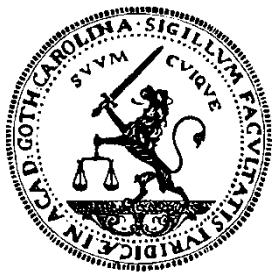

JURIDISKA FAKULTETEN
vid Lunds universitet

Helga Söderström

Adekvat skyddsnivå vid dataöverföring till USA enligt artikel 45 GDPR

LAGF03 Rättsvetenskaplig uppsats

Kandidatuppsats på juristprogrammet
15 högskolepoäng

Handledare: Marja-Liisa Öberg

Termin: HT2020

Innehållsförteckning

Abstract

In 2018, the European Union's *General Data Protection Regulation* (the GDPR) was incorporated into Swedish law, and data protection as such was increasingly noticed and given attention in the media. However, the emergence of data protection began a lot earlier than 2018 and is an important matter as for both individuals such as the state and companies.

Through rapid technological development and smart algorithms, personal information is an increasingly valuable asset for both companies and the state. At the same time, the population is unaware of how their personal data is being collected and how it is used. With increased mass processing of personal data, there is a risk for individuals privacy protection to not be respected. The GDPR therefore sets out several requirements for processing in order to ensure a high level of protection for the privacy of individuals.

Within the EU, there is free movement of personal data, but for transfer of data to third countries such as the United States, the GDPR set out special requirements. One of the requirements for the transfer is that it must ensure an adequate level of protection. The European Commission can, through a decision on adequate level of protection, validate transfers to a third country. Following a decision on adequate level of protection, transfers to the country may take place without any special permissions.

Since the annulment of both of the European Commission's decision on the adequate level of protection for the transfer of personal data to the United States by the European Court of Justice, there is a great need for guidance on what constitutes an essentially equivalent level of protection of personal data.

In a comparative analysis of data protection regulations in the EU and USA, this thesis finds that the perception of individuals' integrity is significantly

different between the EU and USA. The conflicting view of integrity and the rights of individuals is affeciting the European Commissions' work in drafting a new decision. In order for a new decision to be adopted, the thesis has identified three main factors for an adequate level of protection to be considered essentially equivalent to the protection of European citizens personal information within the EU given by the GDPR. The factors are based on case law from the European Court of Justice and depict how a new decision should be exempted and how European citizens' rights can be met in the United States. The fundamental differences between the EU and US data protection are inevitable, but in order to meet a new agreement both parties should strive for harmonization. Finally, the thesis finds that the restrictive and unlimited intelligence laws in the United States must be revised in order for a new decision on an adequate level of protection to be made.

Sammanfattning

År 2018 införlivades Europeiska Unionens dataskyddsförordning i svensk rätt och dataskydd som ämne fick en allt större uppmärksamhet i media och i debatt. Dataskyddets framväxt började dock tidigare än så och är en viktig fråga för både enskild individ som för stat och företag.

Tack vare en snabb teknisk utveckling och smarta algoritmer är personlig information en allt mer värdefull tillgång hos både företag som stat. Samtidigt syns en okunskap hos befolkningen i hur deras personuppgifter samlas in och hur de används. Vid en ökad massbehandling av personuppgifter uppstår en risk för att individers integritetsskydd inte tas tillvara på. Dataskyddsförordningen ställer därför upp flera krav på behandlingen för att säkerställa en hög skyddsnivå för individers integritet.

Inom EU råder fri rörlighet av personuppgifter men för överföring till tredjeland som exempelvis USA ställer dataskyddsförordningens regelverk upp särskilda krav. Ett av kraven för överföring av personlig information handlar om att överföringen måste säkerställa en adekvat skyddsnivå. Ett beslut om att behandling uppfyller kraven på adekvat skyddsnivå kan fattas av Europeiska Kommissionen och överföring till tredjeland får då ske utan något särskilt tillstånd.

Efter att Europeiska kommissionens båda beslut om adekvat skyddsnivå för överföring av personuppgifter till USA har ogiltigförklarats av EU-domstolen är behovet av vägledning stort kring vad som är ett väsentligt likvärdig skydd av personuppgifter likt det skydd som ges europeiska medborgare inom unionen vid överföring av data till USA.

I en komparativ analys av dataskyddets regelverk i EU respektive USA finner uppsatsen att synen på individers integritet skiljer sig väsentligt åt mellan USA respektive EU. Den motstridiga synen på integritet och

enskildas rättigheter påverkar i förlängningen kommissionens arbete vid utformningen av ett nytt beslut. För att ett nytt beslut ska kunna antas har uppsatsen identifierat främst tre faktorer för att en adekvat skyddsnivå ska anses väsentligt likvärdig skyddet för europeiska medborgares personliga information inom EU. Faktorerna grundar sig i rättspraxis och handlar främst om hur ett nytt besluts undantag bör utformas samt om hur europeiska medborgares rättigheter kan tillgodoses i USA. De fundamentala skillnaderna i EU:s respektive USA:s dataskydd är ofrånkomliga men bör i den mån det är möjligt att harmoniseras för båda parternas skull. Uppsatsen finner slutligen att de inskränkande och obegränsade underrättelselagarna i USA måste revideras för att ett nytt beslut om adekvat skyddsnivå ska kunna fattas.

Förord

Tack advokat Dag Wetterberg för inledande inspiration och tips,
Tack fina vänner Emmy Weibull och Emilia Weichbrodt för pepp,
Tack bästa Anton Wilzén för dina värdefulla synpunkter.

