel 44; WP29, 2017, sidan 19; GDPR, artikel 82.
[420] WP29, 2018, sidorna 3 – 4.
[421] WP29, 2018, sidorna 3 och 8.
[422] Jämför GDPR, artikel 49.1 stycke 2.

adekvansbeslut eller lämpliga skyddsåtgärder inte finns att tillgå. Det utnyttjande detta inbjuder till skulle eventuellt kunna motivera en mer nitisk tillsyn för att motverka regelmässigt användande av undantaget. Det skulle förvisso vara svårt för en tillsynsmyndighet att angripa regelmässigheten i den mån alternativen enligt artikel 45 och 46 GDPR inte är tillgängliga. Den nitiska tillsynen är emellertid endast en tanke från min sida och inget det faktiskt finns tecken på.

Den viktigaste parametern att komma ihåg med samtycket är emellertid att det finns ett än större osäkerhetsmoment i denna lösning än för adekvansbeslutsfallet. Adekvansbeslutet kan dras tillbaka i den mån skyddsnivån inte längre uppfylls.[423] Samtycket däremot ska för att över huvud taget vara giltigt kunna dras tillbaka när som helst, *utan att några skäl behöver anges*.[424] Individen äger sitt samtycke. Det innebär naturligtvis också att hen kan välja att inte lämna det. Dessa sista omständigheter innebär att det kanske inte vore stabilt för betaltjänsten och företaget att bygga all sin överföring på samtycke i denna bemärkelse. Här ska dock påminnas om att individen oftast är benägen att samtycka; hen läser sällan villkoren som gäller för samtycket.[425]

7 Analys utifrån de möjliga alternativen – blir det någon skillnad för betaltjänsten och företaget i förhållande till situationen inom unionen och betyder det i sådant fall ett sämre flöde?

I detta avsnitt analyserar jag de olika delarna ovan i ljuset av situation noll. Blir det någon skillnad för aktörerna i tredjelandsfallen i förhållande till situationen i unionen och i sådant fall, hur tar sig skillnaden uttryck? Innebär skillnaden att flödena av personuppgifter kommer att försämras i förhållande till GDPR:s funktion i EU? Alternativen som tagits upp i utredningen ovan ska här att analyseras, för att genom detta till sist kunna dra en slutsats avseende vad Storbritannien som tredjeland egentligen innebär för personuppgiftsflödena – inte minst för aktörerna.

7.1 Adekvansbeslutet och situation noll

Ovan har jag redan redogjort för adekvansbeslutets själva funktion. Väl på plats ska detta, i dess originaltappning, innebära att flödena från betaltjänsten till företaget fungerar som om Storbritannien aldrig hade lämnat EU. Alltså skulle de personuppgifter som rör sig från unionen till Storbritannien flöda utan hinder, precis som i situation noll. Denna funktion stadgas direkt i artikel 45.1 GDPR. När tredjelandet uppfyller de krav på skyddsnivå som ställs enligt adekvansbeslutet och detta beslut väl har tagits och gått igenom övrig granskning, skiljer sig således inte flödena från situation noll. Därför finns inget i adekvansbeslutets konstruktion i sig som ställer upp mer hinder för betaltjänsten och företaget vilka skulle innebära ett sämre flöde.

Adekvansbeslutets svagheter och osäkerhetsmoment ligger istället utom dess faktiska funktion. Först och främst är det processen fram till ett beslut. Processen är beroende av en politisk vilja, vilken EU förvisso enligt vissa uttalanden verkar ha,[426] liksom att den kan ta tid,[427] om inte annat

[423] GDPR, artikel 45.5.
[424] GDPR, artikel 7.3.
[425] Bechmann, 2014, sidan 22.
[426] Politiska deklarationen, sidan 4.
[427] Jämför beslutet i förhållande till Japan, Europeiska kommissionen, 2018, http://europa.eu/rapid/press-release_IP-18-5433_en.htm, använd den 13 december 2018.

till slutet av 2020.[428] Mot bakgrund av det skulle betaltjänsten och företaget behöva andra lösningar fram till beslutet. Utöver den tid det kan ta innan beslutet finns på plats finns dessutom ytterligare en svaghet. I den mån Storbritannien inte längre lever upp till den adekvata skyddsnivån och beslutet dras tillbaka av kommissionen försämras flödena minst sagt avsevärt. För det fallet är det istället förbudet i artikel 44 GDPR som blir gällande och flödena måste avbrytas om betaltjänsten och företaget inte har andra lösningar på plats. På denna grund skulle man kunna ifrågasätta adekvansbeslutets egentliga värde, även om man inte ska underskatta beslutet när konstruktionen och funktionen väl är i bruk.

I förhållande till hinder för flödena och situationen i unionen är det således inte adekvansbeslutet när det väl finns på plats som bjuder motstånd. Istället är det dess tillbakatagande och den beslutslösa situationen före som är adekvansbeslutets problem. Det förbud som gäller, bortsett från övriga lösningar i GDPR, som framförallt kan bli ett problem vid ett mer eller mindre plötsligt tillbakadragande, är själva definitionen av ett hinder mot fria flöden. Inom unionen, där man genom GDPR gemensamt har en och samma skyddsnivå är förbud ackompanjerat av avbrott i flödena inte ens en risk. Denna skillnad beror förstås på att man i unionen säkrat en gemensam skyddsnivå genom förordningen. Man ska emellertid inte glömma bort att flödena i unionen heller inte är beroende av den ensidighet som beslutet om adekvat skyddsnivå är. Betaltjänsten och företaget behöver således i situation noll inte oroa sig för att det ska råda osäkerhet kring flödena, så länge man följer GDPR. I adekvansbeslutsfallet finns den risken, trots att betaltjänsten och företaget för att få föra över även i denna situation måste följa övriga delar i förordningen.[429]

Möjligheten för kommissionen att dra tillbaka sitt beslut är en garanti för de individer vars personuppgifter behandlas. Om Storbritannien inte längre skulle uppfylla adekvat skyddsnivå för personuppgifterna ska inte heller flödena dit stå fria, utan ska förbjudas enligt huvudregeln. Sett till GDPR:s syften, att skydda individen och fria flöden av personuppgifter,[430] prioriterar man här det förra. Det kan i och för sig anses vara befogat att inte prioritera aktörernas intresse av oavbrutna flöden för handel i ett sådant sammanhang, för att skydda den typiskt sett svagare parten.[431] Vad som emellertid visar sig här är att när adekvansbeslutet finns på plats och fungerar finns ingen skillnad i hur *flödena ser ut* i förhållande till situation noll. Däremot finns en skillnad i att adekvansbeslutet har en ensidig karaktär och därmed också en inneboende osäkerhet för betaltjänsten och företaget. Även om flödena som sådana inte skulle påverkas skulle därför aktörernas agerande ändå behöva anpassas till den osäkerhet adekvansbeslutet bjuder. Vad jag åsyftar är att innan ett beslut är på plats behöver betaltjänsten och företaget ändå basera sin överföring på någon annan grund, liksom potentiellt förbereda en annan lösning för det fall kommissionen skulle ta tillbaka beslutet.

Den *egentliga skillnad* som uppstår med adekvansbeslutet är att detta således är ensidigt villkorat, vilket inte gäller i unionen. Den osäkerhet som ensidigheten betyder för aktörerna kan emellertid generera beteenden hos dem som får adekvansbeslutet att skilja mer från unionen än just bara detta. Om adekvansbeslutets flöden kommer med priset av ökad administrativ börda och kostnader

[428] Politiska deklarationen, sidan 4.
[429] GDPR, artikel 44.
[430] GDPR, artikel 1.1.
[431] Jämför Europeiska kommissionen, Insyn i EU-politiken: Konsumentskydd, 2016, sidan 3.

för att vidta säkerhetsåtgärder, liksom att lösa situationen fram till beslutet, innebär det att flödena i detta fall *skiljer sig mer än vid första anblick*. För att åtnjuta de fria flödena under adekvansbeslutet, med någotsånär säkerhet inför framtiden måste aktörerna gardera sig. De facto innebär detta att adekvansbeslutet kommer med fler betungande parametrar för betaltjänsten och företaget att ta hänsyn till och flödet är således, mot bakgrund av detta, *sämre än det fria, bättre flöde som finns i unionen*.

