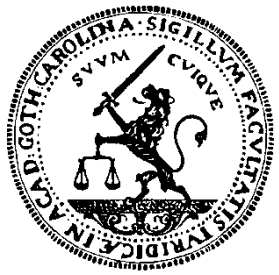

JURIDISKA FAKULTETEN
vid Lunds universitet

Victoria Limnefelt

Europeiska kommissionens standardavtalsklausulers förenlighet med gällande rätt vid en överföring av personuppgifter till tredje land

LAGF03 Rättsvetenskaplig uppsats

Kandidatuppsats på juristprogrammet
15 högskolepoäng

Handledare: David Dryselius

HT 2018

Innehåll

Summary

Today's society is defined by a growing digital character, in which cross-border commercial relationships develop in accordance with the rapidly expanding technology. Such relationships also increase the flow of personal data from the European Union (the Union) to third countries, and are essential for the digital economy. The Member States of the Union are governed by the General Data Protection Regulation (GDPR), whose main purpose is, inter alia, to ensure that the data subjects are adequately protected. In third countries, the same general rules that provide equivalent guarantees, do not exist.

Chapter V in the GDPR contains a specific set of rules that enables a third-country transfer. Primarily, such a transfer may take place if the third country ensures an adequate level of protection. If an adequate level of protection is not achieved, the transfer may be based on the decision of the European Commission on *standard contractual clauses*. Today, there are three sets of standard contractual clauses, all of which are based on the Data Protection Directive. Two out of three of these regulate the relationship when both the transferor and the recipient are a controller. The last set is suitable for the contractual relationship in which the transferor is the controller and the recipient a processor. However, there is a significant risk that the standard contractual clauses do not correspond to the personal data protection provided by today's applicable law.

When transferring personal data from the Union into the United States of America (USA), the contract parties used to apply a specific regulatory framework, the Safe Harbor system. However, in 2015 the system was invalidated by the Court of Justice of the European Union. The Safe Harbor principles aimed to guarantee the data subjects a proper protection of personal data as the Union citizens' information was transferred from the Union into the USA. The generally designed Safe Harbor principles led to the national law to take precedence over the Safe Harbor system if the national law required it. In cases where national law had required a breach of the Safe Harbor principles, it was shown that the breach was not strictly necessary and proportionate. This thesis aims to investigate whether the standard contractual clauses are compatible with today's applicable law from a business perspective.

The thesis finds that the standard contractual clauses demonstrate similar structures to the void Safe Harbor system. The structures give openings to prioritize a third country's national law over the principles of the standard contractual clauses, in a way which can challenge the data protection. With the entry into force of the GDPR, new principles should be taken into account when applying the standard contractual clauses. In conclusion, the thesis finds that the standard contractual clauses should be applied with great caution until they are on trial in the Court of Justice of the European Union.

Sammanfattning

Dagens samhälle präglas av en växande digital karaktär, där gränsöverskridande kommersiella relationer utvecklas i enlighet med den snabbt expansiva tekniken. Sådana relationer ökar även flödet av personuppgifter från unionen till tredje land, som är nödvändiga för den digitala ekonomin. Medlemsländerna inom den Europeiska unionen lyder under dataskyddsförordningen, vars huvudsyfte bland annat ska garantera de registrerade en hög nivå av skydd för personuppgifter. I tredje land existerar dock inte samma generella regelverk som ger motsvarande garantier.

I kapitel V dataskyddsförordningen återfinnes ett särskilt regelverk som möjliggör en tredjelandsöverföring. Enligt huvudregeln får en sådan överföring ske om tredjelandet säkerställer en adekvat skyddsnivå. I andra hand, om en adekvat skyddsnivå inte uppnås, kan överföringen baseras på en tillämpning av kommissionens beslut om *standardavtalsklausuler*. Det finns i skrivande stund tre uppsättningar standardavtalsklausuler vilka samtliga är grundade på dataskyddsdirektivet. Två av tre uppsättningar reglerar relationen då både överförare och mottagare är personuppgiftsansvariga. Den sist beslutade uppsättningen lämpar sig för den avtalsrelation där överföraren är personuppgiftsansvarig och mottagaren ett personuppgiftsbiträde. Det föreligger dock en betydande risk för att standardavtalsklausulerna inte motsvarar det personuppgiftsskydd som gällande rätt uppställer. Denna uppsats ämnar att utreda om standardavtalsklausulerna är förenliga med gällande rätt från ett företagsperspektiv.

Vid en överföring av personuppgifter från unionen till USA tillämpades ett särskilt regelverk, Safe Harbor-systemet, som år 2015 ogiltigförklarades av EU-domstolen. Safe Harbor-principerna skulle garantera de registrerade ett fullgott skydd för personuppgifter då unionsmedborgarnas uppgifter överfördes från unionen till USA. Ogiltigförklarandet baserades på kommissionens underlåtande att konstatera genom vilka åtgärder USA vidtog i sin interna lagstiftning eller internationella åtaganden för att uppnå en adekvat skyddsnivå. De generellt utformade Safe Harbor-principerna medförde även att nationell rätt hade företräde framför Safe Harbor-systemet i de fall den nationella rätten krävde det. I de fall den nationella rätten hade krävt ett åsidosättande av Safe Harbor-principerna visades att åsidosättandet inte varit strängt nödvändigt.

Uppsatsen finner att standardavtalsklausulerna påvisar liknande strukturer som det ogiltigförklarande Safe Harbor-systemet. Strukturerna möjliggör att ett tredje lands nationella rätt ges företräde framför principerna i standardavtalsklausulerna på ett sätt som kan äventyra skyddet av personuppgifter. Med dataskyddsförordningens ikraftträdande införs nya bestämmelser som bör beaktas vid en tillämpning av standardavtalsklausuler. Avslutningsvis finner uppsatsen att standardavtalsklausulerna bör tillämpas med stor försiktighet till dess att de i framtiden prövats av EU-domstolen.

Förkortningar

Artikel 29-gruppen	Artikel 29-arbetsgruppen för skydd av personuppgifter i enlighet med artikel 29, direktiv 95/46/EG
Dataskyddsdirektivet	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
Dataskyddsförordningen	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG
EES	Europeiska ekonomiska samarbetsområdet
EU	Europeiska unionen
FEUF	Fördraget om europeiska unionens funktionssätt
EU-domstolen	Europeiska unionens domstol
EU-stadgan	Europeiska unionens stadga om de grundläggande rättigheterna
Europakonventionen	Europeiska konventionen om de mänskliga rättigheterna
EU-stadgan	Europeiska unionens stadga om de grundläggande rättigheterna
Kommissionen	Europeiska kommissionen
Safe Harbor-systemet	Kommissionens beslut 2000/520/EG av den 26 juli 2000
Standardavtalsklausuler	Kommissionens beslut 2001/497/EG, 2004/915/EG, och 2010/87/EU
OECD	Organisationen för ekonomiskt samarbete och utveckling
Rådet	Europeiska rådet

1 Inledning

1.1 Bakgrund

Den inre marknaden har genom sin allt mer ekonomiska och sociala integration lett till en omfattande ökning av gränsöverskridande flöden av personuppgifter[1]. Samtidigt har den utvecklande tekniken och den ökade globaliseringen gått nya utmaningar till mötes, där skyddet för personuppgifter kräver en stark struktur för att generera den tillit som krävs för att den digitala ekonomin ska fortsätta stärkas.[2]

År 2013 angavs i ett meddelande av kommissionen att tilliten för skyddet av personuppgifter inte var fullgod. Efter Edward Snowdens avslöjanden om den amerikanska underrättelsetjänstens övervakningsprogram uttrycktes nämligen farhågor om att Safe Harbor-systemet[3] med stor sannolikhet överträddes.[4] Safe Harbor-systemet var tidigare det system som möjliggjorde en lagenlig överföring av personuppgifter från Europeiska unionen (nedan unionen) till USA, vars principer skulle motsvara en väsentligen likvärdig skyddsnivå för personuppgifter som unionens.[5] De amerikanska övervakningsprogrammen tillämpades på de flesta amerikanska internetföretag som var anslutna till Safe Harbor-systemet. Safe Harbor-systemet innehöll generella bestämmelser vilka möjliggjorde att amerikansk lagstiftning i en för stor utsträckning hade företräde framför Safe Harbor-principerna, och öppnade således upp en väg för den amerikanska underrättelsetjänsten att få tillgång till personuppgifter som förts över från företag inom unionen.[6] Safe Harbor-systemet innehöll brister som år 2015 kom att leda till att EU-domstolen ogiltigförklarade det. För överföringar av

[1] En *personuppgift* definieras såsom varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras med hänvisning till en identifierare som till exempel ett namn, personnummer, adress, utseende eller andra faktorer specifika för personens identitet. Se artikel 4 (1) dataskyddsförordningen.
[2] Beaktandeskäl 5, 6 och 7 dataskyddsförordningen.
[3] Kommissionens beslut 2000/520/EG.
[4] Kommissionens meddelande, KOM(2013) 847 final, s. 5.
[5] Mål C-362/14 *Maximillian Schrems mot Data Protection Commissioner*, p. 75-76.
[6] Ibid, p. 14, 22 och 31.

personuppgifter från unionen till USA tillämpas idag *Privacy Shield* som ska motsvara en adekvat skyddsnivå för överföring av personuppgifter till USA.[7]

Vid en överföring av personuppgifter av ett företag från en unionsstat, till ett företag i ett tredje land[8] i kommersiellt syfte, kan parterna välja att tillämpa kommissionens *standardavtalsklausuler.*[9] Standardavtalsklausulerna beslutades av kommissionen mot bakgrund av dataskyddsdirektivet[10], som ersattes av dataskyddsförordningen[11] den 25 maj 2018.[12] Mot bakgrund av ogiltigförklarandet av Safe Harbor-systemet är det möjligt att standardavtalsklausulerna innehåller liknande bristfälligheter som Safe Harbor-principerna. Dataskyddsförordningen inför nya materiella bestämmelser vilket medför en risk för att standardavtalsklausulerna inte är förenliga med, i skrivande stund, gällande rätt.