Helga Söderström
Göteborg 4 januari 2021

Förkortningar

9/11	Terrorattackerna den 11 september 2001
BCR	*Binding Corporate Rules* (bindande företagsklausuler)
C.C.C	California Civil Code
CCPA	*California Consumer Privacy Act*
Dataskyddsdirektivet	Europaparlamentets och rådets direktiv 95/46/EG
DSF	Dataskyddsförordningen (eng. *GDPR*)
DoC	*Department of Commerce* (Förenta staternas Handelsministerium)
DPC	*Data Protection Commission* (Irländska Dataskyddsmyndigheten)
E.O 12333	*Executive Order 12333*
EU-domstolen	Europeiska Unionens domstol
EU-stadgan	Europeiska Unionens stadga om de grundläggande rättigheterna
EDPB	*European Data Protection Board* (europeiska dataskyddstyrelsen)
EES	Europeiska ekonomiska samarbetsområdet
EDPB-riktlinje	*European Essential Guarantees for surveillance measures*
FEUF	Fördraget om Europeiska Unionens Funktionssätt
FISA	*Foreign Intelligence Surveillance Act*
FISC	*Foreign Intelligence Surveillance Court*
FTC	*Federal Trade Commission*
GLBA	Gramm-Leach-Bliley Act
HIPAA	*Health Insurance Portability and Accountability Act*
Kommissionen	Europeiska kommissionen
OCR	*Office for Civil Rights*
ODNI	*Office of the Director of National Intelligence*

PII	Personligt identifierbar information
PPD-28	*Presidential Policy Directive-28*
Privacy Shield	Kommissionens genomförandebeslut 2016/1250
Safe Harbour	Kommissionens genomförandebeslut 2000/520/EG
US CLOUD Act	*US Clarifying Lawful Overseas Use of Data Act*
U.S.C	*United States Code*

1 Inledning

1.1 Bakgrund

I oktober 2015 underkände EU-domstolen beslutet om *Safe Harbour* efter att juristen och dataskyddsaktivisten Maximillian Schrems anmält Facebook till DPC på grunden att det var oförenligt med dataskyddsdirektivet.[1] Tillsammans med DoC utarbetade kommissionen därefter fram *Privacy Shield*.[2] I juli 2020 underkände EU-domstolen Privacy Shield och i avsaknad av ett nytt beslut måste företag och organisationer som överför personuppgifter till USA själva reglera villkoren i sina personuppgiftsansvarige- eller biträdesavtal och på egen hand säkerställa att lämpliga skyddsåtgärder för den registrerade föreligger.[3] Då två beslut redan har ogiltigförklarats i EU-domstolen och sanktionsavgifterna kan bli höga om överföring sker felaktigt råder oroligheter kring vad som egentligen gäller.[4] Då USA är en av EU:s främsta handelspartners är behovet av vägledning stort kring vad som är en adekvat skyddsnivå för att överföring av personuppgifter till USA ska ske på ett korrekt och lagligt sätt.[5]

1.2 Syfte och frågeställning

Syftet med uppsatsen är att undersöka vad en adekvat skyddsnivå är enligt dataskyddsförordningen för att besvara frågeställningen hur dataöverföring kan ske från EU till USA på ett lagligt och effektivt sätt. För att uppfylla uppsatsens syfte behandlas och besvaras följande frågeställningar:

- Hur ser lagstiftningen för dataskyddet ut i EU respektive USA och vad skiljer dataskyddsregelverken åt?
- Hur har adekvat skyddsnivå tolkats i praxis från EU-domstolen?

[1] Kommissionens genomförandebeslut 2000/520/EG (**Safe Harbour)**, C-362/14 *Schrems mot DPC* (**Schrems I**)
[2] Kommissionens genomförandebeslut 2016/1250 (**Privacy Shield**)
[3] C-311/18 DPC/Schrems mot Facebook Ireland (**Schrems II**), DSF 46.1
[4] DSF 83.4
[5] Cooper, William H., *EU-US Economic Ties*

1.3 Avgränsningar

En bred undersökning av dataöverföring till tredjeland hade varit önskvärd men på grund av tidsbrist och uppsatsens storlek tar frågeställningen enbart sikte på att undersöka vad som är en adekvat skyddsnivå vid dataöverföring till USA i egenskap av en av EU:s främsta handels- och samarbetspartners. Uppsatsen behandlar således inte överföring av personuppgifter till annat territorium, organisation eller specificerade sektorer vilka även de omfattas av förordningen. Frågeställningen är ytterligare avgränsad till överföring av personuppgifter i kommersiella- eller brottsbekämpande syften och behandlar således inte överföring gällande offentlig förvaltning.

1.4 Forskningsläge, metod och material

För att utröna vad som är en adekvat skyddsnivå undersöks den gällande rätten. Det sker genom en rättsdogmatisk metod genom vilken rättspraxis från EU-domstolen undersöks och analyseras. Mer djupgående behandlas och analyseras lagstiftning, förarbeten och doktrin på området. För en djupare förståelse och bättre kunskap i hur dataskyddet fungerar ställs dataskyddet i EU upp gentemot dataskyddet i USA för en komparativ analys. Forskningsläget är relativt omfattande vad gäller tredjelandsöverföring men i och med ogiltigförklarandet av Privacy Shield finns en ny lucka att fylla. Eftersom dataskyddsrätten präglas av snabb teknisk utveckling och förändring av betydelse för lagstiftningen anses rättsläget vara relativt föränderligt. Så sent som i november 2020 kom nya riktlinjer av stor betydelse för regelverket. Av den anledningen strävar uppsatsen efter att använda sig av senast publicerad doktrin i möjligaste mån. I ambition att hålla så hög kvalitet som möjligt används i uppsatsens tredje avsnitt endast material utgiven av offentliga myndigheter i USA eller artiklar av professorer vid allmänt välkända juristskolor i USA.

1.5 Perspektiv

I uppsatsen behandlas dataskyddslagstiftningen främst utifrån tre perspektiv; individens-, statens- och den kommersiella aktörens perspektiv. Den ständiga avvägningen inom dataskyddets område rör antingen balansen mellan individers- och kommersiella aktörers rättigheter eller balansen mellan individens rättigheter och statens skyldigheter varför uppsatsen främst undersöker dataskyddet utifrån de tre perspektiven. Vidare präglas uppsatsen av ett övergripande komparativt perspektiv. Med ett komparativt perspektiv ges en djupare inblick och bättre förståelse för hur dataskyddet fungerar och varför det ser ut som det gör i EU respektive USA.

1.6 Disposition

För bäst förståelse av uppsatsen och ämnet i sin helhet ges först en översiktlig bild av EU:s dataskyddsförordnings regelverk och definitioner av viktiga begrepp. Därefter ges en översiktlig bild av hur dataskyddet i USA ser ut. I uppsatsen tredje del analyseras rättspraxis från EU-domstolen följt av en komparativ analys av dataskyddsregleringen i EU och USA i uppsatsen fjärde del. Avslutningsvis besvaras uppsatsens frågeställning i en sammanfattning med slutsats i uppsatsens femte del.