Dessutom innebär ett adekvansbeslut, även om en del i detta är att bedöma hur Storbritannien samarbetar med medlemsstaternas tillsynsmyndigheter, att betaltjänsten och företaget förlorar möjligheten att utnyttja OSS i förhållande till Storbritannien. Detta innebär, till skillnad från inom EU, att man kommer att behöva vända sig till både ICO i Storbritannien och till den ansvariga tillsynsmyndigheten där man har sitt huvudsakliga verksamhetsställe. Inte heller individen som vill kontakta en tillsynsmyndighet kommer att kunna välja vilken medlemsstat som helst för detta när ärendet rör tredjeland. ICO ståendes utanför OSS får således det utfallet att betaltjänsten och företaget kommer att behöva ta kontakt med ytterligare en tillsynsmyndighet, istället för bara den ansvariga. Detta kan naturligtvis påverka flödena dem emellan negativt, inte minst med hänsyn till den ytterligare tid ett administrativt förfarande kan ta. Dessutom finns inte samma infrastruktur kvar för samarbetet mellan tillsynsmyndigheterna när ICO står utanför samarbetsmekanismen i GDPR. Det i sig kan också ha negativ inverkan på hur personuppgifter kan flöda eftersom tillsynsmyndigheterna måste finna nya vägar för samarbete med tidsåtgång som följd. Samarbetet mellan ICO och medlemsstaternas tillsynsmyndigheter efter brexit bör således också bereda betaltjänsten och företaget ökad administrativ börda och tidsåtgång och således sämre flöden.

Hur *mycket sämre* detta blir har inte varit föremål för min analys. Däremot kan, mot bakgrund av de kostnader som uppstår vid till exempel avtalsförhandling,[432] adekvansbeslutet minst sagt innebära ökade kostnader för betaltjänsten och företaget. Även om det utifrån mina ramar är svårt att säga hur mycket sämre flödena blir visar ändå analysen att ett adekvansbeslut, som vid första anblick kan antas ge likvärdiga flöden, i själva verket försämrar dem. På detta sätt blir resultatet av ett Storbritannien utanför unionen, försämrade dataflöden genom ökade åtgärder från aktörerna, trots att det rör det fall av undantag från överföringsförbudet i artikel 44 GDPR som egentligen inte ska generera ytterligare åtgärder för betaltjänsten och företaget.[433]

7.2 Vitboken och situation noll

Det som skiljer vitboken från adekvansbeslutet är såväl det ramverk för personuppgiftsutbyte man vill konstruera, som samarbetet med ICO kvar i OSS. Vad som är tydligast ur flödessynpunkt är emellertid att den svaghet som adekvansbeslutet bjuder inte längre finns kvar enligt vitboken. Man skapar istället en större stabilitet, eftersom kommissionen inte kan dra tillbaka ett beslut ensidigt på samma sätt. Detta vore, om än kanske inte ett reellt alternativ av skäl som förklarats ovan,[434] en stabilare lösning för betaltjänsten och företaget.

Genom att ta bort det osäkerhetsmoment ensidigheten ger, betyder att behovet av säkerhetsåtgärder för ett eventuellt återtagande inte finns. Mot bakgrund av att man vill bygga sitt

[432] Kommerskollegium, 2014, sidan 19.
[433] GDPR, artikel 45.1; Europeiska kommissionen, 2017, sidan 6.
[434] Se avsnitt 4.3.

avtal med EU på adekvansbeslutskonstruktionen finns anledning att anta att flödena som sådana kommer att vara fria tack vare adekvat skyddsnivå. Detta innebär att det alternativ som vitboken i sådant fall ställer upp är ett adekvansbeslut utan ensidighet och således utan den osäkerhet det genererar. I förhållande till situation noll blir flödena således inte sämre annat än de åtgärder som måste vidtas från betaltjänsten och företaget fram till dess man faktiskt kommit överens om ett avtal, alternativt detta bryts eller löper ut. Även om det naturligtvis finns en risk att en part skulle bryta avtalet, bör det emellertid inte vara lika troligt att så skulle ske som att ett adekvansbeslut ensidigt skulle tas tillbaka av kommissionen. Detta mot bakgrund av att ett avtalsbrott typiskt sett är förenat med någon påföljd, vilket bör vara tanken även i Storbritanniens förslag. På så sätt skulle båda parter ha incitament att fortsatt ha en överenskommen skyddsnivå och den ena skulle inte ensidigt kunna ångra sin del i avtalet utan att bryta mot detsamma. På samma sätt får det emellertid antas att avvikelser från den skyddsnivå som ska gälla enligt avtalet i och för sig också skulle innebära avtalsbrott. På grund av påföljderna skulle detta dock ligga längre bort än i adekvansbeslutsfallet.

Utifrån detta vore alltså avtalet mellan Storbritannien och EU för personuppgiftsöverföring närmare de fria flödena i situation noll än adekvansbeslutet eftersom de ökade ansträngningarna för betaltjänsten och företaget skulle utebli. Dessutom skulle ett fortsatt deltagande i OSS innebära en klar fördel för betaltjänsten och företaget i myndighetskontakter. Även här skulle alltså avtalet bära med sig större likhet med situation noll än adekvansbeslutet. Ingen ökad börda skulle falla på aktörerna för att finna den ansvariga myndigheten, som annars skulle gälla vid överföring till tredjeland.

Mot bakgrund av ovanstående omständigheter vore de enda problem denna lösning skulle vara behäftad med i förhållande till situation noll tiden före avtalet där andra lösningar måste råda, liksom risken för avtalsbrott och tiden när detta löpt ut. Avtalsbrottet är emellertid en smärre risk i förhållande till ensidigheten hos ett adekvansbeslut med hänsyn till konsekvenser som rimligen följer på brott mot ett ömsesidigt avtal. Dessutom skulle avtalets utlöpande vara något man kunde förbereda sig för i tid och således skulle det inte orsaka behov av akuta åtgärder. Därför skulle flödena bara bli marginellt sämre än i förhållande till situation noll och detta framstår därför som ett bättre alternativ än adekvansbeslutet.

Här ska emellertid erinras om något som nämnts ovan[435] och som är en starkt bidragande orsak till att jag svårligen ser vitbokens lösningar som ett reellt alternativ. EUD skulle kunna ogiltigförklara ett sådant avtal, likt vad man gjorde i Schrems-målet, eftersom kommissionen inte skulle ha agerat i enlighet med GDPR och således lagstridigt.[436] Kommissionen skulle därför inte få tillämpa avtalet ur en EU-rättslig synvinkel. Rimligtvis skulle detta innebära att man skulle bryta avtalet med Storbritannien och få stå för de konsekvenser detta skulle medföra mellan de båda parterna. Poängen med detta är att risken att EUD skulle ogiltigförklara ett sådant avtal är så överhängande i ljuset av dess övervakande funktion, att det i stort sett skulle innebära att betaltjänsten och företaget *vore tvungna* att vidta andra åtgärder för att säkra sin överföring av personuppgifter. Man skulle alltså snarare än något annat vara säker på att avtalet inte fortsatt skulle gälla. Med hänsyn

[435] Ovan avsnitt 4.3.
[436] FEUF, artikel 263 – 266.

till denna sista omständighet skulle därför flödena enligt vitboken avsevärt försämras för betaltjänsten och företaget. De vore tvungna att lösa flödena helt på egen hand, utan att det man kommit överens om på nivån mellan EU och Storbritannien egentligen hade någon betydelse alls, eftersom EUD med all säkerhet skulle fälla ett sådant avtal.

Vitboken ställd mot situation noll skulle således innebära ett *sämre flöde* än det inom unionen. Så som man föreslår att det skulle fungera från Storbritanniens sida är inte ett verkligt alternativ, eftersom man redan nu ser att EUD inte skulle tillåta detta. Således skulle ett avtal med Storbritannien, snarare än något annat, innebära att betaltjänsten och företaget fick ordna med sina överföringar över EU:s yttre gräns på egen hand. Det skulle vara som om EU och Storbritannien inte hade någon lösning mellan sig över huvud taget, inte ens en ensidig sådan. Även om Storbritanniens lösning enligt vitboken således ser ut som att den skulle leda till många lättnader för aktörerna utifrån sett, innebär den, mot bakgrund av hur EU:s regelverk ser ut raka motsatsen vid en analys av dess konsekvenser.