I sammanhanget ska noteras att High Court of Ireland begärt ett förhandsavgörande av EU-domstolen, som kan belysa ämnets aktualitet. Begäran avser att fastställa standardavtalsklausulernas rättsliga status och är i skrivande stund i väntan på en rättslig prövning.[13] Tolkningsfrågorna ska dock prövas mot bakgrund av tillämplig lag som låg till grund för prövning i Irland, vilket var år 2015. Dataskyddsförordningen hade vid denna tidpunkt inte börjat tillämpas.[14]

[7] Kommissionens genomförandebeslut C/2016/4176.
[8] Med *tredje land* avses ett land beläget utanför EU/EES-området, se Datainspektionen, ”*Överföring till tredje land”*.
[9] Kommissionens beslut 2001/497/EG, 2004/915/EG, och 2010/87/EU.
[10] 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.
[11] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG.
[12] Artikel 99 dataskyddsförordningen.
[13] Mål C-311/18 *Data Protection Commissioner mot Facebook Ireland Limited, Maximillian Schrems.*
[14] Artikel 99 dataskyddsförordningen.

1.2 Syfte, målsättning och frågeställning

Uppsatsens överordnade syfte är att utröna rättsläget vad beträffar standardavtalsklausulernas förenlighet med dataskyddsförordningen vid en överföring av personuppgifter till tredje land. För att uppnå uppsatsens syfte är målsättningen att undersöka relevanta materiella bestämmelser i dataskyddsförordningen och dataskyddsdirektivet, där huvudsakligt fokus läggs på de bestämmelser om skydd av personuppgifter som aktualiseras vid överföring av personuppgifter till tredje land. Målet är även att identifiera de tolkningsstrukturer som återfinnes i *Maximillian Schrems mot Data Protection Commissioner*[15] (nedan Maximillian Schrems-målet), som EU-domstolen tillämpade vid ogiltigförklarandet av Safe Harbor-systemet. Tolkningsstrukturerna är avsedda att tillämpas på standardavtalsklausulerna, tillsammans med relevanta bestämmelser i dataskyddsförordningen, för att utläsa huruvida standardavtalsklausulerna är förenliga med dataskyddsförordningen. Inom ramen för det angivna syftet ämnar uppsatsen att besvara följande frågeställningar:

Vilka materiella förändringar avseende skyddet av personuppgifter medför dataskyddsförordningen i förhållande till dataskyddsdirektivet? Hur är standardavtalsklausulerna och Safe Harbor-principerna uppbyggda? Vilka utgör de tolkningsstrukturer EU-domstolen tillämpade vid ogiltigförklarande av Safe Harbor-systemet?

1.3 Metod, material och perspektiv

För att utreda rättsläget vad beträffar standardavtalsklausulernas förenlighet med dataskyddsförordningen baseras uppsatsen på en rättsdogmatisk metod, med utgångspunkt i lagtext, rättspraxis, förarbeten, doktrin samt andra allmänna principer.[16] Uppsatsen kommer även att behandla EU-rättsliga

[15] Mål C-362/14 *Maximillian Schrems mot Data Protection Commissioner*.
[16] Nääv och Zamboni (2018), s. 24.

regelverk, vilket gör att en traditionell EU-rättslig metod kommer att tillämpas. Utredningen sker utifrån primärrätt, sekundärrätt, allmänna rättsprinciper samt EU-domstolens rättspraxis. Tolkningen av unionsrätten avviker i vissa aspekter från svensk rätt. EU-rätten har till exempel inte förarbeten till varje rättsakt likt de svenska rättsakterna. Tolkningen av rättsakterna sker istället utifrån ett antal centrala principer, där en teleologisk tolkning intar en betydande ställning och innehar en stor roll i uppsatsen.[17]

Vidare tillämpas icke-bindande EU-rättsliga dokument i form av riktlinjer och vägledningar.[18] Dessa rättsakter faller under så kallad soft law, i syfte att indikera att de oavsett avsaknad av bindande rättslig verkan kan vara av rättslig betydelse vid tolkning av rättsakter.[19] Uppsatsen använder sig även av beaktandeskälen till rättsakter, där motiven till varje förordnings och direktivs uppkomst anges.[20] Likt soft law är preambeln icke-bindande, men eftersom syftet preciseras genom att det anges vad som beaktats vid utfärdandet av rättsakten tillmäts beaktandeskälen ett viktigt tolkningsstöd.[21]

Uppsatsen genomsyras av huvudsakligen ett företagsperspektiv. Standardavtalsklausulerna tillämpas uteslutande av företag och organisationer vid överföring av personuppgifter i ett kommersiellt syfte. Uppsatsen har därför för avsikt att rikta sig gentemot företag och organisationer som faller under dataskyddsförordningens jurisdiktion, för att dessa företag och organisationer ska kunna ta ställning till rättsläget och göra en avvägning om hur standardavtalsklausulerna bör hanteras inom just deras organisation.

[17] Bernitz m.fl. (2017), s. 74 f. och Nääv och Zamboni (2018), s. 122.
[18] Nääv och Zamboni (2018), s. 128.
[19] Derlén, Ingmanson och Lindholm (2015), s. 39.
[20] Artikel 296.2 FEUF.
[21] Bernitz m.fl. (2017), s. 73.

1.4 Disposition

Detta avsnitt, *avsnitt ett,* ger en inledande presentation av ämnet. Följande *avsnitt två* redogör för dataskyddsförordningens bakgrund och syfte. I *samma* avsnitt behandlas därefter förutsättningarna för en överföring till tredje land i enlighet med dataskyddsförordningen. Avsnitt *tre* presenterar tidigare relevant lagstiftning för personuppgiftsskydd. Härigenom behandlas dataskyddsdirektivet på samma sätt som dataskyddsförordningen, för att belysa de rättsliga ändringar som dataskyddsförordningen medfört men även de grunder standardavtalsklausulerna baseras på. *Samma* avsnitt berör Safe Harbor-principerna, som är av vikt att utreda med hänsyn till att uppsatsen i ett senare avsnitt kommer att behandla ogiltigförklarandet av dessa principer. Uppsatsens *fjärde* avsnitt anför en redogörelse för de olika uppsättningarna av standardavtalsklausuler. Avsnitt *fem* behandlar ogiltigförklarandet av Safe Harbor-systemet.

En avslutande analys och slutsatser om standardavtalsklausulernas förenlighet med gällande rätt anförs i uppsatsens *sjätte* avsnitt.

1.5 Forskningsöversikt

Uppsatsen grundar sin utredning på EU-rättsliga källor. Dels behandlas dataskyddsförordningen, dels används tidigare dataskyddslagstiftning som tillämpades innan dataskyddsförordningens ikraftträdande. Vad beträffar tidigare dataskyddslagstiftning återfinnes en god mängd material, med forskning, rättspraxis och doktrin. Material hänförligt till dataskyddsförordningen med inriktning på tredjelandsöverföring och standardavtalsklausulerna intar dock en mer begränsad ställning.

Forskningen på området är dock expansiv. Efter ogiltigförklarandet av Safe Harbor-systemet[22] har ämnet uppmärksammats i allt större utsträckning. För

[22] Mål C-362/14 *Maximillian Schrems mot Data Protection Commissioner*, p. 27-28.

närvarande inväntar standardavtalsklausulernas giltighet en rättslig prövning[23], dock i förhållande till dataskyddslagstiftning som utgjorde gällande rätt innan dataskyddsförordningen började tillämpas.