2 Dataskydd i EU

2.1 Inledning

Omfattningen av insamling och delning av personuppgifter har ökat avsevärt under 2000-talet. På grund av en snabb teknisk utveckling och en mer globaliserad värld har nya utmaningar för lagstiftaren uppstått på området för skydd av personuppgifter. Tekniken möjliggör för både privata företag och offentliga myndigheter att använda sig av personuppgifter i en helt ny omfattning samtidigt som allt fler medborgare gör sina personliga uppgifter allmänt tillgängliga på plattformar världen över.[6] EU vill säkerställa en hög skyddsnivå för personuppgifter och samtidigt gynna en ekonomisk utveckling och social integration i inre marknaden med hjälp av det fria flödet av personuppgifter.[7] Skyddsmekanismen för det är idag dataskyddsförordningen (härefter förordningen).[8]

2.2 Bakgrund

Före 1995 såg lagstiftningen gällande skyddet av personuppgifter olika ut inom EU. På grund av oro för obalans på den inre marknaden tillkom därför det harmoniserande dataskyddsdirektivet.[9] I Sverige infördes i och med direktivet personuppgiftslag (1998:204) vilken ersatte den tidigare gällande datalag (1973:289) från 1973.[10] Personuppgiftslagen gällde fram till den 25 maj 2018 då dataskyddsförordningen trädde i kraft.

2.3 Syfte

Förordningens två grundläggande syften är att skydda fysiska personer med avseende på behandling av personuppgifter och att skapa förutsättningar för

[6] DSF beaktandeskäl 6
[7] DSF beaktandeskäl 5–6
[8] Europaparlamentet och rådets förordning 2016/679
[9] Europaparlamentets och rådets direktiv 95/46/EG
[10] Prop. 1997/98:44

det fria flödet av personuppgifter inom unionen.[11] Avsikten med förordningen är att beakta syftena och bidra till att skapa ett område med frihet, säkerhet, rättvisa, en ekonomisk union, ekonomiska och sociala framsteg, konvergens av ekonomierna inom den inre marknaden samt fysiska personers välbefinnande.[12]

2.4 Rättigheter

Dataskyddsförordningen grundar sig främst på rätten till integritet.[13] Rätten till integritet är inte en absolut rättighet utan en avvägning mellan andra grundläggande rättigheter sker i varje enskilt fall.[14] Å ena sidan stärks den ekonomiska unionen av ett fritt flöde av personuppgifter då det skapar bättre förutsättningar för ekonomiska och sociala framsteg. Samtidigt ska enskildas integritet skyddas.[15] Exempel på när EU-domstolen har vägt rättigheter mot varandra är i målet *Google v. Spain.*[16] Målet är omtalat då det gav upphov till ”rätten att bli glömd”.[17] I målet ville en spansk medborgare (Gonzales) att länkar med inaktuell personlig information om honom skulle plockas bort ifrån Googles sökmotor. Förenklat ansåg EU-domstolen att Gonzales rätt till integritet vägde tyngre än Googles rätt till näringsfrihet och internetanvändares rätt till informationsfrihet.[18]

2.5 Territoriellt tillämpningsområde

Förordningen är till alla delar bindande och direkt tillämplig i varje medlemsstat. Både företag inom EU och företag etablerade utanför unionen som erbjuder varor eller tjänster till registrerade i unionen omfattas av förordningen oavsett om behandlingen av personuppgifter sker inom unionen eller inte så länge behandlingen rör medborgare inom unionen.[19]

[11] DSF 1.1
[12] DSF beaktandeskäl 2
[13] DSF beaktandeskäl 1
[14] Artikel 8.1 EU-stadgan, artikel 16.1 FEUF, DSF beaktandeskäl 4
[15] DSF beaktandeskäl 4
[16] C-131/12 *Google mot Spanien*
[17] Frydinger m.fl. s.30
[18] Ibid
[19] DSF 3

2.6 Materiellt tillämpningsområde

Förordningen är främst ett skydd för medborgares rätt till integritet och ska därför skydda personuppgifter. [20] Förordningen tillämpas på behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling av personuppgifter som ingår eller kommer att ingå i ett register.[21] Behandling av personuppgifter som företas i rent privat natur eller i samband med ens hushåll omfattas inte av förordningen.[22] Behandlingen måste vara en del i en verksamhet av kommersiell eller ideell natur eller som en del av offentlig förvaltning för att förordningen ska vara tillämplig.

2.6.1 Personuppgifter

Varje upplysning avseende en fysisk person utgör en personuppgift oavsett om den kan kopplas direkt till en fysisk person eller indirekt kombinerad med en annan uppgift.[23] Att indirekta personuppgifter utgör personuppgifter bekräftades i ett mål där den examinerades svar utgjorde en personuppgift. Examinationssvaret var bland annat handskrivet och hade examinatorns examinationsanteckningar i marginalen vilka i anslutning till svaren gjorde examinationssvaret identifierbart.[24] Det finns *generella personuppgifter* och *personuppgifter av särskilda kategorier* vilket i tidigare gällande personuppgiftslagen kallades ”känsliga personuppgifter”, exempelvis uppgift om etniskt ursprung, politisk åsikt, religiös eller filosofisk övertygelse, medlemskap i fackförening, genetiska uppgifter, biometriska uppgifter eller uppgift om hälsa och sexualitet.[25] Exempel på generella personuppgifter kan vara namn, personnummer, adress, telefonnummer, fotografi, video- eller ljudklipp, IP-adress och GPS-information.[26]

[20] EU-stadgan 7–8, DSF 2
[21] DSF 2.1
[22] DSF 2.2.c
[23] DSF 4.1
[24] C-434/16, *Nowak*
[25] DSF 9.1, personuppgiftslag 13 §
[26] Frydinger m.fl. s.44, C-101/01, *Lindqvist*

2.6.2 Behandling av personuppgifter

Med *behandling* avses i princip varje åtgärd eller kombination av åtgärder beträffande personuppgifter som kan företas, exempelvis insamling, registrering, organisering, strukturering, lagring, bearbetning, ändring, framtagning, läsning, utlämning, överföring, överföring till tredjeland, spridning, tillhandahållande, justering, sammanförande, begränsning, radering eller förstöring oavsett om det sker passivt eller aktivt, automatiserat eller inte.[27]