7.3 Ett partiellt adekvansbeslut och situation noll

Eftersom adekvansbeslutet i detta fall bara är partiellt så innebär det att, utöver de delar som skiljer adekvansbeslutsfallet från ordningen inom EU, gäller beslutet bara en viss sektor och potentiellt bara för aktörer som certifierats. Med ett partiellt adekvansbeslut går man således från fria flöden som gäller i unionen, till flöden som inte bara begränsas av åtgärder som bland annat behöver vidtas från aktörerna till följd av osäkerhet i relation till beslutets bestånd och myndighetskontakter. Det blir dessutom så att flödena begränsas, antingen av att företaget i Storbritannien inte omfattas av den aktuella sektorn, som är risken enligt den kanadensiska modellen, eller av att man måste invänta självcertifiering från företaget, enligt den amerikanska. För det fall man faller inom den sektor som omfattas blir inte skillnaden i förhållande till situation noll någon annan än den i adekvansbeslutsfallet. I den mån så inte är fallet måste man däremot helt och hållet lösa överföringen på egen hand utifrån övriga alternativ i GDPR. För att inte falla tillbaka på förbudet innebär det således att åtgärder måste vidtas med tid och kostnader som följd. Rör det sig istället om ett självcertifieringssystem måste företaget först uppfylla adekvat skyddsnivå, istället för att bara allmänt sett följa lagen i Storbritannien och man hamnar således även här i administrativ börda.

Klart är att båda typerna av partiella adekvansbeslut genererar en skillnad i förhållande till situation noll, vilken resulterar i en försämring av flödena. Utgår man från att man ändå omfattas av relevant sektor i det kanadensiska fallet skiljer sig denna dock inte mer från situation noll än det ordinära adekvansbeslutet och är en mer fördelaktig lösning än självcertifiering. Den senare modellen består i ytterligare ansvar för det administrativa på aktörerna, särskilt på företaget som måste se till att adekvat skyddsnivå uppfylls, innan man kan föra över uppgifter enligt beslutet. Man kan således ifrågasätta, i synnerhet för den amerikanska modellen, vilket incitamentet är att över huvud taget fatta ett sådant beslut när det finns andra snarlika lösningar i andra artiklar i GDPR. Med de snarlika lösningarna avses de lämpliga skyddsåtgärderna, som också innebär ökad administrativ börda för betaltjänsten och företaget. Amerikanska staten står förvisso för en del garantier och tillsyn i sammanhanget, dock, utifrån ett aktörsperspektiv är det svårt att se vad denna typ av beslut fyller för funktion och varför det kallas adekvansbeslut, om än partiellt.

7.4 Lämpliga skyddsåtgärder och situation noll

Som framgår ovan i detta avsnitt tillför tredjelandsöverföring i regel ytterligare förfaranden för aktörerna som innebär att flödet försämras när ett land går från medlemsstat till tredjeland. Lämpliga skyddsåtgärder är inget undantag. Dessutom, i typfallet, tycks konsekvenserna bli än större än om det hade rört sig om ett mindre företag.

För alla åtgärderna i artikel 46 GDPR som är aktuella i detta fall läggs den administrativa bördan i stort sett på aktörerna, med undantag för att det är kommissionen eller tillsynsmyndigheterna som tar fram bland annat standardavtalsklausuler.[437] Det är emellertid aktörerna som ska inkorporera dessa i sina avtal och för betaltjänstens del innebär det att man ska förhandla in dem och komma överens med företaget. I förhållande till situation noll syns bördan tydligt – i det senare fallet behöver företaget bara följa GDPR och inte vidta några egna åtgärder. Samma skillnad uppstår i relation till det ordinära adekvansbeslutet. De lämpliga skyddsåtgärderna måste på något sätt genomföras på aktörsnivå, detsamma gäller uppförandekod, certifiering och avtalsklausuler enligt artikeln. Just vad gäller standardavtalsklausulerna är dessa mer anpassade för mindre företag och en aktör i betaltjänstens storlek beläggs med en stor börda när sådana ska förhandlas i varje enskilt avtal, även om klausulerna som sådana förvisso inte tas fram av betaltjänsten själv.

Till detta läggs också att varje del fortfarande, likt adekvansbeslutet, är beroende av att kommissionen de facto utformar verktygen enligt artikeln, godkänner det som en tillsynsmyndighet tar fram, eller att detta ska behandlas inom ramen för styrelsen. Samtidigt som man alltså har en stor del av den administrativa bördan och potentiellt får ökade kostnader av att verktygen enligt artikeln inte passar alla typer av aktörer är man också beroende av det offentligas bedömning. Således innebär de lämpliga skyddsåtgärderna betungande konsekvenser för betaltjänsten och företaget. Man beläggs med den administrativa bördan i mångt och mycket, med tidsåtgång och därtill ökade kostnader för att få flödena att fungera till Storbritannien. Samtidigt är man beroende av de offentliga aktörerna, nationellt och på EU-nivå för godkännande och yttranden. Som nämnts ovan, blir det en dubbel förlust för aktörerna både i jämförelse med adekvansbeslutet och situation noll och innebär således sämre flöden.

7.5 Undantag i särskilda situationer – samtycke och situation noll

I alla olika fall enligt GDPR måste man fortsatt följa förordningen för att få föra över personuppgifter till tredjeland.[438] De alternativ som sedan ges för överföring till tredjeland innebär *ytterligare åtgärder*, utöver GDPR. I detta avseende skiljer sig samtycke något från de andra delarna i kapitel V GDPR. Även om WP29 är av en annan åsikt,[439] går det enligt min mening att betrakta samtycket som inget annat än en *förlängning* av vad som redan gäller i unionen och således inte en ytterligare åtgärd.

Samtycket innebär att man ska följa förordningen som inom unionen, med det tillägget att samtycket ska omfatta det som stadgas enligt artikel 49.1 a GDPR och inte bara utgöras av den enklare varianten av samtycke enligt artikel 6.1 a GDPR. Den förlängning jag talar om innebär

[437] GDPR, artikel 46.2 c – d.
[438] GDPR, artikel 44.
[439] Europeiska kommissionen, 2017, sidan 3.

således att det är *uttryckligt* samtycke som ska lämnas och att detta ska lämnas först sedan individen *informerats om de risker* som adderas vid överföring till tredjeland. Till skillnad från de andra alternativen innebär därför inte samtycket något egentligt ytterligare förfarande, utan en utvidgning av den rättsliga grund som redan finns inom EU. Med detta inte sagt att samtycket enligt artikel 49 GDPR inte innebär att några ytterligare åtgärder behöver vidtas från aktörernas sida, i förhållande till situation noll.

Vad som emellertid är problemet, alternativt möjligheten, med samtycket är att det egentligen inte är preciserat vad dessa specifika krav för överföring till tredjeland har för betydelse. WP29 exemplifierar det uttryckliga samtycket med att det kan bestå i att kryssa i rutor, precis som samtycket i unionen, om än med också andra exempel som tvåstegsautentisering. I den mån man ändå utgår från att det behövs något ytterligare i individens uttryck av samtycke i detta fall jämfört med EU, framstår i och för sig till exempel tvåstegsautentisering som ett förhållandevis lindrigt alternativ. Det är lindrigt i så måtto att det inte nödvändigtvis betyder samma börda som alternativen ovan. Det innebär förvisso att till exempel tvåstegsautentisering måste tas fram från betaltjänstens sida. Dock bör detta sedan kunna ske automatiserat och således utan den förhållandevis stora administrativa börda man ser i fallen ovan.

Den information som ska lämnas är, mot bakgrund av den ledning som ges av EU, också svårtydd. Denna otydlighet ligger dels i att information i samband med samtycke generellt är något som inte lämnas med enkelhet, dels ligger det i att man beroende på tredjelandet i fråga kan ha svårt att överblicka de ytterligare risker som är förenade med överföring just dit. Oavsett om man ser på situationen före eller efter brexit är det likväl ett problem att varken betaltjänsten eller företaget kan överblicka all den behandling som kan komma att ske med insamlade uppgifter. Denna svårighet är inbyggd i samtyckets struktur och är inget som hindrat överföring tidigare, varken inom eller utom unionen. Därför låter sig det ytterligare informationskrav som finns i artikeln svårligen konkretiseras. Artikeln stipulerar emellertid att man ska informera om de *eventuella* risker överföring skulle kunna innebära när adekvat skyddsnivå eller lämpliga skyddsåtgärder inte finns. I denna formulering ligger förvisso ett krav på att informera, men knappast ett krav på att informera uttömmande, dels för att man som utgångspunkt inte kan det, dels för att tredjelandsöverföringen i sig eventuellt inte möjliggör det. Utifrån detta är min tolkning att informationskravet bör bestå i att betaltjänsten ska informera ”så gott den kan” om de risker det skulle innebära att föra över uppgifter till företaget i Storbritannien när inga andra åtgärder finns vidtagna enligt GDPR.