1.6 Avgränsning

Skyddet för personuppgifter vid en tredjelandsöverföring är ett ämne som ger upphov till många komplexa frågor. Av denna anledning är det därför av vikt att tydligt dra gränser gentemot vilka områden uppsatsen inte kommer att behandla. Uppsatsen ämnar till att bedöma standardavtalsklausulernas rättsliga ställning mot bakgrund av dataskyddsförordningen och de tolkningsprinciper som identifieras i Maximillian Schrems-målet. Samtliga materiella skillnader mellan dataskyddsförordningen och dataskyddsdirektivet kommer inte att beröras. Endast de bestämmelser som är relevanta för en överföring av personuppgifter till tredje land med användande av standardavtalsklausulerna kommer att ges en redogörelse. Av utrymmesskäl kan uppsatsen inte behandla samtliga rättsliga principer i Safe Harbor-systemet och standardavtalsklausulerna.

Uppsatsen gör vidare en gränsdragning gentemot andra alternativ för en överföring till tredje land som dataskyddsförordningen uppställer, till exempel bindande företagsbestämmelser eller godkända uppförandekoder och certifieringsmekanismer, eftersom de faller utanför uppsatsens frågeställning. Av utrymmesskäl kommer respekten för privatliv och skyddet för personuppgifter enligt regeringsformen, EU-stadgan och Europakonventionen inte att ges en närmare redogörelse, utan uppsatsen kommer endast framhålla att skyddet för fysiska personer vid behandling av personuppgifter är en grundläggande rättighet enligt dessa regelverk.

[23] Mål C-311/18 *Data Protection Commissioner mot Facebook Ireland Limited, Maximillian Schrems.*

2 Rådande skydd för personuppgifter vid tredjelandsöverföring

2.1 Allmän dataskyddsförordning

2.1.1 Bakgrund och syfte

I syfte att förstå motiven till dataskyddsförordningen och dess uppkomst inleds följande kapitel med ett yttrande från propositionen till den dåvarande personuppgiftslagen (1998:204), men som idag likväl kan användas såsom vägledning för en inledande förståelse för dataskyddsförordningens tillkomst.[24] Bakgrunden till reformbehovet av Sveriges förutvarande dataskyddslagstiftning beskrevs nämligen vara delvis på grund av att ”utvecklingen inom informationstekniken har gått rasande fort under de senaste årtiondena, och inget talar för att den kommer att hejdas eller mattas av inom den närmaste framtiden.”[25]

Rätten till personlig integritet utgör en mänsklig rättighet, vilket stadgas i svensk grundlag genom regeringsformen, och återfinnes även i EU-stadgan och Europakonventionen.[26] Dataskyddsförordningen såsom generell reglering av personuppgifter inom unionen började tillämpas den 25 maj 2018 och ersatte därmed dataskyddsdirektivet. I dataskyddsförordningens första artikel utläses två primära syften. Artikeln anger att dataskyddsförordningen ämnar att främja överföringen av data inom unionen och till tredjeländer,

[24] Frydlinger m.fl. (2018), s.30.
[25] Prop. 1997/98:44, s. 30 och Frydlinger m.fl. (2018), s.30.
[26] Artikel 7 och 8 EU-stadgan, artikel 7 Europakonventionen och 2 kap 6 § regeringsformen.

samtidigt som en hög nivå ska säkerställas vid behandlingar[27] av fysiska personers personuppgifter.[28]

I beaktansskälen till dataskyddsförordningen anges att tidigare reglering inte gått den nya utvecklingen tillmötes. Den rättsliga säkerheten och smidigheten för fysiska personer, ekonomiska operatörer och myndigheter bör stärkas, och dataskyddet inom unionen kräver nu en stark och mer sammanhängande ram med stöd av ett kraftfullt tillsynsarbete.[29] Medlemsstaterna har genom olika implementeringar av dataskyddsdirektivet uppnått varierande skyddsnivåer.[30] I en rapport från kommissionen uttrycktes att skillnaderna mellan medlemsstaternas sätt att införliva direktivet kräver en rad olika lösningar. De registrerade[31] har begränsade kunskaper om sina rättigheter och tillsynsmyndigheterna betraktar inte dataskyddslagstiftningen som ett åtagande av hög prioritet.[32] Nya utmaningar vad gäller skyddet av personuppgifter har skapats av den snabba tekniska utvecklingen och globaliseringen sedan dataskyddsdirektivets tillkomst, vilka dataskyddsförordningen är avsedd att hantera.[33]

Sammantaget avser dataskyddsförordningen således att skydda fysiska personers personuppgifter, men även det fria flödet av personuppgifter inom unionen. Dataskyddsförordningen ämnar följaktligen till att värna om bådadera intressen, vilket resulterar i att skyddet för personuppgifter inte är en absolut rättighet.[34]

---

[27] En *behandling* (av personuppgifter) avser en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring. Se artikel 4 (2) dataskyddsförordningen.
[28] Artikel 1 och beaktandeskäl 6 och 101 dataskyddsförordningen.
[29] Beaktandeskäl 7 dataskyddsförordningen.
[30] Beaktandeskäl 9 dataskyddsförordningen.
[31] Den person vars personuppgifter behandlas. Se artikel 4 (1) dataskyddsförordningen.
[32] Kommissionens rapport KOM(2003) 265 slutlig, s. 11 f.
[33] Beaktandeskäl 5, 6 och 7 dataskyddsförordningen.
[34] Beaktandeskäl 4 dataskyddsförordningen och Datainspektionens allmänna råd, ”Allmän vägledning för integritetsanalys”, s. 6.

2.1.2 Territoriell tillämplighet

Med anledning av att uppsatsen syftar till att behandla det område inom dataskyddsförordningen som reglerar överföringar av personuppgifter från unionen till tredje land är det av vikt att utreda dataskyddsförordningens territoriella tillämplighet.

I skälen till dataskyddsförordningen betonas vikten av att den säkerhetsnivå som fysiska personer ges inom unionen genom denna förordning inte undermineras då överföring av personuppgifter sker från unionen till tredje land, utan en sådan överföring får endast ske i full överensstämmelse med dataskyddsförordningen.[35] En överföring av personuppgifter till tredje land regleras specifikt i kapitel V i dataskyddsförordningen.[36] Dataskyddsförordningen är således avsedd att tillämpas fullt ut för de personer som berörs av en överföring från en organisation inom unionen till en organisation i ett tredje land.

Vad beträffar begränsningar av dataskyddsförordningens tillämplighet, anger dataskyddsförordningen att då en personuppgiftsbehandling grundar sig på medlemsländernas nationella rätt ska begränsningen utgöra en nödvändig och proportionell åtgärd i ett demokratiskt samhälle.[37]

En avslutande aspekt som i detta sammanhang kan lyftas fram, men inte behandlas närmare på grund av avgränsningsskäl, är följande. Enligt dataskyddsförordningen torde artikel 3 (2) och kapitel V kunna tillämpas parallellt. I de fall artikel 3 (2) dataskyddsförordningen är tillämplig vid en överföring av personuppgifter till tredje land uppkommer därav frågan om inte kapitel V i dataskyddsförordningen blir överflödigt, då artikel 3 (2) i sig anger att dataskyddsförordningen fullt ut ska tillämpas.[38]

[35] Beaktandeskäl 101 dataskyddsförordningen.
[36] Artikel 44-50 dataskyddsförordningen.
[37] Jfr. till exempel beaktandeskäl 19, 50, 73 och artikel 6 (4) och 23 dataskyddsförordningen.
[38] Holtz, SvJT, 2018, s. 245.

2.1.3 Förutsättningar för överföring av personuppgifter till tredje land

Medlemsstaterna i unionen ska genom dataskyddsförordningen tillförsäkra ett harmoniserat skydd för personuppgifter för sina medborgare. I tredje land existerar dock inte samma generella regelverk som ger motsvarande garantier. Dataskyddsförordningen uppställer därför bestämmelser om under vilka förutsättningar det är tillåtet att överföra personuppgifter från unionen till tredje land, som under alla omständigheter endast får utföras i full överensstämmelse med dessa regler.[39]

Dataskyddsförordningen anger i kapitel V en hierarkisk ordning med de förutsättningar som fordras för en laglig överföring av personuppgifter till tredje land. Kapitlet fungerar såsom en verktygslåda[40] innehållandes mekanismer bestående av följande. I första hand får personuppgifter överföras om tredje land säkerställer en adekvat skyddsnivå.[41] I andra hand, om inte en adekvat skyddsnivå föreligger, får överföring ske om den personuppgiftsansvarige[42] eller personuppgiftsbiträdet[43] (företaget) inom unionen företagit lämpliga skyddsåtgärder. Standardavtalsklausuler betraktas såsom lämplig skyddsåtgärd.[44] I sista hand kan överföring ske om överföringen utgör en särskild situation.[45]

2.1.3.1 Adekvat skyddsnivå

En tredjelandsöverföring kan ske på grundval av att kommissionen beslutat att tredjelandet ifråga säkerställer en adekvat skyddsnivå.[46] Ett sådant beslut