2.6.2.1 Legalitetsprincipen

Personuppgifter får behandlas endast om det finns lagstöd i dataskyddsförordningen eller speciallagstiftning. Huvudregeln är att allt är förbjudet om det inte finns stöd i lag.[28] De sex lagliga grunderna för behandling av personuppgifter är samtycke, fullgörande av avtal, fullgörande av rättslig skyldighet, skyddande av intresse av grundläggande betydelse för den registrerade, utförande av uppgift av allmänt intresse eller myndighetsutövning samt intresseavvägning.[29]

2.6.2.2 Principen om öppenhet och korrekthet

I ett demokratiskt samhälle är transparens av stor vikt varför behandling av personuppgifter ska vara korrekt och öppen i förhållande till den registrerade.[30] Principen om öppenhet betonar kravet på transparens och den registrerades rätt till information om när dennes personuppgifter samlas in och hur de används.[31] Att behandlingen ska vara korrekt kan däremot tolkas på flera sätt. *Korrekt* avser något *riktigt* men eftersom en *princip om riktighet* redan finns i förordningen är det uppenbart att *korrekthet* inte avser uppgifternas kvalitet utan snarare den personuppgiftsansvarige uppträdande i förhållande till den registrerade.[32] En möjlig tolkning av principen är ”i

[27] DSF 4.2
[28] Frydinger m.fl. s.35
[29] DSF 6.1
[30] DSF 5.1, beaktandeskäl 39
[31] DSF 13–14
[32] Holtz & Ledendal, *Överlappning mellan dataskydd och marknadsrätt*

enlighet med god tro” vilket innebär att en intresseavvägning måste ske i varje enskilt fall.[33] I förhållande till den engelska motsvarigheten *fairness* kan den svenska översättningen vara missvisande om den inte ses i ljuset av *rätten till självbestämmande*.[34] En personuppgiftsansvarig får inte tillskansa sig personuppgifter genom påtryckningar och måste beakta den registrerades förväntningar på basis av den information om behandlingen som den registrerade har tagit del av.[35] Principen ger då uttryck för en slags norm om ”skälighet” mer likt den engelska översättningen *fair*. Till principen hör också en *rätt till rättelse* om en uppgift är felaktig eller utdaterad och behandlingen kan begränsas till dess personuppgiftsansvarig fått möjlighet att kontrollera invändningen.[36]

2.6.2.3 Principen om ändamålsbegränsning, uppgiftsminimering och lagringsminimering

Personuppgifter ska behandlas i minsta möjliga mån. Personuppgifter får samlas in endast för särskilda, uttryckligt angivna och berättigade ändamål. De insamlade personuppgifterna får inte senare behandlas på ett sätt som är oförenligt med de ursprungliga ändamålen.[37] Behandlingen ska vara adekvat, relevant samt inte alltför omfattande i förhållande till ändamålet.[38] Den personuppgiftsansvarige får inte samla in eller behandla fler personuppgifter än vad som är nödvändigt för att uppfylla syftet med behandlingen.[39] När uppgifterna inte längre behövs ska de raderas eller om möjligt anonymiseras.[40]

2.7 Personuppgiftsansvar

För att få behandla personuppgifter krävs en personuppgiftsansvarig som bestämmer medel och ändamål med behandling av personuppgifter. Den

[33] Prop. 2017/18:105 s.47
[34] Frydinger m.fl. s.36
[35] DSF 13–14, Frydinger m.fl. s.37
[36] DSF 5.1.d, 18.1.a
[37] DSF 5.1.b
[38] DSF 5.1.c
[39] Holtz & Ledendal, *Överlappning mellan dataskydd och marknadsrätt*
[40] DSF 5.1.e

personuppgiftsansvarige kan vara en fysisk eller juridisk person, offentlig myndighet, annat organ- eller institution.[41] Den personuppgiftsansvarige kan i sin tur anlita ett personuppgiftsbiträde som i sin tur behandlar personuppgifter för den personuppgiftsansvariges räkning. Det övergripande ansvaret tillfaller personuppgiftsansvarige.[42]

2.8 Tillsynsmyndighet

Det nationella personuppgiftsansvaret tillfaller tillsynsmyndigheten vars uppgift är att oberoende säkerställa att förordningen tillämpas och efterlevs.[43] Tillsynsmyndigheten ska verka för en ökad medvetenhet och kunskap om dataskydd hos personuppgiftsansvariga som befolkning.[44] Det är upp till varje medlemsstat själva att bestämma vilken- eller vilka nationella myndigheter som ska vara ansvariga för att övervakningen.[45] I Sverige är ansvarig tillsynsmyndighet *Datainspektionen*.[46]

2.9 EDPB

EDPB består av huvudet för varje nationell dataskyddsmyndighet samt EU:s datatillsynsman.[47] Kommissionen har tillgång till styrelsens möten men utan rösträtt.[48] EDPB har det övergripande ansvaret att dataskyddsförordningen tillämpas enhetligt inom unionen och har till uppgift att verka för ett gott samarbete mellan medlemsländernas dataskyddsmyndigheter.[49] EDPB utfärdar även riktlinjer och rekommendationer.[50] I en av riktlinjerna framgår att den registrerade har rätt till information om när dennes personuppgifter samlas in och hur det används, en rätt att till registerutdrag av ens personuppgifter samt rätten till dataportabilitet.[51]

---

[41] DSF 4
[42] Frydinger m.fl. s.51
[43] DSF 51, 57
[44] Förordning (2007:975) med instruktion för Datainspektionen
[45] DSF 51.1
[46] Förordning (2007:975)
[47] DSF 68
[48] DSF 68.5
[49] DSF 70
[50] DSF 70.d
[51] Riktlinje 2016/679, DSF 20

2.10 Dataöverföring till tredjeland

I och med dataskyddsförordningen har alla medlemsländer ett likvärdigt skydd för personuppgifter och inom EU råder därför fri rörlighet av personuppgifter.[52] Överföring av personuppgifter till länder utanför EU är som utgångspunkt förbjudet.[53] Med tredjeland menas en stat som varken ingår i EU eller är ansluten till EES.[54] Flödet av personuppgifter till och från länder utanför unionen är dock nödvändiga för utvecklingen av internationell handel och internationellt samarbete.[55] Eftersom själva processen att överföra personuppgifter till tredjeland i sig utgör en behandling av personuppgifter blir artikel 7-8 i EU-stadgan tillämpliga på överföringen.[56] Den registrerade är då berättigad ett väsentligt likvärdigt skydd av personuppgifter tillika det skydd som garanteras inom unionen.[57] Tredjelandsöverföring får ske enbart under förutsättningen att ett likvärdigt skydd säkerställs enligt förordningen.[58]