Mot situation noll står också undantagskaraktären ut som en skillnad. Inte heller denna omständighet är emellertid helt konkret. I den mån det varken finns adekvansbeslut eller exempelvis standardavtalsklausuler att tillgå verkar emellertid undantaget vara mer eller mindre ovillkorligt tillämpligt, varför det i sådant fall skulle stå fritt för aktörerna att använda detta.[440] Dock under förutsättning att hänsyn till övriga GDPR och mänskliga rättigheter tas.[441] Så som reglerna är uppbyggda görs undantaget till ett attraktivt och förhållandevis lättillgängligt alternativ i förhållande till *alla* andra tredjelandslösningar. Särskilt eftersom samtycket, vilket förvisso motiverar skarp kritik, generellt ska vara informerat men knappast faktiskt är det. Icke desto mindre

[440] WP29, 2018, sidan 3 – 4.
[441] GDPR, artikel 44; WP29, 2018, sidan 3 – 4.

finns det som en grund för överföring såväl inom som utom unionen och står således till betaltjänsten och företagets förfogande för att säkra fortsatt överföring till Storbritannien.

Potentiellt innebär grundens relativa lättillgänglighet ett incitament för ökad kontroll från tillsynsmyndigheternas sida. De har behörigheten att göra detta.[442] Detta är emellertid en reflektion från min sida och det finns inga tecken på att någon sådan riktad tillsyn faktiskt görs. I den mån man ändå använder undantaget regelmässigt gör man förstås detta med risk för reaktion från myndighetshåll. Det är emellertid svårt att se hur man från en tillsynsmyndighets sida skulle motivera att användandet av samtycke skulle vara fel i en situation där adekvansbeslut och lämpliga skyddsåtgärder saknas, mot bakgrund av vad som sägs i EU:s vägledningar. Kanske är det troligare att den svaghet som finns i samtyckesgrunden är en större osäkerhet för aktörerna än tillsynen. Risken är att individen tar tillbaka sitt samtycke, detta är emellertid inget som skiljer sig från situationen i EU. Något som däremot fortfarande skiljer sig från EU, även i denna situation, är att man inte längre kommer att kunna utnyttja OSS vid sin myndighetskontakt, det är reserverat för Storbritanniens förslag i vitboken.

Utifrån att de största riskerna med samtycket finns inbyggt i dess konstruktion och således är oberoende av om detta tillämpas inom eller utom unionen, kan följande skillnader sammanfattas finnas mellan situation noll och efter brexit. Samtycket ska användas undantagsvis, även om det verkar ovillkorligt motiverat i avsaknad av andra lösningar enligt GDPR, det ska vara uttryckligt och ytterligare informerat. Ingen av dessa omständigheter är förtydligad från EU:s sida och därför bör omständigheterna, i ljuset av den utredning jag gjort, inte bereda aktörerna några särdeles svåra problem. Det uttryckliga samtycket och den ytterligare information man ska lämna innebär naturligtvis mer administrativt arbete och kostnad för betaltjänsten och företaget. Dock torde detta sedermera kunna ske mer eller mindre automatiserat och således inte innebära alls samma börda som att till exempel förhandla om standardavtalsklausuler i varje avtal.

Med avstamp i analysen ovan och vad som sagts tidigare är detta vad jag menar med att samtycket är en något mer extensiv variant av vad som gäller i unionen, men innebär egentligen inget ytterligare förfarande. Dock är avsaknaden av OSS fortfarande ett faktum, vilket innebär en osmidighet och potentiellt längre väg till fungerande flöden. Samtycket i artikel 49 GDPR innebär således också försämrade flöden i förhållande till situation noll, i och med en något ökad administrativ börda med tillkommande kostnad, liksom avsaknaden av OSS. Det framstår emellertid som den lösning som faktiskt bereder minst skillnad och minst försämrade flöden för aktörerna jämfört med situation noll. Samtycket utmanar således adekvansbeslutet som den främsta lösningen för personuppgiftsflöden till tredjeland.

8 Slutsatser och diskussion – potentiella konsekvenser för aktörerna, Storbritannien och EU

Slutsatsen blir att gemensamt för alla alternativ till överföring till Storbritannien efter brexit är att de i någon mån kommer att innebära svårigheter för betaltjänsten och företaget, det kommer att bli sämre flöden från unionen till Storbritannien. Något annat hade förvisso heller inte kunnat

[442] GDPR, artikel 55 – 57.

väntas eftersom ett land för första gången går från att vara medlemsstat till att bli tredjeland; EU har inte motsvarande fria flöden i relation till tredjeländer som inom unionens gränser. Utifrån analysen med situation noll som måttstock framstår emellertid en något annan bild än som var min förväntning inför detta arbete. Den lösning som verkar bereda minst problem för betaltjänsten och företaget och som dessutom skiljer sig minst från situation noll är samtycke enligt artikel 49.1 a GDPR. Det är genomgående ett problem som kommer att generera sämre flöden i så måtto att myndighetskontakten inte kommer att vara lika enkel som i unionen. Det enda alternativ som kommer runt det är det som Storbritannien föreslår, men det är knappast ett alternativ som skulle kunna bli verklighet. Inte minst mot bakgrund av EU:s inställning till en sådan lösning, liksom vad EU-domstolens reaktion av allt att döma skulle bli på ett sådant avtal från kommissionen.

Den grund för överföring till tredjeland som såväl EU som Storbritannien i viss mån verkar sträva efter är ett adekvansbeslut. För aktörerna vore emellertid att ”bli lämnade i fred” och använda sig av samtycke en enklare lösning och den som ligger närmast situationen som råder i förhållande till Storbritannien idag, hösten 2018. Det är ett än större undantag från förbudet i artikel 44 GDPR jämte adekvansbeslutet, men samtyckets otydliga karaktär gör det mycket användbart och till en förhållandevis friktionsfri lösning för aktörerna. För att återkoppla till mitt syfte står det klart att alla de olika alternativen kommer att rendera skillnader för aktörerna i förhållande till unionen. Dessa tar sig uttryck i bland annat administrativa bördor, krångligare myndighetskontakter och på dessa följande kostnader för att lösa flödena av personuppgifter till Storbritannien. Alla alternativ bereder således ett *sämre flöde i förhållande till unionens friare och bättre flöde*. Något förvånade är emellertid att det som bereder bäst flöde av de sämre flödena är samtyckesundantaget. Klart är också att, även om det ännu inte är säkert hur utgången kommer att bli kommer det att finnas vägar för aktörerna att lösa sin överföring till Storbritannien efter brexit. Utifrån min utredning syns att flödena av personuppgifter mellan EU och Storbritannien egentligen inte alls riskerar att avbrytas, särskilt inte på grund av avsaknad av adekvansbeslut eller andra lösningar enligt artikel 46 GDPR. Istället skulle det rent av kunna fungera bättre i den mån man avstår från lösningarna enligt artikel 45 – 46 GDPR. Det viktiga för aktörerna är dock att man måste förbereda sig för att inte riskera att fångas av förbudet i artikel 44 GDPR.

Kanske är slutsatsen med avseende på samtycket emellertid inte så förvånande som man kan tro. Alla andra delar är beroende av någon typ av medgivande från offentligt håll. Samtycket är inte avhängigt detta. Istället är det, i relation till Storbritannien efter brexit, behäftat med samma osäkerhetsmoment som till ett Storbritannien inom unionen – att den enskilda kan ta tillbaka sitt samtycke. En reflektion från min sida är att personuppgifternas karaktär, oavsett om de är av det vanligare slaget, som i mitt typfall, eller särskilda sådana, innebär att det måste finnas någon form av säkerhetsventil. Det vill säga, antingen nationellt, från EU eller individen själv. Personuppgifter är information som på grund av dess karaktär inte kan flöda fullständigt fritt, utan kräver någon typ av kontroll. I detta sammanhang blir de problem som samtyckeskonstruktionen är behäftad med ytterst intressanta, även om samtycket som sådant finns som lösning för betaltjänsten som vill skicka uppgifter till företaget i Storbritannien. Det verkar onekligen så att individen, mot bakgrund av att inte ens aktörerna vet hela vidden av den behandling som sker, de facto aldrig kan ge ett fullständigt informerat samtycke. Därför bör man kanske också ifrågasätta att det över huvud taget kallas informerat samtycke, eller att det över huvud taget finns som grund för behandling inom eller utom EU. Således är kanske också risken att individen ska ta tillbaka sitt samtycke snarare

teoretisk än reell. De flesta individer läser inte de villkor som gäller och vet således förmodligen heller inte om den möjlighet de har.[443] Dessa anledningar gör också att det faller sig naturligt att samtycket, som jag noterat som en del av motivet till varför jag vill behandla just detta, förmodligen är den mest praktiskt användbara grunden.