[39] Beaktandeskäl 101 dataskyddsförordningen och Datainspektionen, *"Överföring till tredje land"*.
[40] Kommissionens meddelande KOM(2017) 7 final, s. 4.
[41] Artikel 45 dataskyddsförordningen.
[42] En *personuppgiftsansvarig* är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Med en e contrario-tolkning kan denne de facto inte vara personuppgiftsbiträde för den behandlingen. Se artikel 4 (7) dataskyddsförordningen och Juridisk Publikation 2/2017 s. 275.
[43] Ett *personuppgiftsbiträde* är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. Se artikel 4 (8) dataskyddsförordningen.
[44] Artikel 46 dataskyddsförordningen.
[45] Artikel 49 dataskyddsförordningen.
[46] Artikel 45 (1) dataskyddsförordningen.

bekräftar att ett tredje land genom nationell lagstiftning eller internationella åtaganden tillhandahåller en jämförbar nivå av skydd för personuppgifter i förhållande till unionslagstiftningen.[47]

Enligt grundläggande värderingar som unionen bygger på, exempelvis skyddet av mänskliga rättigheter, ska kommissionen basera sitt beslut på grundval av hur tredje land bland annat respekterar de mänskliga rättigheterna och de grundläggande friheterna, rättsstatsprincipen, relevant lagstiftning i landet, dataskyddsregler och om en effektivt fungerande oberoende tillsynsmyndighet finns.[48]

Ett beslut om adekvat skyddsnivå anses vara ett levande instrument.[49] Om tredjelandet inte längre kan säkerställa en adekvat skyddsnivå bör överföringen av personuppgifter förbjudas, undantaget om överföring som ovan nämnts kan ske med stöd av lämpliga skyddsåtgärder.[50]

Artikel 29-gruppen utarbetade en referensram[51] för adekvat skyddsnivå i samband med det tidigare dataskyddsdirektivets ikraftträdande. Till följd av införandet av dataskyddsförordningen och EU-domstolens dom i Maximillian Schrems-målet, valde artikel 29-gruppen att revidera denna referensram.[52] EU-domstolen angav att nivån av skydd måste vara väsentligen likvärdig med den adekvata skyddsnivå som garanteras inom unionen, men att metoderna som tredjelandet använder för att uppnå denna nivå av skydd får avvika från de medel unionen använder för att uppnå en adekvat säkerhetsnivå.[53]

2.1.3.2 Lämpliga skyddsåtgärder

Om kommissionen beslutar att tredjeland inte uppnår en adekvat skyddsnivå kan överföring av personuppgifter till tredjelandet ske om den

[47] Kommissionens meddelande KOM(2017) 7 final., s. 7.
[48] Beaktandeskäl 104 och artikel 45 (2 a – b) dataskyddsförordningen.
[49] Kommissionens meddelande KOM(2017) 7 final, s. 8.
[50] Beaktandeskäl 107 dataskyddsförordningen.
[51] Artikel 29-gruppens yttrande, WP 12.
[52] Artikel 29-gruppens yttrande, WP 254 rev. 01, s. 2.
[53] Mål C-362/14 *Maximillian Schrems mot Data Protection Commissioner*, p. 73 och 74.

personuppgiftsansvarige eller personuppgiftsbiträdet istället vidtar lämpliga skyddsåtgärder.[54] Skyddsåtgärderna kan företas i form av bindande företagsbestämmelser, standardbestämmelser om dataskydd som antagits av kommissionen (standardavtalsklausuler), standardbestämmelser om dataskydd som antagits av en tillsynsmyndighet eller avtalsbestämmelser som godkänts av en tillsynsmyndighet.[55]

Uppsatsen avgränsas och syftar till att utreda standardavtalsklausulerna, vilka ges en vidare utredning i avsnitt fyra.

2.1.4 Personuppgiftsincident

En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som behandlats.[56] En sådan incident kan innebära risker för människors fri- och rättigheter, till exempel identitetsstöld, bedrägeri eller skadat anseende.[57] Om en personuppgiftsincident sker ska den personuppgiftsansvarige anmäla incidenten till tillsynsmyndigheten utan dröjsmål. Den registrerade ska informeras om personuppgiftsincidenten utan dröjsmål, om incidenten sannolikt leder till hög risk för den registrerades fri- och rättigheter.[58]

[54] Artikel 46 (1) dataskyddsförordningen.
[55] Artikel 46 (2) och beaktandeskäl 108 dataskyddsförordningen.
[56] Artikel 4 (12) dataskyddsförordningen.
[57] Beaktandeskäl 85 dataskyddsförordningen.
[58] Artikel 33-34 dataskyddsförordningen.

3 Tidigare reglering avseende överföring av personuppgifter till tredje land

3.1 Dataskyddsdirektivet

Dataskyddsdirektivet var den generella reglering inom unionen avseende personuppgiftsbehandling innan det ersattes av dataskyddsförordningen den 25 maj 2018.[59] Samtliga uppsättningar standardavtalsklausuler är grundade på dataskyddsdirektivet. I syfte att uppnå en djupare förståelse för standardavtalsklausulernas uppbyggnad, men även för att utröna hur skyddet för personuppgifter och det fria flödet av personuppgifter har förändrats med införandet av dataskyddsförordningen, ges i detta kapitel en granskning av för uppsatsämnet relevanta avsnitt från dataskyddsdirektivet.

3.1.1 Bakgrund och syfte

Dataskyddsdirektivet utfärdades år 1995.[60] I beaktansskälen till dataskyddsdirektivet angavs att olikheter i nationella lagar resulterade i en skillnad i skyddsnivån för personuppgifter. Ett antal medlemsländer innehade en total avsaknad av dataskyddslagstiftning.[61] Nivåskillnaden konstaterades kunna utgöra hinder för att utöva en rad ekonomiska aktiviteter på gemenskapsnivå, varför en mer harmoniserad reglering var önskvärd.[62]

Syftet med dataskyddsdirektivet var dels att skydda fysiska personers grundläggande fri- och rättigheter i samband med behandling av personuppgifter, dels att medlemsstaterna inte skulle få begränsa eller förbjuda det fria flödet av personuppgifter.[63] Från ett rättsligt perspektiv

[59] Artikel 99 dataskyddsförordningen.
[60] Artikel 1 dataskyddsdirektivet.
[61] Kommissionens rapport KOM(2003) 265 slutlig, s. 12.
[62] Beaktandeskäl 7, 8 och 14 dataskyddsdirektivet.
[63] Artikel 1 dataskyddsdirektivet.

konstaterades att dataskyddsdirektivet i det väsentliga var inriktat på den fria rörligheten för personuppgifter.[64]

3.1.2 Förutsättningar för överföring av personuppgifter till trejde land

Dataskyddsdirektivet stadgade en hierarkisk ordning med regler för en lagenlig överföring av personuppgifter till tredje land. Huvudregeln var att personuppgifter fick överföras om tredje land säkerställde en adekvat skyddsnivå.[65] Om en adekvat skyddsnivå inte kunnat uppnås, fick överföring ske om den registeransvarige ställt tillräckliga garantier för att privatliv och enskilda personers grundläggande fri- och rättigheter skyddades.[66]

3.1.2.1 Adekvat skyddsnivå

I dataskyddsdirektivet stadgades att medlemsstaterna skulle föreskriva att överföringen av personuppgifter som var under behandling, eller som var avsedda att behandlas efter överföring till tredje land, endast fick ske om ifrågavarande tredje land säkerställde en adekvat skyddsnivå.[67] Huruvida skyddsnivån var adekvat skulle bedömas med hänsyn till nationell lagstiftning, uppgiftens art, den eller de avsedda behandlingarnas ändamål och varaktighet, ursprungslandet och det slutliga bestämmelselandet.[68] Dataskyddsdirektivet gav till sin ordalydelse, till skillnad från dataskyddsförordningen, ett utrymme för medlemsstaterna att själva avgöra huruvida tredjelandet uppfyllde en adekvat skyddsnivå.[69]

Artikel 29-gruppen angav i sin referensram för adekvat skyddsnivå att en sådan skyddsnivå kunde uppnås om dataskyddsdirektivet och övriga internationella akter om skydd för personuppgifter användes såsom utgångspunkt. Vidare anfördes att utanför unionen fanns sällan

[64] Kommissionens rapport KOM(2003) 265 slutlig, s. 12 och beaktandeskäl 3 dataskyddsförordningen.
[65] Artikel 25 (1) dataskyddsdirektivet.
[66] Artikel 26 (2) dataskyddsdirektivet.
[67] Artikel 25 (1) dataskyddsdirektivet.
[68] Artikel 25 (2) dataskyddsdirektivet.
[69] Datainspektionen, ”*Hur vet vi om ett tredje land har en adekvat skyddsnivå?”*.

förfarandemässiga instrument för att garantera efterlevnaden av principerna om skydd av personuppgifter. Som exempel angav Artikel 29-gruppen OECD:s riktlinjer i vilka bestämmelserna endast skulle *beaktas* och säkerställde således inte några instrument för att garantera att bestämmelserna de facto tillsåg det skydd som avsågs.[70]

3.1.2.2 Lämpliga garantier

Om en adekvat skyddsnivå inte kan uppnås, får en tredjelandsöverföring ske om den registeransvarige (nuvarande terminologi enligt dataskyddsförordningen är *"personuppgiftsansvarig"*) ställer tillräckliga garantier för att privatliv och enskilda personers grundläggande fri- och rättigheter skyddas samt för utövningen av motsvarande rättigheter. Tillräckliga garantier kan framgå av lämpliga avtalsklausuler.[71] Kommissionen kan besluta att standardavtalsklausuler ställer sådana tillräckliga garantier.[72] Standardavtalsklausulerna behandlas i en djupare utredning i avsnitt 4.