2.10.1 Adekvat skyddsnivå

Den första förutsättningen under vilken tredjelandsöverföring kan ske är om kommissionen har fattat ett beslut om adekvat skyddsnivå.[59] Anser kommissionen att en adekvat skyddsnivå föreligger beslutas det i en genomförandeakt i vilken det framgår att landet uppfyller villkoren för en adekvat skyddsnivå.[60] Genom genomförandeakten inrättas en mekanism för regelbunden översyn om minst vart fjärde år som beaktar all relevant utveckling i det tredjelandet och vilken antas i enlighet med ett granskningsförfarande.[61] Kommissionen kan genom genomförandeakten

[52] Linden, Oliver; Dahlberg, Erik, *Data Flows – a fifth freedom for the internal market*, Frydinger m.fl. s.235
[53] DSF 44
[54] Sjöberg Magnusson, Cecilia, *lagkommentar nr.239 till dataskyddsförordningen* (Juno)
[55] DSF beaktandeskäl 101
[56] Schrems II p.83
[57] Schrems II p.96
[58] DSF 44
[59] DSF 45.1
[60] DSF 45.3
[61] DSF 45.3, 93.2

återkalla, ändra eller upphäva beslutet om adekvat skyddsnivå om kommissionen anser att tredjelandet inte längre uppfyller en adekvat skyddsnivå.[62]

2.10.1.1 Bedömning av adekvat skyddnivå

Till sin bedömning ser kommissionen primärt på det tredjelandets rättsstatsprincip, tillsynsmyndighet samt internationella åtaganden.[63] Kommissionen beaktar det tredjelandets lagstiftning och tillämpning av lagstiftningen, rättspraxis, respekt för mänskliga rättigheter och grundläggande friheter, offentliga myndigheters tillgång till personuppgifter, säkerhetsbestämmelser samt möjlighet för den registrerade till rättslig prövning.[64] Kommissionen undersöker det tredjelandets tillsynsmyndighets oberoende, verkställighetsbefogenheter, möjlighet att ge individ råd och assistens samt samarbete med andra myndigheter.[65] Slutligen ser kommissionen på det tredjelandets internationella åtaganden och andra skyldigheter som följer av rättsligt bindande konventioner eller instrument, särskilt rörande skyddet av personuppgifter.[66] För ett beslut om adekvat skyddsnivå krävs att den registrerades rätt till rättslig prövning är ”väsentligt likvärdig” med den som garanteras inom unionen.[67] Med anledning av ogiltigförklarandet av Privacy Shield utformade EDPB en rekommendation att använda vid bedömningen.[68]

2.10.1.2 EDPB-riktlinje

Syftet med rekommendationen är att tillhandahålla grunder för att undersöka om övervakningsåtgärder som tillåter tillgång till personuppgifter av offentliga myndigheter såsom nationella säkerhets- eller brottsbekämpande myndigheter i ett tredjeland kan betraktas som ett berättigat ingripande eller

[62] DSF 45.5
[63] DSF 45.2
[64] DSF 45.2.a
[65] DSF 45.2.b
[66] DSF 45.2.c
[67] DSF 45.1, EU-stadgan 47, EDPB-riktlinje 1.4
[68] *Recommendations on the European Essential Guarantees for surveillance measures,* 10 november 2020

inte.[69] Med *berättigat ingripande* avses det undantag från vilket en registrerads rätt till integritet kan komma att ge vika då den personuppgiftsansvariges intressen anses väga tyngre i en avvägning.[70] Det är dock upp till den personuppgiftsansvarige att motivera varför dennes berättigade intressen väger tyngre.[71] Rekommendationen utgör en grund att konsultera men är inte heltäckande.[72] För att motivera begränsning av dataskydd och individens rätt till integritet ska fyra krav garanteras:

A. Behandling av personuppgifter ska baseras på tydliga, exakta och tillgängliga regler.
B. Ändamål med behandling ska vara legitim, nödvändig och proportionerlig.
C. En oberoende översynsmekanism bör finnas.
D. Effektivt rättsmedel måste finnas tillgänglig för individen.[73]

2.10.2 Lämpliga skyddsåtgärder

Vid avsaknad av ett giltigt beslut om adekvat skyddsnivå kan tredjelandsöverföring ske om den personuppgiftsansvariga eller personuppgiftsbiträdet har vidtagit lämpliga skyddsåtgärder och på villkor att lagstadgade rättigheter och effektiva rättsmedel för de registrerade finns tillgängliga.[74] Exempel på lämpliga skyddsåtgärder kan vara att använda sig av *standardavtalsklausuler* vilka antas direkt av EU-kommissionen eller en tillsynsmyndighet i enlighet med ett fastställt granskningsförfarande som godkänts av kommissionen.[75] Klausulerna innehåller skyldigheter för den personuppgiftsansvariga som vill föra över personuppgifter till tredjeland och för den personuppgiftsansvarige som tar emot uppgifterna i tredjeland samt reglerar frågor kring överföringen, registrerades rättigheter samt hur tvister med anledning av avtalet ska lösas.[76] Klausulerna kan upphävas helt

[69] EDPB-riktlinje 1.7
[70] DSF 6.1.f, beaktandeskäl 113
[71] DSF beaktandeskäl 69
[72] DSF 46, EDPB-riktlinje 1.8
[73] EDPB riktlinje 3.24.a-d
[74] DSF 46.1–2
[75] DSF 57.1.j, 93.2, Frydinger m.fl. s.239
[76] DSF 28.8

eller delvis av EU-domstolen trots ett ursprungligt godkännande av kommissionen och är därför inte en helt tillförlitlig mekanism.[77] En annan lämplig skyddsåtgärd kan vara genom bindande företagsbestämmelser vilka godkänts av en tillsynsmyndighet, en godkänd uppförandekod eller en godkänd certifiering under förutsättningen att de blir rättsligt bindande och verkställbara även gentemot mottagaren av uppgifterna.[78] Liksom standardavtalsklausuler är BCR inte en helt tillförlitlig mekanism eftersom amerikansk lag kan komma att påverka skyddet som tillhandahålls efter senaste Schrems II-domen.[79]