Från EU:s sida verkar man lyfta fram adekvansbeslutet som något av den ultimata lösningen för tredjelandsöverföringar, det är ständigt adekvansbeslutet man eftersträvar och återkommer till i diskussionen. Dessutom, som syns i utredningen ovan, är alla delar utom särskilda skyddsåtgärder och undantag i särskilda situationer baserade på adekvansbeslutet. Utifrån det drar jag slutsatsen att det råder ett slags konsensus i EU:s relation med tredjeländer kring att adekvansbeslutet är den mest fördelaktiga lösningen. Med denna utgångspunkt är det svårt att tro att det man avsåg med samtycket enligt artikel 49.1 a GDPR var att detta skulle vara den mest fördelaktiga lösningen för aktörerna. Utvägen via det uttryckliga samtycket kan verka väl enkel i relation till andra tredjelandslösningar. Därför kan det också ifrågasättas om detta verkligen var den funktion som EU tänkte sig i arbetet med framtagandet av GDPR.[444]

Med det som grund kan man fråga sig om inte skarpare riktlinjer är att vänta från EU. Det är en spekulation från min sida, men utifrån att samtycket som sådant kan kritiseras, samt att man med GDPR vill ha ett högt skydd för individen är frågan om samtyckeskonstruktionen är ändamålsenlig. Man skulle rent av kunna tänka sig att den potentiella säkerhetsrisk som samtycket till tredjelandsöverföring innebär kan vara ett incitament för kommissionen att inleda en adekvansprövning för att sedermera fatta ett beslut. Utifrån artikel 45.7 GDPR är adekvansbeslutet eventuellt inte direkt avgörande för samtyckets användning av aktörerna. WP29 understryker dock att samtycket ska vara ett undantag för situationen när adekvansbeslut eller lämpliga skyddsåtgärder inte finns.[445] Den regelmässighet detta inbjuder till skulle i sin tur kunna påverka den politiska viljan att inleda ett adekvansförfarande från kommissionen. EU har förvisso uttryckt i den politiska deklarationen att man har för avsikt att inleda en dylik prövning. Deklarationen är dock inte juridiskt bindande och man kan bestämma annorlunda. Ännu en indikation som talar för att kommissionen kommer att fatta ett adekvansbeslut skulle emellertid utifrån min utredning vara samtyckeskonstruktionen som incitament.

Som jag tolkar adekvansbeslutet i förhållande till samtycket är fördelen med det förra att skyddet för individen potentiellt blir starkare. Man ska emellertid komma ihåg att aktörerna ändå måste följa GDPR vid användandet av samtycket i artikel 49, varför skyddet för individen teoretiskt sett inte borde bli sämre. Ökad inblandning från det offentliga, som är följden av ett adekvansbeslut, motverkar kanske förvisso missbruk och oärligt användande av samtycket från aktörernas sida. Dock är inte samtycket enligt artikel 49 något som utesluter myndighetstillsyn, snarare inbjuder det till ytterligare kontroll, enligt min reflektion ovan.[446] I ljuset av det kan tänkas att samtycket kanske är att föredra även när man ser till såväl skyddsaspekten för individen som de fria flödena. Om jag

[443] Bechmann, 2014, sidan 22.
[444] Det ska dock nämnas att liknande regler fanns även i GDPR:s föregångare, även om dessa var än mer otydliga, och dessutom inom ramen för ett direktiv som skulle genomföras nationellt. Således är de heller inte fullständigt jämförbara, direktiv 95/46, artikel 26.
[445] WP29, 2018, sidorna 3 – 4.
[446] Avsnitt 7.5.

tillåter mig att använda en utilitaristisk formulering, skulle nyttan maximeras totalt sett med den lösningen framför ett adekvansbeslut. Här kvarstår emellertid problemet med samtyckets informerade karaktär. Ett extensivt användande av samtycke, om än en enkel lösning för aktörerna, äventyrar således individens skydd för personuppgifter, oaktat myndighetstillsyn. Här ska dock tilläggas att i sådant fall gäller det även skyddet inom EU.

Vad gäller den politiska dimensionen av adekvansbeslutet finns den politiska deklarationen från rådet som riktlinje.[447] Signalerna från kommissionen har emellertid inte varit helt entydiga och de andra lösningarna för tredjelandsöverföring lyfts fram såväl som adekvansbeslutet.[448] Att inte inleda ett förfarande för att fatta beslut om adekvat skyddsnivå skulle alltså potentiellt kunna hända. Det skulle kunna röra sig om ett slags markering mot Storbritannien från kommissionens sida för att visa motstånd mot brexit. En dylik markering skulle dock förmodligen ses som ett oansvarigt sätt att agera av kommissionen, med hänsyn till vilken nära relation man har till Storbritannien i egenskap av tidigare medlemsstat. Det skulle urholka förtroendet för hur EU agerar mot tredjeländer. Med avstamp i detta, liksom i den förhållandevis enkla lösning som samtycket innebär, pekar det allra mesta på att en adekvansprövning är vad vi kan förvänta oss. Med det inte sagt att Storbritannien faktiskt anses uppnå adekvat skyddsnivå, men en prövning är av allt att döma vad vi har att vänta. I och med att mycket pekar i denna riktning finns emellertid risken att man som aktör inte helt förbereder sig på vad som kan komma att ske, i den mån adekvansbeslutet drar ut på tiden, eller om Storbritannien inte anses ha en adekvat skyddsnivå. Som aktör är det därför viktigt att ändå vara beredd på att lösa sin överföring med andra medel för att inte riskera att bryta mot förbudet mot överföring och de påföljder det kan få. En lösning i detta avseende kan vara just samtycket i artikel 49.1 a GDPR.

Utifrån Storbritanniens position tycks, utöver vad jag redogjort för i min utredning, en underliggande ton vara att man känner sig säker i förhållande till personuppgiftsflödena. Eftersom den nationella lagen tillkommit i anslutning till GDPR finns en ton i vitboken som antyder att man har en ”det kommer att ordna sig”-attityd. Dessutom visar man på ett visst självförtroende när man i vitboken närmast utmanar, eller i alla fall vill agera startskott för, kommissionen att börja arbeta med ett utvidgat samarbete med tredjeländer enligt artikel 50 GDPR. Utifrån den argumentationen verkar man vilja uttrycka att det inte finns något hinder mot att få ett adekvansbeslut och ej heller potentiellt en utvidgad variant av detta. Vad man emellertid undviker att kommentera är huruvida man egentligen kan översätta GDPR nationellt med hänsyn till stadgan och de eventuellt unika rättigheterna däri. Min analys har visat att Storbritannien potentiellt måste stödja sig på ett slags naturrättslig konsensus-resonemang för att hävda att stadgans rättigheter existerar oberoende av densamma.[449] Man ignorerar således det faktum att konvention 108 och stadgan fortfarande inte är helt motsvarande, trots de ändringar som gjorts av den förra. Som jag konstaterat ovan innebär det att man kan ifrågasätta om det finns en sådan konsensus som Storbritannien potentiellt verkar stödja sitt resonemang på. Den attityd som genomsyrar vitboken är mot bakgrund av detta riskfylld för Storbritannien. Den översättning av GDPR som ska göras via Withdrawal Act 2018 kan potentiellt behäfta den nationella rätten med läckage och rent av utgöra grund för ett påstående

[447] Politiska deklarationen, sidan 4.
[448] Europeiska kommissionen, Withdrawal of the United Kingdom from the Union and the EU Rules in the Field of Data Protection, 2018.
[449] Avsnitt 3.1.1.2.

om att GDPR inte kan översättas till nationell rätt på det sätt Storbritannien konstruerat. Avståndet mellan vad som står skrivet i stadgan respektive konvention 108 kan synas vara marginellt och kanske finns där inte ens en skillnad. Icke desto mindre skulle det, baserat på mitt resonemang, kunna innebära att GDPR inte är tillämplig nationellt trots översättningen. I ljuset av detta verkar Storbritannien i vart fall ha all anledning att fråga sig om det faktiskt kommer att ordna sig.