3.2 Safe Harbor-systemet

I kommissionens beslut om Safe Harbor-systemet återfanns de principer som möjliggjorde en lagenlig överföring av personuppgifter från unionen till USA.[73] Vid dataskyddsdirektivets ikraftträdande ansågs USA inte uppnå en adekvat skyddsnivå. Artikel 25 (6) dataskyddsdirektivet stadgade dock, att om ett tredje land inte uppnådde en adekvat skyddsnivå kunde kommissionen besluta att ett tredje land, genom sin interna lagstiftning eller internationella åtaganden, uppnådde en adekvat skyddsnivå.[74]

Ett anslutande till Safe Harbor-systemet genomfördes via självcertifiering, som skulle efterföljas av en offentlig deklaration om att principerna

[70] Artikel 29-gruppens yttrande, WP 12 s. 3 f.
[71] Artikel 26 (2) dataskyddsdirektivet.
[72] Artikel 25 (6) (2) dataskyddsdirektivet.
[73] Artikel 1 och beaktandeskäl 5, kommissionens beslut 2000/520/EG.
[74] Artikel 25 (6) dataskyddsdirektivet.

efterlevdes.[75] Efterlevnaden av principerna kunde begränsas om nationell lag uppställde krav hänförliga till nationell säkerhet, allmänintresset eller rättsefterlevnaden. Vidare kunde en avvikelse från principerna ske om nationella föreskrifter, lagar eller rättspraxis antingen gav uttryckliga befogenheter eller gav upphov till motstående skyldigheter. Avvikelsen var tvungen att anses vara nödvändig.[76]

Kommissionens beslut om Safe Harbor-systemet ogiltigförklarades år 2015 av EU-domstolen i Maximillian Schrems-målet[77], vilket avsnitt fem behandlar närmare.

[75] Artikel 1 (3), kommissionens beslut 2000/520/EG.
[76] Preambeln till bilaga 1 i kommissionens beslut 2000/520/EG.
[77] Mål C-362/14 *Maximillian Schrems mot Data Protection Commissioner* p. 106.

4 Standardavtalsklausuler

4.1 Överföring av personuppgifter till tredje land genom avtalsreglering

I de fall tredje land inte uppnår en adekvat skyddsnivå har det konstaterats att en överföring av personuppgifter ändå får ske om den registeransvarige (nuvarande terminologi enligt dataskyddsförordningen är *”personuppgiftsansvarig”*) ställer tillräckliga garantier för att privatliv och enskilda personers grundläggande fri- och rättigheter skyddas samt för utövningen av motsvarande rättigheter. Kommissionen kan besluta att vissa standardavtalsklausuler ställer de tillräckliga garantier som avses.[78] För en vidare förståelse av standardavtalsklausulerna som överföringsmekanism inleds detta avsnitt med en förklaring av skillnaden mellan avtalet vid en överföring inom unionen och avtalet vid en överföring från unionen till tredje land.

Vid en överföring av personuppgifter inom unionen är avtalets syfte att reglera ansvaret för hur personuppgiftsskyddet ska fördelas mellan överförare[79] och mottagare[80]. Avtalet vid en tredjelandsöverföring måste gå längre än vid en överföring inom unionen. Utöver ansvarsreglering krävs nämligen ytterligare garantier för den registrerade, eftersom mottagaren i tredje land inte behandlar personuppgifterna i enlighet med ett adekvat skydd.[81] Standardavtalsklausulerna ska fungera såsom mallar och uppväga de brister som finns i tredjelandets skydd för personuppgifter.[82]

I de flesta fall hanteras standardavtalsklausulerna som en bilaga till avtalet. [83] Avtalsparterna kan välja att införliva standardavtalsklausulerna i avtalet, i

[78] Artikel 26 dataskyddsdirektivet.
[79] Den aktör i unionen som överför personuppgifterna till tredje land.
[80] Den aktör i tredje land som mottar personuppgifterna från unionen.
[81] Artikel 29-gruppens yttrande, WP 9 s. 2 ff. och 1/2001, s. 3.
[82] Beaktandeskäl 1, kommissionens beslut 2004/915/EG och WP 9 s. 3.
[83] Frydlinger m.fl. (2018), s. 243.

vilket andra avtalsvillkor får tilläggas avtalet under förutsättning att de inte strider mot standardavtalsklausulerna.[84]

Idag finns två centrala varianter av standardavtalsklausuler, som fortsätter att tillämpas till dess att kommissionen ändrar eller ersätter dem.[85] En variant tillämpas för en överföring av personuppgifter där både överförare och mottagare är personuppgiftsansvariga, som i en uppsättning godkändes år 2001[86] och i en reviderad ytterligare uppsättning år 2004.[87] Överförare och mottagare kan fritt välja en av dessa uppsättningar standardavtalsklausuler.[88] Den andra varianten av standardavtalsklausuler beslutades år 2010 och tillämpas för en överföring då överföraren är personuppgiftsansvarig och mottagaren är ett personuppgiftsbiträde.[89]

4.1.1 Kommissionens beslut om standardavtalsklausuler år 2001

I 2001 års uppsättning av standardavtalsklausuler ska information om vilka kategorier av personuppgifter som behandlas och för vilka ändamål överföringen grundas på ses såsom en inordnad del av standardavtalsklausulerna.[90] Överföraren ska garantera att personuppgiftsbehandlingen, till och med överföringen, överensstämmer med rådande skydd i den medlemsstat där överföraren är etablerad.[91]

Mottagaren av personuppgifterna ska garantera att denne inte har anledning att förmoda att nationell lagstiftning hindrar efterlevnaden av avtalsvillkoren. Överföraren av personuppgifter får häva avtalet om lagstiftningen i tredje landet ändras så att standardavtalsklausulerna troligtvis påverkas

[84] Frydlinger m.fl. (2018), s. 242 f., och Voigt och von dem Bussche (2017) pp. 87-140 samt beaktandeskäl 5, kommissionens beslut 2001/497/EG.
[85] Frydlinger m.fl. (2018), s. 242.
[86] Kommissionens beslut 2001/497/EG.
[87] Kommissionens beslut 2004/915/EG.
[88] Beaktandeskäl 3, kommissionens beslut 2004/915/EG.
[89] Kommissionens beslut 2010/87/EU.
[90] Klausul 2 kommissionens beslut 2001/497/EG.
[91] Ibid, klausul 4.

ofördelaktigt.[92] Vidare ska mottagaren följa ett antal obligatoriska principer[93] som följer av avtalsvillkoren, vilka ska tolkas i ljuset av dataskyddsdirektivet. Principerna kan undantas vid obligatorisk tillämpning av mottagarens nationella rätt såvida de nationella kraven går att hänföra till exempelvis statens säkerhet, allmän säkerhet och försvaret.[94]

De nationella tillsynsmyndigheterna inom unionen får förbjuda eller tillfälligt avbryta flödet av personuppgifter till tredje land, om krav i tredjelandets nationella lagstiftning resulterar i att personuppgiftsskyddet frångås på ett sätt som går utöver de restriktioner[95] som krävs i ett demokratiskt samhälle enligt dataskyddsdirektivet. Kraven måste sannolikt ha en avsevärd negativ inverkan på de garantier som ges i standardavtalsklausulerna. Ett förbud eller ett tillfälligt avbrytande av flödet av personuppgifter till tredje land får också ske om mottagaren inte efterlevt standardavtalsklausulerna, eller om det finns skälig anledning att anta att standardavtalsklausulerna inte följs. En fortsatt överföring ska medföra en överhängande risk för allvarlig skada för de registrerade.[96]

I de fall det föreligger ett gemensamt personuppgiftsansvar[97] för överförare och mottagare ställer artikel 26 i dataskyddsförordningen krav på ett ”inbördes arrangemang”. Kravet bör tillmätas större betydelse än under tidigare dataskyddslagstiftning.[98] Parterna ska under öppna former fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt dataskyddsförordningen, och det väsentliga innehållet i arrangemanget ska tillgängliggöras för den registrerade.[99]

---

[92] Klausul 5 (a), kommissionens beslut 2001/497/EG.
[93] Principerna avser ändamålsbegränsning, uppgifternas kvalitet och proportionalitet, informationsplikt, säkerhet och sekretess, rätt till tillgång, rättelse, utplåning och invändning, begränsning av vidareöverföring, särskilda kategorier av uppgifter, direkt marknadsföring samt databehandlade beslut om enskilda, se princip 1-9 tillägg 2 och princip 1-3 tillägg 3, kommissionens beslut 2001/497/EG.
[94] Preambeln till tillägg 2 och 3 och klausul 5 (b), kommissionens beslut 2001/497/EG.
[95] Till exempel statens säkerhet, försvaret, allmän säkerhet, förebyggande, undersökning, och avslöjande av brott. Se artikel 13 dataskyddsdirektivet.
[96] Artikel 4, kommissionens beslut 2001/497/EG.
[97] Om två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen med och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga. Se artikel 26 dataskyddsförordningen.
[98] Juridisk Publikation 2/2017, s. 273.
[99] Artikel 26 (1) och (3) dataskyddsförordningen.