2.10.3 Undantag

I sista hand kan undantag bli aktuellt mot förbjudet om tredjelandsöverföring. För att tillsynsmyndighet ska godkänna undantaget ska samtliga bestämmelser i fjärde kapitlet dataskyddsförordningen vara uppfyllda.[80] Ett utnyttjande av undantagen kan därmed aldrig leda till en situation där grundläggande rättigheter kringgås.[81] Ett giltigt undantag kan vara om den registrerade uttryckligen har lämnat samtycke till att uppgifterna får överföras. För giltigt samtycke ska den registrerade först ha blivit informerad om de eventuella riskerna med överföringen.[82] Ett annat undantag är om överföringen är nödvändig för att en part ska kunna ingå eller fullgöra en förpliktelse i ett avtal. Särskilda skäl för undantag är om överföringen sker på grund av allmänintresse eller för att skydda den registrerades eller andra personers grundläggande intressen när vederbörande är fysiskt eller rättsligt förhindrad att ge sitt samtycke själv.[83]

[77] *Jämför Schrems-II*
[78] DSF 46.2.b, 46.2.e-f, Frydinger m.fl. s.40
[79] Datainspektionen, *Förtydligande med anledning av Privacy Shield-domen*
[80] DSF 49.1
[81] Frydinger m.fl. s.40
[82] DSF 13–14
[83] DSF 49.1.f

2.11 Sanktioner

Vid överträdelser av förordningen ska varje tillsynsmyndighet säkerställa att påförande av administrativa sanktionsavgifter är effektivt, proportionellt och avskräckande.[84] Hur hög sanktionsavgiften blir beror på överträdelsens karaktär, svårighetsgrad, varaktighet, omfattning och bakomliggande syfte och om överträdelsen har skett med uppsåt eller inte.[85] Det administrativa sanktionsbeloppet får totalt inte överstiga det belopp som fastställs för den allvarligaste överträdelsen.[86] Maxbelopp för administrativ sanktionsavgift är 20 miljoner euro alternativt upp till 4 procent av den totala globala årsomsättningen föregående budgetår beroende på vilket värde som är högst om det gäller ett företag.[87]

[84] DSF 83
[85] DSF 83.2.a-b
[86] DSF 83.3
[87] DSF 83.4

3 Dataskydd i USA

3.1 Inledning

USA är en federal stat vars legaldefinition är ”en sammansatt stat vars suveränitet för hela staten är uppdelad mellan den centrala eller federala regeringen och de lokala regeringarna i de flera konstituerade staterna; en union av stater där kontrollen av alla medlemsstaters yttre förbindelser har överlämnats till en centralregering så att den enda staten som existerar för internationella ändamål är den som bildats av unionen”. [88] Definitionen är viktigt för förståelse av hur dataskyddet har utformats i USA och hur det samverkar gentemot internationella parter. I USA finns federala lagar vilka gäller nationellt och delstatliga lagar vilka gäller i respektive delstat.[89] Det finns ingen omfattande federal lag som reglerar dataskydd utan lagstiftningen är snarare utformat efter sektorer såsom finans, sjukvård och handel.[90] Systemet av federala och statliga lagar kan överlappa och motsäga varandra.[91] Vid normkollision är det upp till USA:s högsta domstol att tolka och bedöma vad som gäller, i enlighet med dess Common Law-tradition.[92]

3.2 Bakgrund

Under 2000-talet sågs i USA en alarmerande trend av dataintrång vilka resulterade i identitetsstölder. År 2004 beräknades 10 miljoner amerikanska medborgare ha utsatts för identitetsstöld vilket resulterade i en förlust om 50 miljarder för företag och 5 miljarder för konsumenter. Identitetstöld var därmed det främsta brottet i USA och lagstiftning på dataskyddets område ökade.[93] Den 11 september 2001 utsattes USA för terrorattacker. Kort därpå stiftades flera lagar vilka gav staten utökade möjligheter att övervaka,

[88] Steenken, Beau & Brooks, Tina M., *Sources of American Law,* s.3, Black’s Laws Dictionary 1627
[89] *Sources of American Law*, s.4
[90] *Data Protection Law: An Overview*
[91] *Sources of American Law*, s.5
[92] Amerikanska konstitutionen artikel 3, *Sources of American Law* s.12
[93] *Data Security: the discussion draft of data protection legislation* s.3

avlyssna och ta del av personlig information och data i terrorbekämpande syfte och för den nationella säkerhetens skull.[94]
Idag ligger flera av världens största och mest framgångsrika IT-bolag i USA. I toppen återfinns företag såsom *Microsoft, Amazon, Apple, Facebook Inc, Twitter, Snapchat, Google* och *Palantir*.[95] Gemensamt för nämnda företag är deras syn på- och värdering av data. För samtliga företag är en av de största tillgångar kundernas data.[96] För exempelvis Twitter, Facebook och Snapchat är produkten som företaget erbjuder gratis i utbyte mot kundens data. I en sådan digital marknad är data valutan.[97] För att skydda konsumenter från otillbörligt utnyttjande har lagstiftning på dataskyddets område ökat.

3.3 Materiellt tillämpningsområde

Personlig identifierbar information är ett av de mest centrala begreppen i amerikansk dataskyddslagstiftning och utgör grunden till all tillämpning.[98] Vad som utgör PII skiljer sig åt mellan olika lagstiftningar.[99] Vid behandling av PII blir dataskyddslagstiftning tillämplig och é contrario kan samma lag vid avsaknad av PII inte tillämpas. Att det inte finns någon enhetlig definition av PII inom dataskyddslagstiftningen i USA menar en del kritiker är problematiskt.[100]

3.4 Territoriellt tillämpningsområde

I *United States v. Verdugo-Urquidez* uttalade den högsta domstolen att det fjärde tillägget i amerikanska konstitutionen inte omfattar icke-medborgare som befinner sig utanför USA.[101] Domen innebär att amerikanska

[94] Solove, Daniel J., *"I've got nothing to Hide" and Other Misunderstandings of Privacy,* s.745
[95] *Fortune 500*
[96] Larsson, Stefan & Ledendal, Jonas, *Konsumentverkets rapport 2017:4*, s.9
[97] Ibid
[98] Schwartz, Paul M. & Solove, Daniel J., *Reconciling Personal Information in the United States and the European Union*, s.5
[99] Jämför *15 U.S.C § 6809.4.A*, *C.C.C § 1798.140(o)(1)*
[100] Schwartz, Paul M. & Solove, Daniel J., *The PII Problem*
[101] United States v. Verdugo-Urquidez (1990)

medborgare omfattas av fjärde tilläggets grundlagsskydd endast på amerikansk mark. Om det är möjligt att komma till samma slutsats gällande andra medborgerliga rättigheter är utanför uppsatsens område. Amerikansk dataskyddslagstiftnings territoriella tillämpningsområde kommer inte att redogöras för djupare.