Något Storbritannien inte heller hörsammat är att kommissionen har adekvansbeslutet som gräns för vad som kan tillåtas för en tredjelandslösning.[450] Inget annat har nämnts från EU. Inte ens i anslutning till Storbritanniens försök att inleda ett mer extensivt tredjelandssamarbete från EU via artikel 50 GDPR. Istället lämnar EU inget mer utrymme för speciallösningar än det som finns i de amerikanska och kanadensiska fallen. Att ställa dessa i relation till den speciallösning Storbritannien önskar visar på viktiga kontraster. Utifrån vitboken kan det konstateras att den amerikanska och kanadensiska lösningen ligger långt ifrån det Storbritannien föreslår. Självcertifierande företag utifrån ramar satta av ett ensidigt beslut från kommissionen skulle inte uppnå den stabilitet Storbritannien verkar vilja skapa genom sitt avtal. Detsamma gäller i det kanadensiska fallet. Dessutom är det PS-ramverkets föregångare, safe harbor-principerna,[451] Storbritannien använder som exempel på hur flöden kan avbrytas abrupt på grund av ett unilateralt beslut.[452] I detta ligger att PS-ramverkets föregångare också bestod i ett självcertifieringssystem.[453] Prövningen av safe harbor-principerna i Schrems-målet är vidare ett exempel på hur EU-domstolen kan ogiltigförklara ett beslut som inte är fattat helt i enlighet med artikel 45 GDPR. Alltså, det tidigare amerikanska exemplet i kombination med det nuvarande är i varje del motsatsen till vad Storbritannien önskar med sitt förslag.

Detta betyder på intet sätt att Storbritannien löper större eller mindre risk att få ett partiellt adekvansbeslut, det beror av omständigheterna så som kommissionen bedömer dem. Dock vill jag lyfta ironin i att man argumenterar för att man ska få en speciallösning från kommissionen genom att välja ut delar av dess argumentation. Samtidigt använder man en av de speciallösningar som finns (eller har funnits) för att visa på ett dåligt exempel, trots att man är medveten om att speciallösningarna hittills enkom har inneburit att man begränsat adekvansbeslutet, inte utvidgat det. Storbritannien vet således gränserna för speciallösningarna, men använder ändå en speciallösning för att argumentera för att den *ordinarie* lösningen i adekvansbeslutet inte är tillräckligt bra och att man själv borde få en *annan typ* av speciallösning.

Även om flödena från EU till Storbritannien knappast kommer att stanna helt och det förefaller vara så att aktörerna alltid kommer att hitta en väg för dessa genom GDPR, kan ändå faktumet att alla tredjelandsalternativ innebär försämrade flöden av personuppgifter ha negativa följder. Vi har redan nu sett hur företag förbereder sig inför brexit, kanske inte just på dataflödesområdet, men

[450] Europeiska kommissionen, 2017, sidorna 9 – 10.
[451] De så kallade "Safe Harbor"-principerna, Europeeiska 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 (EGT L 215, 25.8.2000, s. 7–47), 2000.
[452] Exiting the European Union Committee, 2018; The Government of the United Kingdom, Technical Note: Benefits of a New Data Protection Agreement, 2018.
[453] Europeeiska kommissionen, 2000.

väl vad gäller till exempel företagsstruktur,[454] eller hur man lägger sin produktion.[455] Detta tyder på att företagen ser Storbritannien som en i någon mån mindre attraktiv marknad än den inre marknaden i EU. Inte bara på personuppgiftsområdet förväntas flödena alltså bli sämre, utan även på andra. I konsekvens med reaktionerna från aktörer blir också effekterna på den brittiska ekonomin negativa.[456] Som följd av oklarheterna kring brexit har dessutom brittisk export gått ner,[457] vilket inte minst påverkar de som efterfrågar brittiska produkter på marknader bortom Storbritanniens nationella, det vill säga exempelvis på EU:s inre marknad.

Med utgångspunkt i flödenas försämring kan tänkas att det vore bättre ur ett aktörsperspektiv för kommissionen att hålla sig ifrån ett adekvansbeslut och låta aktörerna sköta detta utifrån samtycket i artikel 49 GDPR. Här skulle man kunna tänka sig att kommissionen, även om en adekvansprövning vore påkallad enligt de kriterier som ställs upp för denna,[458] som en speciallösning för det specialfall brexit är, lämnar över hanteringen av flödena till aktörerna. Detta skulle kunna bli den speciallösning som vore aktuell för Storbritannien, istället för det som föreslås i vitboken eller ett partiellt adekvansbeslut. Dock, med tanke på samtyckets undantagskaraktär och GDPR:s syfte vore det en väl djärv lösning från EU:s sida. GDPR finns förvisso för fria flöden av personuppgifter, men dessa ska slås vakt om inom unionen och inte till tredjeland, inte ens om tredjelandet är en före detta medlemsstat. Mot bakgrund av vad EU uttalat kan därför Storbritannien inte vänta sig någon form av specialbehandling. På samma sätt som ett avstående från en adekvansprövning av politiska skäl skulle urholka EU:s förtroende skulle specialbehandling av Storbritannien via samtycket också sätta förtroendet i gungning. Det är dessutom så att man i sådant fall skulle stimulera flödena av personuppgifter, på bekostnad av individens skydd för dessa. Det senare är GDPR:s primära syfte,[459] och om något skulle innebära anledning till försvagat förtroende för EU och ifrågasättande av ansvarstagande så vore det att börja spekulera med skyddet för individen och dess personuppgifter.

[454] TT, *Handelsbanken brexit-säkrar verksamheten*, Svenska dagbladet, den 3 december 2018, https://www.svd.se/handelsbanken-brexit-sakrar-verksamheten/om/handelsbanken, använd den 5 december 2018.
[455] Morrison, Caitlin, *Mercedes-Benz abandoned plans to move production to UK plant after Brexit vote*, The Independent, den 4 oktober 2018, https://www.independent.co.uk/news/business/news/mercedes-benz-brexit-production-move-nissan-plant-sunderland-a8568331.html, använd den 5 december 2018.
[456] Kleja, Monica, *Brexit - dyr affär för Storbritannien*, Europaportalen, den 29 november 2018, https://www.europaportalen.se/2018/11/brexit-dyr-affar-storbritannien, använd den 5 december 2018.
[457] Europaportalen, *Drastisk nedgång i brittisk export av varor*, Europaportalen den 17 december 2018.
[458] Europeiska kommissionen, 2017, sidan 8.
[459] GDPR, artikel 1.

Litteraturförteckning

Offentliga tryck

Anon., 2018. *Personal Information Protection and Electronic Documents Act.* s.l.:Minister of Justice.

Council of Europe, 1981. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108).* Strasbourg: Council of Europe.

EFTA, 1960. *Convention Establishing the European Free Trade Association.* Stockholm: EFTA.

Europaparlamentet och rådet, 1995. *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 (EGT L 281, 23.11.1995, s. 31–50).* Bryssel: Europeiska unionen.

Europaparlamentet och rådet, 1998. *Europaparlamentets och rådets direktiv 98/34/EG av den 22 juni 1998 om ett informationsförfarande beträffande tekniska standarder och föreskrifter (EGT L 204, 21.7.1998, s. 37–48).* Bryssel: Europaparlamentet och rådet.

Europaparlamentet och rådet, 1998. *Europaparlamentets och Rådets direktiv 98/48/EG av den 20 juli 1998 om ändring av direktiv 98/34/EG om ett informationsförfarande beträffande tekniska standarder och föreskrifter (EGT L 217, 5.8.1998, s. 18–26).* Bryssel: Europaparlamentet och rådet.

Europaparlamentet och rådet, 1998. *Europaparlamentets och rådets direktiv 98/84/EG av den 20 november 1998 om det rättsliga skyddet för tjänster som bygger på eller utgörs av villkorad tillgång (EGT L 320, 28.11.1998, s. 54–57).* Bryssel: Europaparlamentet och rådet.

Europaparlamentet och rådet, 2000. *Europaparlamentets och rådets direktiv 2000/31 av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (EGT L 178, 17.7.2000, s. 1–16).* Bryssel: Europaparlamentet och rådet.

Europaparlamentet och rådet, 2002. *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) (EGT L 201, 31.7.2002, s. 37–47).* Bryssel: Europaparlamentet och rådet.

Europaparlamentet och rådet, 2018. *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 hävande av direktiv 95/46/EG (EUT L 119, 4.5.2016, s. 1–88).* Bryssel: Europaparlamentet och rådet.

Europaparlamentet och rådet, 2018. *Europaparlamentets och rådets förordning (EU) 2018/1807 av den 14 november 2018 om en ram för det fria flödet av andra data än personuppgifter i Europeiska unionen (EUT L 303, 28.11.2018, s. 59–68).* Bryssel: Europaparlamentet och rådet.

Europarådet, 2010. *Europeiska konventionen om skydd för de mänskliga rättigheterna (Rom, 4.XI.1950).* Strasbourg: Europarådet.

Europarådet, 2018. *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.* Strasbourg: s.n.

Europeiska unionen, 2012. *Europeiska unionens stadga om de grundläggande rättigheterna (EUT C 326, 26.10.2012, s. 391–407).* Bryssel: Europeiska unionen.