4.1.2 Kommissionens beslut om standardavtalsklausuler år 2004

Kommissionens beslut om 2004 års standardavtalsklausuler fattades för att ett antal handelssammanslutningar utformat en annan variant av standardavtalsklausuler utöver 2001 års standardavtalsklausuler. Uppsättningen av 2004 års standardavtalsklausuler överensstämmer med det personuppgiftsskydd som återfinnes i 2001 års standardavtalsklausuler, men är bättre lämpade för ekonomiska aktörer.[100]

De nationella myndigheterna inom unionen får förbjuda eller tillfälligt avbryta flödet av personuppgifter till tredje land i de fall överföraren vägrar att efterleva standardavtalsklausulerna eller om denne, efter meddelande från tillsynsmyndighet, vägrar att vidta adekvata åtgärder för att tillämpa standardavtalsklausulerna gentemot mottagaren inom en månad. En förvägran är undantagen såtillvida det förekommer obligatoriska krav i nationell lagstiftning som inte går utöver vad som är nödvändigt i ett demokratiskt samhälle enligt dataskyddsdirektivet.[101]

4.1.3 Kommissionens beslut om standardavtalsklausuler år 2010

För en lagenlig överföring av personuppgifter från en personuppgiftsansvarig inom unionen till ett personuppgiftsbiträde etablerat i tredje land återfinns 2010 års standardavtalsklausuler. Mottagaren av personuppgifterna får enbart behandla dessa för överförarens räkning och i enlighet med dennes instruktioner.[102] Mottagaren kan lägga ut sin uppgiftsbehandlingstjänst på entreprenad. Därigenom överför mottagaren personuppgifterna till en underentreprenör (nuvarande terminologi enligt dataskyddsförordningen är

[100] Beaktandeskäl 2, 4 och 12, kommissionens beslut 2004/915/EG.
[101] Se artikel 13 dataskyddsdirektivet och artikel 1 (2), kommissionens beslut 2004/915/EG.
[102] Beaktandeskäl 15 kommissionens beslut 2010/87/EU.

”*underbiträde”*[103]*)*, vilket får ske med överförarens föregående samtycke. Utläggningen ska ske genom ingående av skriftligt avtal.[104]

De nationella tillsynsmyndigheterna bör ha rätt att förbjuda eller avbryta en överföring av personuppgifter då det konstaterats att en överföring sannolikt har en avsevärt skadlig inverkan på de garantier som ska säkerställa adekvat skydd för den registrerade. Förbud eller avbrytande av flödet av personuppgifter får ske då mottagaren eller ett underbiträde enligt nationell lagstiftning går utöver de restriktioner som krävs i ett demokratiskt samhälle enligt dataskyddsdirektivet, eller om det finns skälig anledning att anta att standardavtalsklausulerna inte efterlevs. I sistnämnda fall krävs, för att tillsynsmyndigheten ska få genomföra ett förbud eller ett avbrytande av överföringen, att en fortsatt överföring medför en överhängande risk för allvarlig skada för den registrerade.[105]

I dataskyddsförordningens artikel 28 återfinnes regler för när en personuppgiftsansvarig överför personuppgifter till ett personuppgiftsbiträde. Artikeln föreskriver att personuppgiftsbehandlingen ska föregås av ett avtal eller annan rättsakt som är bindande för personuppgiftsbiträdet med avseende på den personuppgiftsansvarige. Rättsakten ska ange föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter. Artikeln anger sedan en uppräkning av skyldigheter för personuppgiftsbiträdet som rättsakten ska reglera, till exempel skyldigheten att respektera villkoren för anlitande av ett underbiträde.[106]

[103] Ett personuppgiftsbiträde som behandlar personuppgifter för den personuppgiftsansvariges räkning har ofta själv anlitat en underleverantör, som benämns underbiträde i kedjan av personuppgiftsbehandlare. Det kan således skapas en lång kedja av personuppgiftsbehandlare. Se artikel 28 dataskyddsförordningen.
[104] Klausul 11 kommissionens beslut 2010/87/EU.
[105] Beaktandeskäl 11 kommissionens beslut 2010/87/EU.
[106] Beaktandeskäl 79 och artikel 28 (3) dataskyddsförordningen.

5 Maximillian Schrems mot Data Protection Commissioner

5.1 Bakgrund

År 2013 anförde kommissionen att unionsmedborgares personuppgifter som överfördes till USA genom tillämpning av Safe Harbor-systemet var tillgängliga för amerikanska myndigheter. Personuppgifterna kunde bli föremål för en behandling som strider mot syftet för vilket personuppgifterna ursprungligen samlades in. I samband med Edward Snowdens avslöjanden år 2013 om den amerikanska underrättelsetjänstens program uttryckte de tyska dataskyddsmyndigheterna att de var bekymrade över att Safe Harbor-principerna med stor sannolikhet överträddes.[107] Dessa övervakningsprogram tillämpades på de flesta amerikanska internetföretag som var anslutna till Safe Harbor-systemet. Safe Harbor-principerna öppnade således upp en väg för den amerikanska underrättelsetjänsten att få tillgång till personuppgifter som ursprungligen behandlats inom unionen, där organ såsom National Security Agency och Federal Bureau of Investigation kunde ägna sig åt övervakning i stor omfattning.[108]

Maximillian Schrems är österrikisk medborgare och användare av Facebook. Vid registrering till Facebook ingås ett avtal med Facebook Irland, dotterbolag till Facebook Inc., som har sitt verksamhetsställe i USA. Unionsmedborgares personuppgifter som insamlas av Facebook Irland överförs till Facebook Inc. Maximillian Schrems inkom med en anmälan till ombudsmannen i vilken han begärde att överföringen av personuppgifter från Facebook Irland till Facebook Inc. skulle förbjudas, eftersom Safe Harbor-systemet inte säkerställde en adekvat skyddsnivå i den mening som avses i dataskyddsdirektivet.[109] Hans begäran gick vidare till High Court of Ireland

[107] Kommissionens meddelande KOM(2013) 847 final, s. 5.
[108] Mål C-362/14 *Maximillian Schrems mot Data Protection Commissioner,* p. 14, 22 och 31.
[109] Artikel 25 dataskyddsdirektivet och mål C-362/14 *Maximillian Schrems mot Data Protection Commissioner*, p. 27-28.

som hänsköt frågan till EU-domstolen med en begäran om förhandsavgörande.[110]

5.2 Ogiltigförklarandet av Safe Harbor-systemet

I Maximillian Schrems-målet förklarades Safe Harbor-principerna ogiltiga.[111] EU-domstolen anförde att artikel 25 (6) i dataskyddsdirektivet, som möjliggjorde att ett tredje land genom sin interna lagstiftning eller internationella åtaganden anses uppnå en adekvat skyddsnivå, i och för sig inte kräver en identisk skyddsnivå som unionen ska garantera.[112] Skyddsnivån för den personliga integriteten ska dock de facto säkerställa en motsvarighet som är väsentligen likvärdig med unionens, eftersom skyddsnivån och syftet med bestämmelsen annars kan kringgås. Kommissionen ska bedöma innehållet i tredjelandets interna lagstiftning, praxis eller internationella åtaganden, samt regelbundet säkerställa att eventuella förändringar av den interna lagstiftningen fortfarande motsvarar en adekvat skyddsnivå.[113] Kommissionen ansågs inte uppfylla sin skyldighet att konstatera genom vilka åtgärder i sin interna lagstiftning eller internationella åtaganden USA vidtog för att uppnå en adekvat skyddsnivå.[114]

Som angivits i avsnitt 3.2 kunde krav i nationell lagstiftning vad beträffade nationell säkerhet, allmänintresset eller intern lagstiftning medföra att Safe Harbor-principerna inskränktes. EU-domstolen konstaterade att detta undantag var av generell karaktär och att dessa nationella krav gavs företräde framför Safe Harbor-principerna. Organisationer i USA kunde därmed frångå principerna utan begränsningar.[115] EU-domstolen anförde att det saknades ett konstaterande av kommissionen om att amerikanska myndigheter kan få

[110] Mål C-362/14 *Maximillian Schrems mot Data Protection Commissioner*, p. 36.
[111] Ibid p. 106.
[112] Ibid p. 73.
[113] Ibid p. 75-76.
[114] Ibid p. 83.
[115] Ibid p. 86.