3.5 Relevant lagstiftning

3.5.1 Amerikanska konstitutionen

I amerikanska konstitutionens fjärde tillägg finns en bestämmelse om ”sökning och beslag” (eng. *search and seizure*) vilken innefattar ett förbud mot orimlig husrannsakan, övervakning och avlyssning.[102] Förbudet skyddar enskilda från regeringens intrång men ger ingen grundlagsskyddad rätt gentemot privata aktörer.[103]

3.5.2 US Privacy Act (1974)

Lagen reglerar federala myndigheters möjlighet till insamling, behandling, användning och spridning av personuppgifter i syfte att balansera regeringens behov av att upprätthålla information om medborgare med individens rätt till skydd mot oberättigat intrång i integriteten.[104] För bäst förståelse av lagen är det viktigt att se dess historiska sammanhang. År 1974 ville kongressen begränsa den olagliga övervakningen och utredningen av individer av federala myndigheter som hade blivit utsatta under *Watergate*-skandalen.[105] Lagen ger amerikanska medborgare rätt att begära ut data som förvaras hos federala myndigheter och en rätt till rättelse om sådan information är felaktig och innehåller även principer om ändamålsbegränsning och krav på berättigade syften.[106]

[102] US Constitution 4th Amendment
[103] *Data Protection Privacy: An Overview,* s.1
[104] US Department of Justice, *Overview of the Privacy Act of 1974*, s.1
[105] Perry, James M., *Watergate Case Study*
[106] *Overview of the Privacy Act*, s.4

3.5.3 Executive Order 12333 (1981)

År 1981 utfärdade dåvarande president Ronald Reagan en exekutiv order vilken fastställer ramverket för de verkställande delarna av USA:s nationella underrättelsetjänst i syfte att skydda integritet och medborgerliga friheter vid genomförandet av underrättelsetjänster. Ordern reviderades senast 2008 av dåvarande president George W. Bush i syfte att anpassa ordern utefter nya hot.[107] Den reviderade ordern fokuserar på att förtydliga myndigheternas befogenheter och gäller än idag.[108]

3.5.4 HIPAA (1996)

Lagen reglerar individers integritetsskydd vid insamling och behandling av PII rörande individs hälsa i samband med sjukvårdsförsäkringar. HIPAA innehåller skydd för personlig integritet och ställer upp olika säkerhetskrav, bland annat har den skapat en nationell standard för krav på sekretess vid behandling av hälsoinformation. Exempelvis kräver HIPAA samtycke från patient för att närstående ska få ta del av journalen. Samtycke krävs också för att patientens data ska få användas i marknadsföringssyfte.[109]

3.5.5 GLBA (1999)

På området bank- och finans skyddas personlig information genom bland annat GLBA[110] Personlig informationen definieras i lagen som ”information insamlad om en individ i anslutning till ett tillhandahållande av en finansiell produkt eller tjänst, om inte den informationen annars är offentlig”.[111] Exempel på information som skyddas under GLBA är uppgifter om äganderättshistorik, avbetalningsinformation och finansiella medel.[112] GLBA ställer upp krav på så kallade *”opt-out”* mekanismer vilket innebär att konsument ska kunna återkalla sitt samtycke till behandling av data.

---

[107] *Jämför 9/11*
[108] ODNI, *Civil Liberties and Privacy Information Paper,* s.3
[109] HHS, *Summary of HIPAA Security Rule*
[110] FTC: *Data Security & Privacy Report 2019*, s.7
[111] 15 U.S.C § 6809.4.A
[112] FTC: *Privacy and Data Security Update 2019*

Konsument har också rätt att neka att information delas med en tredje part. GLBA inrymmer dock en gråzon där en tredje part som är ”associerad” med banken kan ta del av information utan kundens uttryckliga samtycke.[113]

3.5.6 FISA (1978)

Lagen är ett ramverk för statliga myndigheters möjlighet att samla in underrättelse med hjälp av bland annat elektronisk övervakning, fysiska sökningar, avlyssning och signalspaning för ändamål relaterade till amerikansk nationell säkerhet.[114] Åtgärder som vidtas med stöd av FISA är begränsade till amerikanskt territorium och tillämplig endast på utländska medborgare. Amerikanska medborgares rätt till privatliv skyddas genom konstitutionens fjärde tillägg. Genom *FISA Amendements Act* tillkom 2008 Avsnitt 702 vilket utökar lagens territoriella tillämpningsområde för riktad övervakning av utländska personer till syfte att skydda USA och dess allierade från fientliga makt.[115] Till FISA hör specialdomstolen *Foreign Intelligence Surveillance Court* vars uppgift är att övervaka åtgärder som vidtas med stöd av FISA.[116] Enligt Avsnitt 702 godkänner FISC inte individuella övervakningsåtgärder men däremot övervakningsprogram. Ett godkännande av ett program sker på en årlig basis och ger ett certifikat under vilken programmet klassas som tillåten. FISC avgör inte om det är lämpligt att övervaka enskilda utan bedömer enbart om övervakningen kan klassas som en övervakningsåtgärd eller inte.[117]

3.5.7 PPD-28 (2014)

År 2014 utfärdade dåvarande presidenten Barack Obama direktivet *PPD-28* vilken innehåller principer för övervakning och underrättelse.[118] Direktivet gäller än idag och begränsar i viss mån insamling, lagring och spridning av utländska personers personuppgifter som inhämtats inom ramen för