Europeiska unionen, 2012. *Fördraget om Europeiska unionen (EUT C 202, 7.6.2016, s. 1–388).* Bryssel: Europeiska unionen.

Europeiska unionen, 2012. *Fördraget om Europeiska unionens funktionssätt (EUT C 202, 7.6.2016, s. 1–388*. Bryssel: Europeiska unionen.

Förenta nationerna, 1969. *No. 18232 Vienna Convention on the law of treaties (with annex). Concluded at Vienna on 23 May 1969*. Wien: s.n.

The Governement of the United Kingdom, 2018. *Data Protection Act 2018*. s.l.:s.n.

The Government of the United Kingdom, 2016. *Investigatory Powers Act 2016*. London: The Government of the United Kingdom.

The Government of the United Kingdom, 2018. *European Union (Withdrawal) Act 2018*. s.l.:s.n.

The Government of the United Kingdom, 2018. *Regulation of Investigatory Powers Act 2000*. s.l.:s.n.

EU, Canada, 2017. *Comprehensive Economic and Trade Agreement (CETA).* s.l.:s.n.

EU; Japan, 2017. *Economic Partnership Agreement between the European Union and Japan.* Bryssel: s.n.

Europeiska gemenskapen mfl. länder, 1994. *Agreement on the European Economic Area (OJ No L 1, 3.1.1994 p. 3; and EFTA States' official gazettes).* s.l.:s.n.

Europeiska kommissionen, 2018. *TF50 (2018) 55, Draft Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, as agreed at negotiators' level on 14 November 2018*. Bryssel: Europeiska kommissionen.
Europeiska kommissionen, 2018. *Withdrawal of the United Kingdom from the Union and the EU Rules in the Field of Data Protection.* Bryssel: Europeiska kommissionen.

Europeiska kommissionen, 2000. *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) (EGT L 215, 25.8.2000, s. 7–47).* Bryssel: Europeiska kommissionen.

Europeiska kommissionen, 2001. *Kommissionens beslut av den 20 december 2001 i enlighet med Europaparlamentets och rådets direktiv 95/46/EG om adekvat skydd för personuppgifter genom den kanadensiska lagen om elektroniska handlingar och skydd för personuppgifter (2002/2/EG) (EGT L 2, 4.1.2002, s. 13–16).* Bryssel: Europeiska kommissionen.

Europeiska kommissionen, 2003. *Kommissionens beslut av den 21 november 2003 om skyddsnivån för personuppgifter på Guernsey (2003/821/EG) (EUT L 308, 25.11.2003, s. 27–28).* Bryssel: Europeiska kommissionen.

Europeiska kommissionen, 2004. *Kommissionens beslut av den 28 april 2004 om skyddsnivån för personuppgifter på Isle of Man (2004/411/EG) (EUT L 151, 30.4.2004, s. 48–51).* Bryssel: Europeiska kommissionen.

Europeiska kommissionen, 2008. *Kommissionens beslut av den 8 maj 2008 i enlighet med Europaparlamentets och rådets direktiv 95/46/EG om adekvat skydd för personuppgifter på Jersey (2008/393/EG) (EUT L 138, 28.5.2008, s. 21–23).* Bryssel: Europeiska kommissionen.

Europeiska kommissionen, 2010. *Kommissionens beslut av den 5 februari 2010 om standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredjeland i enlighet med Europaparlamentets och rådets direktiv 95/46/EG(EUT L 39, 12.2.2010, s. 5–18).* Bryssel: Europeiska kommissionen.

Article 29 Data Protection Working Party, 2005. *2093/05/EN WP 114 Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995.* Bryssel: Article 29 Data Protection Working Party.

Article 29 Data Protection Working Party, 2017. *17/ EN WP 259 rev. 01 Guidelines on consent under Regulation 2016/679.* Bryssel: Article 29 Data Protection Working Party.

Article 29 Data Protection Working Party, 2018. *18/EN WP 261 Guidelines on Article 49 of Regulation 2016/679.* Bryssel: Article 29 Data Protection Working Party.

Europeiska kommissionen, 2016. *Insyn i EU-politiken: Konsumentskydd.* Luxemburg: Europeiska kommissionen.

Europeiska kommissionen, 2017. *Meddelande från kommissionen till Europaparlamentet och rådet, Utbyte och skydd av personuppgifter i en globaliserad värld, COM(2017) 7 final av den 10 januari 2017.* Brysssel: Europeiska kommissionen.

Europeiska kommissionen, 2018. *Withdrawal of the United Kingdom from the Union and the EU Rules in the Field of Data Protection.* Bryssel: Europeiska kommissionen.

Europeiska unionens råd, 2018. *Political declaration setting out the framework for the future relationship between the European Union and the United Kingdom.* Bryssel: Europeiska unionens råd.

The Government of the United Kingdom, 2018. *Technical Note: Benefits of a New Data Protection Agreement.* London: s.n.

The Register of the Court, 2018. *Some aspects of UK surveillance violate Convention.* Strasbourg: The Register of the Court.

Department for Exiting the European Union Correspondence Unit, 2018. London: s.n.

Barnier, M., 2018. *Speech by Michel Barnier at the 28th Congress of the International Federation for European Law.* Bryssel: s.n.

Rättsfall och avgöranden

Big Brother Watch and Others v. the United Kingdom (applications nos. 58170/13, 62322/14 and 24960/15) (2018).

Domstolens dom (stora avdelningen) av den 21 december 2016, C-203/15 och C-698/15, EUT C 53, 20.2.2017, s. 11–12, (2016).

Domstolens dom (stora avdelningen) av den 6 oktober 2015. Maximillian Schrems mot Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650 (2015).

Rapporter

International Chamber of Commerce Sweden, 2011. *ICC:s Regler för Reklam och Marknadskommunikation.* Stockholm: s.n.
Kommerskollegium, 2014. *No Transfer, No Trade - the Importance of Cross-Border Data Transfers for Companies Based in Sweden,* Stockholm: Kommerskollegium.

Kommerskollegium, 2016. *Data Flows A Fifth Freedom for the Internal Market?,* Stockholm: Kommerskollegium.

Kommerskollegium, 2018. *Efter brexit - analys av svenska intressen inför kommande förhandlingar,* Stockholm: Kommerskollegium.

Kommerskollegium, 2018. *Storbritanniens vitbok om den framtida relationen med EU, en analys av förslagen,* Stockholm: Kommerskollegium.

Litteratur

Bechmann, A., 2014. Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook. *Journal of Media Business Studies*, 1 mars, Volume 11, pp. 21 - 38.

Berinato, S., 2018. Stop Thinking about Consent: It Isn't Possible and It Isn't Right. *Harvard Business Review*, 24 september, pp. 1 - 8.

Bladini, M., 2016. Objektivitet i dömandet – på gott och på ont?. *Svensk Juristtidning,* Issue 3016, pp. 303 - 312.

Carlsson, B., 1985. En rationell diskurs; "Tillbaka till Russeau". *Tidskrift för rättssociologi*, Volume 2, pp. 163 - 179.

Jonsson, M., Magnusson Sjöberg, C., Söderqvist, U. & Törngren, D., 2018. *Kommentarer till förordning 679/2016*. Stockholm: Karnov Group.

Larsson, S., 2018. *Den kvantifierade konsumenten: Om behovet av tillit och transparens på datadrivna marknader,* Stockholm: Lunds universitet.

Stenhammar, F., 2008. Hård rättspositivism i folkrätten. *Svensk juristtidning*, pp. 1 - 29.

Tidningsartiklar

Elliott, K. A., 2018. Who Won in the NAFTA Renegotiation? A Preliminary Assessment. *World Politics Review*, 2 oktober.

Europaportalen, 2018. May vill förlänga övergångstid. *Europaportalen*, 19 oktober.

Europaportalen, 2018. Drastisk nedgång i brittisk export av varor. *Europaportalen*, 17 december.

Herszenhorn, D. M. & De La Baume, M., 2018. Barnier dismantles UK's Brexit white paper. *Politico*, 26 juli.

Hill, R., 2018. Data flows post-Brexit: 'Leave it to government to make sure you've got a smooth run in.' Er, OK. *The Register*, 8 november.

Kleja, M., 2018. Brexit - dyr affär för Storbritannien. *Europaportalen*, 29 november.

Kleja, M., 2018. EU ställer ultimatum – tiden rinner ut för brexitavtal. *Europaportalen*, 20 september.

Morrison, C., 2018. Mercedes-Benz abandoned plans to move production to UK plant after Brexit vote. *The Independent*, 4 oktober.

Schwab, K., 2018. How Widely Do Companies Share User Data? Here's A Chilling Glimpse. *Fast Company*, 19 januari.