åtkomst till personuppgifterna vid legitima syften, till exempel nationell säkerhet. Likaså saknar Safe Harbor-systemet ett effektivt rättsligt skydd mot sådana ingrepp.[116] Personuppgiftsbehandlingen har i dessa fall konstaterats gå utöver vad som är strängt nödvändigt och proportionerligt för att tillgodose den nationella säkerheten. Behandlingen är inte strängt nödvändig då lagstiftningen möjliggör en generell lagring av personuppgifter såtillvida det inte anges begränsningar eller undantag med hänsyn till det syfte som ska motivera ingreppet. En senare användning måste avgränsas till bestämda, strängt begränsade syften som kan motivera detta ingrepp.[117]

EU-domstolen anförde att artikel 3 (1) i Safe Harbor-principerna undantog de nationella tillsynsmyndigheternas befogenheter som de tilldelats i artikel 28 dataskyddsdirektivet, eftersom artikel 3 (1) i Safe Harbor-principerna utgjorde ett hinder för tillsynsmyndigheterna att säkerställa att artikel 25 dataskyddsdirektivet om en adekvat skyddsnivå efterlevdes.[118] De nationella tillsynsmyndigheterna hade enligt artikel 28 dataskyddsdirektivet möjlighet att göra en fullständigt oberoende utredning av varje begäran om skydd för en persons fri- och rättigheter om personuppgiftsbehandling rörande vederbörande.[119]

Mot bakgrund av angivna skäl ogiltigförklarade EU-domstolen Safe Harbor-systemet då systemet enligt artikel 25 (6) i dataskyddsdirektivet inte gick dess krav tillmötes.[120] Eftersom överföringar av personuppgifter är en viktig del av de transatlantiska förbindelserna antogs dock därefter ett nytt beslut för att uppnå lagenliga överföringar av personuppgifter från unionen till USA.[121] Nuvarande rätt utgörs av *Privacy Shield*[122] som amerikanska företag kan ansluta sig till, men som inte kommer att beröras närmare på grund av utrymmesskäl.

[116] Ibid p. 88-89.
[117] Ibid p. 93.
[118] Ibid p. 101-102.
[119] Artikel 28 (3) dataskyddsdirektivet och mål C-362/14 *Maximillian Schrems mot Data Protection Commissioner* p. 99.
[120] Mål C-362/14 *Maximillian Schrems mot Data Protection Commissioner* p. 98.
[121] Kommissionens meddelande KOM(2015) 566 final, s. 2.
[122] Beaktandeskälen till kommissionens genomförandebeslut C/2016/4176.

5.2.1 Beslut om att ändra standardavtalsklausulerna efter ogiltigförklarandet av Safe Harbor-systemet

Till följd av ogiltigförklarandet av Safe Harbor-systemet antog kommissionen ett beslut om ändring av 2001- och 2010 års standardavtalsklausuler.[123] Revideringen avsåg artikel 4 i bådadera uppsättningar standardavtalsklausuler, med hänsyn till EU-domstolens utlåtande om artikel 3 (1) i Maximillian Schrems-målet. Artikel 4 i standardavtalsklausulerna utgjorde en inskränkning av de nationella tillsynsmyndigheternas befogenheter som var jämförbar med artikel 3 (1) i de ogiltigförklarade Safe Harbor-principerna.[124]

[123] Beaktandeskälen till kommissionens genomförandebeslut C/2016/8471.
[124] Artikel 1 och 2 och beaktandeskäl 6 och 7, kommissionens genomförandebeslut C/2016/8471.

6 Analys

I följande avsnitt ges en återkoppling till de frågeställningar som presenterades i avsnitt ett. Uppsatsen har sökt att identifiera de nya bestämmelserna i dataskyddsförordningen som är relevanta för standardavtalsklausulerna. De tolkningsprinciper som EU-domstolen tillämpade i Maximillian Schrems-målet för ogiltigförklarandet av Safe Harbor-systemet har utretts i avsnitt fem. Dessa strukturer appliceras nedan på standardavtalsklausulerna i en tolkning av huruvida dessa strider mot gällande rätt.

6.1 Standardavtalsklausulerna i förhållande till dataskyddsförordningen

Standardavtalsklausulerna antogs genom beslut av kommissionen under dataskyddsdirektivets tid. Kommissionen konstaterade att det övervägande syftet i dataskyddsdirektivet, sett från ett rättsligt perspektiv, varit att underlätta det fria flödet för personuppgifter. Innan dataskyddsdirektivets ikraftträdande förekom hinder för denna rörlighet, eftersom unionsländerna hade olika lagstiftningar eller fullständigt saknade lagstiftning på området. Med dataskyddsförordningens införande finner uppsatsen ett syftesskifte. I beaktansskälen till dataskyddsförordningen anges att tidigare reglering inte gått den nya utvecklingen tillmötes, där medlemsstaterna genom olika implementeringar av dataskyddsdirektivet uppnått varierande skyddsnivåer för personuppgifter. Den personliga integriteten och tillsynsarbete har fått ett ökat fokus, med hänsyn till de utmaningar den tekniska utvecklingen och globaliseringen gett upphov till. Fysiska personer bör idag, undantaget att dataskyddslagstiftningen inte föreskriver annat, ha kontroll över sina personuppgifter. Företag ska inte behandla en personuppgift såsom en ägodel. Utgångspunkten är att uppgifterna är företag till låns och där ett tydligt syfte till respektive kategori av personuppgift kan anges.

Standardavtalsklausulernas principer ska enligt sin ordalydelse tolkas i ljuset av dataskyddsdirektivet. Med dataskyddsförordningens ikraftträdande finner uppsatsen att detta bör förstås som att principerna i standardavtalsklausulerna idag ska tolkas med ledning av denna förordning. En annan tolkning torde i sig strida mot dataskyddsförordningen. De inledande beaktansskälen till dataskyddsförordningen anger att en överföring till tredje land endast får ske i full överensstämmelse med nämnda förordning. Standardavtalsklausulernas principer sätts således i ett annat ljus genom tillämpningen av dataskyddsförordningen.

Dataskyddsförordningen medför även striktare krav vad beträffar det inbördes arrangemang som ska göras i de fall en personuppgiftsöverföring sker. För en överföring av personuppgifter mellan en personuppgiftsansvarig och ett personuppgiftsbiträde ska de bestämmelser som stadgas i artikel 28 dataskyddsförordningen följas. Artikeln avspeglas dock inte fullt ut i 2010 års standardavtalsklausuler för en sådan avtalsrelation. Vidare anges i artikel 26 dataskyddsförordningen, i de fall de personuppgiftsansvariga är gemensamt personuppgiftsansvariga, ett krav på ett inbördes arrangemang som konstaterats torde få en större betydelse i dataskyddsförordningen än tidigare dataskyddslagstiftning. Standardavtalsklausulerna bygger i detta hänseende på dataskyddsdirektivet, och torde därmed sakna ett fullgott skydd som i sin helhet står i överensstämmelse med dataskyddsförordningen. Ett företag eller organisation som lyder under dataskyddsförordningen bör tills vidare undersöka de delar i artikeln som inte redan reglerats parterna emellan, och komplettera de krav som uppställs.

6.2 Standardavtalsklausulerna i förhållande till Safe Harbor-systemet

Uppsatsen finner att standardavtalsklausulerna innehåller liknande materiella svagheter som det ogiltigförklarade Safe Harbor-systemet. Som konstaterats

i avsnitt tre och fyra möjliggör bådadera överföringsmekanismer att undantag med hänsyn till nationell rätt kan ske, om avvikelsen är nödvändig. Vad beträffar den interna lagstiftningen i USA konstaterades det i Maximillian Schrems-målet att amerikansk lag de facto hade företräde framför Safe Harbor-principerna på grund av principernas generella karaktär. Under förutsättning att Safe Harbor-principerna stod i strid med amerikansk lagstiftning kunde de självcertifierade företagen frångå principerna. EU-domstolen konstaterade dock att personuppgifterna inte behandlades inom ramen för vad som är *strängt* nödvändigt. Enligt Maximillian Schrems-målet antyds att kravet för en överträdelse av skyddet för personuppgifter, baserad på en generellt utformad bestämmelse som möjliggör att ett tredje lands nationella rätt ges företräde, stramas upp.

Standardavtalsklausulerna ger de nationella myndigheterna en rätt att förbjuda eller tillfälligt avbryta flödet av personuppgifter till tredje land, om tredje lands nationella lagstiftning resulterar i att personuppgiftsskyddet frångås på ett sätt som går utöver de restriktioner som krävs i ett demokratiskt samhälle enligt dataskyddsdirektivet. Kraven måste sannolikt ha en avsevärt negativ inverkan på de garantier som ges i standardavtalsklausulerna. Ett förbud eller avbrytande av flödet kan även ske om det finns skälig anledning att anta att standardavtalsklausulerna inte efterlevs och att en fortsatt överföring medför en överhängande risk för allvarlig skada för de registrerade.

Uppsatsen finner att det går att argumentera för att dessa bestämmelser är vaga till sin utformning, och ger ett tredje land ett relativt stort utrymme att åsidosätta standardavtalsklausulerna. Bestämmelsen kräver nämligen att överträdelsen av standardavtalsklausulerna, *utöver* att personuppgiftsskyddet ska frångås på ett sätt som går utöver de restriktioner som krävs i ett demokratiskt samhälle, har en avsevärt negativ inverkan på de garantier som ges i standardavtalsklausulerna. Skyddet för personuppgifter torde äventyras så snart överträdelsen går utöver de restriktioner för vad om krävs i ett demokratiskt samhälle. Att det dessutom appliceras ett högt krav, där

inverkan på garantierna ska vara avsevärt negativ, möjliggör att personuppgiftsskyddet och standardavtalsklausulerna med ett ännu större utrymme kan åsidosättas av tredje lands nationella rätt. För att anknyta till dataskyddsförordningen anges i avsnitt två, att om en begränsning av en behandling av personuppgifter sker i överensstämmelse med dataskyddsförordningen, ska denna begränsning utgöra en nödvändig och proportionell åtgärd i ett demokratiskt samhälle. Genom ett krav där inverkan på standardavtalsklausulerna ska vara avsevärt negativ är det därför möjligt att standardavtalsklausulerna ger allt för stora öppningar som gör att ett tredjelands nationella rätt ges företräde framför principerna i standardavtalsklausulerna. Det finns därför en risk för att skyddet för personuppgifter på detta sätt åsidosätts.

I de fall ett förbud eller avbrytande av flödet istället sker med hänsyn till en överhängande risk för allvarlig skada uppkommer frågan hur begreppet ”allvarlig skada”, ska tolkas. Begreppet är av generell karaktär och öppnar upp för tolkningsfrågor. En personuppgiftsincident enligt dataskyddsförordningen är en säkerhetsincident där en personuppgift har blivit förstörd, gått förlorad eller kommit i orätta händer, och som innebär en risk för den registrerades fri- och rättigheter. Dataskyddsdirektivet innehåller inga förfaranderegler för vad parterna ska göra vid en personuppgiftsincident. Företag som faller inom dataskyddsförordningens tillämpning torde i detta hänseende, för att vara förenliga med gällande rätt, tolka klausulen i ljuset av dataskyddsförordningen tills rättsläget är klarlagt.

6.3 Avslutande kommentar

Även om ett av dataskyddsförordningens syften utgör ett kommersiellt sådant, med en strävan efter att underlätta flödet av personuppgifter till tredje land, väger detta syfte i förevarande fall inte tyngre än en hög nivå av skydd för personuppgifter. Att tillämpa standardavtalsklausulerna kan medföra en risk för att detta skydd åsidosätts. I vissa delar är standardavtalsklausulerna

otillräckligt utformade för att överensstämma med dataskyddsförordningen. Standardavtalsklausulerna påvisar även likande bristfälligheter som det ogiltigförklarade Safe Harbor-systemet präglades av.

Sammantaget finner uppsatsen att företag och organisationer bör tillämpa samtliga standardavtalsklausuler med stor försiktighet.

7 Käll- och litteraturförteckning

Offentligt tryck

EU

Beslut, meddelanden och rapporter

Kommissionens beslut av den 15 juni 2001 om standardavtalsklausuler för överföring av personuppgifter till tredje land enligt direktiv 95/46/EG

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

Kommissionens beslut av den 27 december 2004 om ändring av beslut 2001/497/EG om standardavtalsklausuler för överföring av personuppgifter till tredje land

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

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

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

Kommissionens genomförandebeslut (EU) 2016/2297 av den 16 december 2016 om ändring av beslut 2001/497/EG och 2010/87/EU rörande standardavtalsklausuler för överföring av personuppgifter till tredjeländer och till registerförare etablerade i tredjeländer i enlighet med Europaparlamentets och rådets direktiv 95/46/EG

Kommissionens rapport – Första rapporten om genomförandet av dataskyddsdirektivet (95/46/EG), KOM(2003) 265 slutlig, 15 maj 2003

Meddelande från kommissionen till Europaparlamentet och rådet “Om hur principerna om integritetsskydd (safe harbour) fungerar när det gäller EU:s

medborgare och företag som är etablerade i EU”, KOM(2013) 847 final, 27 november 2013

Meddelande från kommissionen till Europaparlamentet och rådet ”Om överföring av personuppgifter från EU till Amerikas förenta stater enligt direktiv 95/46/EG med anledning av domstolens dom i mål C-362/14 (Schrems)”, KOM(2015) 566 final, 6 november 2015

Meddelande från kommissionen till Europaparlamentet och rådet ”Utbyte och skydd av personuppgifter i en globaliserad värld”, KOM(2017) 7 final, 10 januari 2017

Meddelande från kommissionen till Europaparlamentet och rådet, ”Återskapande av förtroendet för dataflöden mellan EU och Förenta staterna”, KOM(2013) 846 final, 27 november 2013

Rekommendationer och yttranden

Artikel 29-gruppens yttrande 1/2001 ”Utkastet till kommissionens beslut om standardavtalsklausuler för överföring av personuppgifter till tredje land enligt artikel 26.4 i direktiv 95/46”, antagen 26 januari 2001

Artikel 29-gruppens yttrande 8/2003 ”Om förslaget till standardavtalsklausuler som framlagts av en grupp näringslivsorganisationer (”det alternativa standardavtalet”)”, antagen 17 december 2003

Artikel 29-gruppens yttrande WP 12 ”Överföring av personuppgifter till tredje land: tillämpning av artiklarna 25 och 26 i EU:s dataskyddsdirektiv”, antagen 24 juli 1998

Artikel 29-gruppens yttrande WP 254 rev.01 ”Adequacy Referential”, antagen 28 November 2017

Artikel 29-gruppens yttrande WP 9 ”Utkast till arbetsdokument: Användning av avtalsreglering vid överföring av personuppgifter till tredje land”, antagen 1998

Förordning och direktiv

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

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG

Svensk rätt

Propositioner

Prop. 1997/98:44

Vägledningar, rekommendationer och yttranden

Datainspektionens allmänna råd, ”*Allmän vägledning för integritetsanalys*” nr 1/2017

Litteratur

Bernitz, Ulf; Heuman, Lars; Leijonhufvud, Madeleine; Seipel, Peter; Vogel, Hans-Heinrich: *Finna rätt: juristers källmaterial och arbetsmetoder*, Norstedts juridik, Stockholm 2014

Derlén Mattias; Ingmansson Staffan & Lindholm Johan: *Grundläggande EU-rätt*, Liber, 2015

Frydlinger, David; Edvardsson, Tobias; Olstedt Carlström Caroline & Beyer, Sandra, *GDPR: - Juridik, organisation och säkerhet enligt dataskyddsförordningen*, 2018

Kahn, Johan & Gustafsson, Fredrik, Juridisk publikation: vid Stockholms universitet, *Gemensamt personuppgiftsansvar – vanligare under GDPR?*, i Juridisk publikation, nr. 2, Stockholm, 2017

Voigt, Paul & von dem Bussche, Axel, *The EU general data protection regulation (GDPR) - A Practical Guide*, Cham, 2017

Artiklar

Holtz, Hajo Michael ”*Den nya allmänna dataskyddsförordningen – några anmärkningar*”, Svensk Juristtidning 2018.

Elektroniska källor

Datainspektionen, *Överföring till tredje land*, https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/tredjelandsoverforing/ (hämtad 2018-10-20)

Datainspektionen, *Hur vet vi om ett tredje land har en adekvat skyddsnivå?,* https://www.datainspektionen.se/lagar--

regler/dataskyddsforordningen/tredjelandsoverforing/hur-vet-vi-om-ett-tredje-land-har-adekvat-skyddsniva/ (Hämtad 2018-11-29)

Rättsfallsförteckning

EU-domstolen

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

C-311/18 *Data Protection Commissioner mot Facebook Ireland Limited, Maximillian Schrems,* ännu inte publicerad i REU