Stupp, C., 2017. Commission conducting review of all foreign data transfer deals. 9 november.

TT, 2018. Handelsbanken brexit-säkrar verksamheten. *Svenska dagbladet*, 3 december.

Wintour, P., 2018. Norwegian politicians reject UK's Norway-plus Brexit plan. *The Guardian*, 7 december.

Elektroniska källor

Department for Digital, Culture, Media & Sport, 2018. *www.gov.uk.* [Online]
Tillgänglig på: https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal/data-protection-if-theres-no-brexit-deal
[Använd 27 november 2018].

Drooms Global, 2018. *www.drooms.com.* [Online]
Tillgänglig på: https://drooms.com/en/blog/gdpr-disadvantages-of-model-clauses-and-binding-corporate-rules
[Använd 29 november 2018].

Dyevre, A., 2018. *www.blogs.lse.ac.uk.* [Online]
Tillgänglig på: http://blogs.lse.ac.uk/europpblog/2018/11/13/have-british-judges-already-left-the-eu-the-impact-of-the-brexit-vote-on-eu-law-in-the-uk/
[Använd 27 november 2018].

EFTA, 2018. *www.efta.in.* [Online]
Tillgänglig på: http://www.efta.int/eea-lex/32016R0679
[Använd 10 december 2018].

EFTA, 2018. *www.efta.int.* [Online]
Tillgänglig på: http://www.efta.int/Advisory-Bodies/news/EFTA-Parliamentary-Committee-members-discuss-Brexit-counterparts-UK-507866
[Använd 14 oktober 2018].

Europaparlamentet, 2010. *www.europarl.europa.eu.* [Online]
Tillgänglig på: http://www.europarl.europa.eu/sides/getDoc.do?language=SV&type=IM-PRESS&reference=20100507STO74260
[Använd 12 december 2018].

Europarådet, 2018. *www.coe.int.* [Online]
Tillgänglig på: https://www.coe.int/en/web/conventions/full-list/-

/conventions/treaty/country/UK?p_auth=qaopIGxq
[Använd 11 oktober 2018].

Europarådet, 2018. *www.coe.int.* [Online]
Tillgänglig på: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/declarations?p_auth=DdNsMbLo
[Använd 11 oktober 2018].

Europarådet, 2018. *www.coe.int.* [Online]
Tillgänglig på: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures?p_auth=DdNsMbLo
[Använd 11 oktober 2018].

Europarådet, 2018. *www.coe.int.* [Online]
Tillgänglig på: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures?p_auth=Q4OaIJ6M
[Använd 12 december 2018].

Europarådet, 2018. *www.coe.int.* [Online]
Tillgänglig på: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures?p_auth=9tiU0QIN
[Använd 10 oktober 2018].

Europarådet, n.d. *www.coe.int.* [Online]
Tillgänglig på: https://www.coe.int/en/web/portal/47-members-states
[Använd 15 december 2018].

Europeiska kommissionen, 2016. *EU-U.S. Privacy Shield: Frequently Asked Questions.* [Online]
Tillgänglig på: http://europa.eu/rapid/press-release_MEMO-16-2462_en.htm
[Använd 29 november 2018].

Europeiska kommissionen, 2018. *Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council on the adequate protection of personal data by Japan.* [Online]
Tillgänglig på: https://ec.europa.eu/info/sites/info/files/draft_adequacy_decision.pdf
[Använd 22 november 2018].

Europeiska kommissionen, 2018. *www.ec.europa.eu.* [Online]
Tillgänglig på: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
[Använd 27 november 2018].

Europeiska kommissionen, 2018. *www.ec.europa.eu.* [Online]
Tillgänglig på: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
[Använd 14 december 2018].

Europeiska kommissionen, 2018. *www.europa.eu.* [Online]
Tillgänglig på: http://europa.eu/rapid/press-release_IP-18-5433_en.htm
[Använd 12 december 2018].

Europeiska kommissionen, n.d. *www.ec.europa.eu.* [Online]
Tillgänglig på: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en
[Använd 22 december 2018].

Europeiska unionen, n.d. *www.europa.eu.* [Online]
Tillgänglig på: https://europa.eu/european-union/eu-law/legal-acts_sv
[Använd 21 oktober 2018].

Europeiska unionen, n.d. *www.europa.eu.* [Online]
Tillgänglig på: https://europa.eu/european-union/eu-law/legal-acts_sv
[Använd 10 oktober 2018].

Exiting the European Union Committee, 2018. *www.publications.parliament.uk.* [Online]
Tillgänglig på:
https://publications.parliament.uk/pa/cm201719/cmselect/cmexeu/1317/131701.htm
[Använd 28 november 2018].

General Secretariat of the Council, 2018. *www.consilium.europa.eu.* [Online]
Tillgänglig på: http://www.consilium.europa.eu/en/press/press-releases/2018/03/23/european-council-art-50-guidelines-on-the-framework-for-the-future-eu-uk-relationship-23-march-2018/
[Använd 21 september 2018].

Information Commissioner's Office, 2018. *www.ico.org.uk.* [Online]
Tillgänglig på: https://ico.org.uk/about-the-ico/our-information/history-of-the-ico/
[Använd 11 oktober 2018].

Information Commissioner's Office, 2018. *www.ico.org.uk.* [Online]
Tillgänglig på: https://ico.org.uk/action-weve-taken/enforcement/
[Använd 12 oktober 2018].

Information Commissioner's Office, 2018. *www.ico.org.uk.* [Online]
Tillgänglig på: https://ico.org.uk/action-weve-taken/enforcement/oaklands-assist-uk-limited/
[Använd 12 oktober 2018].

Information Commissioner's Office, 2018. *www.ico.org.uk.* [Online]
Tillgänglig på: https://ico.org.uk/action-weve-taken/enforcement/boost-finance-limited/
[Använd 12 oktober 2018].

Information Commissioner's Office, 2018. *www.ico.org.uk.* [Online]
Tillgänglig på: https://ico.org.uk/for-organisations/data-protection-act-2018/
[Använd 23 oktober 2018].

i-scoop, n.d. *www.i-scoop.eu.* [Online]
Tillgänglig på: https://www.i-scoop.eu/gdpr/consent-gdpr/
[Använd 12 december 2018].

Kala, K., 2017. *www.e-estonia.com.* [Online]
Tillgänglig på: https://e-estonia.com/free-movement-of-data-as-the-5th-fundamental-freedom-

of-the-european-union/
[Använd 24 september 2018].

Kommerskollegium, n.d. *www.kommers.se.* [Online]
Tillgänglig på: https://www.kommers.se/verksamhetsomraden/EUs-inre-marknad/Allmant/De-fyra-friheterna/
[Använd 14 september 2018].

Linklaters, 2018. *www.linklaters.com.* [Online]
Tillgänglig på: https://www.linklaters.com/Brexit-SI-Tracker
[Använd 22 december 2018].

Nadkarni, T. I., 2018. *www.europarl.europa.eu.* [Online]
Tillgänglig på: www.europarl.europa.eu/news/en/press-room/20180926IPR14403/free-flow-of-non-personal-data-parliament-approves-eu-s-fifth-freedom
[Använd 12 december 2018].

PayPal, 2018. *www.paypal.com.* [Online]
Tillgänglig på: https://www.paypal.com/ie/webapps/mpp/ua/third-parties-list-prev
[Använd 20 september 2018].

Reuters, 2018. *www.reuters.com.* [Online]
Tillgänglig på: https://www.reuters.com/finance/stocks/company-profile/PYPL.O
[Använd 29 november 2018].

The Government of the United Kingdom, 2018. *www.gov.uk.* [Online]
Tillgänglig på: https://www.gov.uk/government/publications/the-future-relationship-between-the-united-kingdom-and-the-european-union?utm_source=e5b3260b-2069-4b57-a5bd-24e9ea02aa88&utm_medium=email&utm_campaign=govuk-notifications&utm_content=immediate
[Använd 21 september 2018].

Tillväxtverket, 2018. *www.verksamt.se.* [Online]
Tillgänglig på: https://www.verksamt.se/driva/gdpr-dataskyddsregler/vad-ar-en-personuppgift
[Använd 21 september 2018].

Vahl, M., 2018. *www.efta.int.* [Online]
Tillgänglig på: http://www.efta.int/EEA/news/General-Data-Protection-Regulation-incorporated-EEA-Agreement-509291
[Använd 20 september 2018].

Vodafone, 2018. *www.vodafone.co.uk.* [Online]
Tillgänglig på: https://www.vodafone.co.uk/privacy
[Använd 5 november 2018].