[113] FTC: *Privacy and Data Security Update 2019*
[114] McAdams, James G., *Foreign Intelligence Surveillance Act: An Overview*
[115] ODNI, *Section 702 Overview*
[116] FISC: *About U*s
[117] ODNI, *Section 702 Overview*, s.3
[118] PPD-28 avsnitt 2

signalspaningsverksamhet.[119] Insamlingen måste vara godkänd enligt lag alternativt ske med presidentens tillstånd och syftet bakom insamlingen måste vara i enlighet med konstitutionen eller lagstiftningen.[120] Om insamling sker i syfte att bekämpa terrorism är behandlingen lagenlig.[121]

3.5.8 US CLOUD Act (2018)

Lagens huvudsakliga syfte är att underlätta amerikanska brottsbekämpande myndigheters möjlighet att begära ut bland annat kommunikationsdata hos leverantörer av telekom- och molntjänster under förutsättningen att det föreligger sannolika skäl för att ett specifikt brott har begåtts, att uppgifterna är av relevans för utredningen av brottet och att leverantören omfattas av amerikansk jurisdiktion. [122] Uppgifterna behöver inte vara lagrad i USA utan det räcker att datan omfattas av amerikansk jurisdiktion, vilket alla bolag med amerikanska ägare gör.[123]

3.5.9 CCPA (2018)

I Kalifornien regleras företag som har 25 miljoner USD i årliga intäkter grundade till hälften på intäkter från försäljning av konsumentdata alternativt årligen köpa eller sälja 50 000 eller fler konsumenters PII för kommersiella syften genom CCPA.[124] Lagen gäller insamling och försäljning av PII både online som offline.[125] I CCPA definieras PII som ”information vilken identifierar eller kan kopplas till en fysisk person eller hushåll”.[126] Företag måste tydligt informera hur och vilka personuppgifter som samlas in på sin hemsida.[127] CCPA ger konsumenter rätt att veta vilken information som samlats in och en rätt att få uppgifter raderade.[128]

[119] ODNI, *Status of Implementation of PPD-28*
[120] PPD-28 1.a
[121] PPD-28 1.c
[122] CLOUD Act 2.1, 2.3
[123] US Department of Justice: *The Purpose and Impact of the CLOUD Act,* CLOUD Act 2.2
[124] C.C.C § 1798.140(C)
[125] C.C.C § 1798.175
[126] C.C.C § 1798.140(O)
[127] C.C.C § 1798.135.2(A)
[128] C.C.C § 1798.100, § 1798.105

3.6 Tillsynsmyndigheter

3.6.1 Federal Trade Commission

Federala konkurrensmyndighetens uppgift är att skydda konsumenter mot otillbörliga metoder inom handeln samt stärka konkurrensen.[129] Ursprungligen var FTC:s uppgift att tillvarata konsumenters rätt genom att agera mot ”orättvisa eller vilseledande handlingar och metoder i handeln” och ett sätt FTC agerade på var genom att granska företags integritetspolicies.[130] Om företag inte levde upp till sina löften kunde FTC agera på grunden att det är vilseledande metoder i handeln. På så vis utökades FTC:s befogenheter från konkurrens till in på dataskyddets område. FTC genomför tillsyn över nästan alla vinstdrivande enheter i USA som hanterar personuppgifter undantaget företag som lyder under speciallagstiftning exempelvis inom sjukvården. Vid brister i hanteringen av PII utfärdar FTC föreskrifter. Om företag bryter mot en föreskrift kan FTC yrka för civilrättsliga påföljder. FTC verkar även i utbildande syfte och genomför studier, utfärdar rapporter, arrangerar utbildningar samt utvecklar utbildningsmaterial för både konsumenter och företag. De kommenterar även lagförslag och kan vittna inför kongressen i sakkunnighetsfrågor.[131]

3.6.2 Office for Civil Rights

För lagstiftning relaterad till hälsa- och sjukvård är OCR ansvarig tillsynsmyndighet. OCR ansvarar exempelvis för efterlevnaden av HIPAA och ställer krav på regelbunden utvärdering av sjukförsäkringars integritetspolicies samt översyn av vilken data de innehar. OCR:s mål är att verka för att skydda individers privatliv.[132]

[129] Hartzog, Woodrow, Solove, Daniel J., *The Scope and Potential of FTC Data Protection*
[130] 15 U.S.C § 45.a.1
[131] FTC: *Privacy Data Security Update 2019*, s.2
[132] HHS, *About Us*

3.6.3 ODNI

Vad gäller lagstiftning kring nationell säkerhet och underrättelsetjänst fungerar den nationella underrättelsetjänsten *Office of the Director of National Intelligence* som överordnat organ för underättelsegemenskapen i USA. Myndigheten är presidentens och det nationella säkerhetsrådet främsta rådgivare.[133]

3.7 Sanktioner

På grund av dataskyddets utspridning på olika tillsynsmyndigheter ser också sanktionssystemet olika ut beroende på vilken typ av dataskyddslag som har överträtts. Om ett företag bryter mot exempelvis GLBA kan sanktioner utfärdas av FTC och OCR kan utfärda sanktioner vid överträdelser av HIPAA. Hur stor sanktionen blir beror på vad för typ av överträdelse samt vilken lag som överträdelsen har begåtts emot. På grund av uppsatsen storlek behandlas sanktioner inte djupare än så.

[133] Intelligence Reform and Terrorism Prevention Act (2004)

4 Rättspraxis

4.1 Varför ogiltigförklarades Safe Harbour-beslutet i EU-domstolen?

Precis som i dataskyddsförordningen var tredjelandsöverföringar som utgångspunkt i tidigare gällande dataskyddsdirektivet förbjudna.[134] Däremot kunde kommissionen fatta beslut om att ett tredjeland uppfyllde krav på en adekvat skyddsnivå.[135] I förhållande till USA hade kommissionen fattat beslutet *Safe Harbour* (härefter ”beslutet”). I Schrems I-målet undersökte EU-domstolen om beslutet motsvarade de krav som följde av dataskyddsdirektivet och EU-stadgan och om beslutet i så fall var giltigt.[136] EU-domstolen bedömde att ett undantag i beslutet gav upphov till risk för att det skydd som direktivet gav EU-medborgares personuppgifter skulle tvingas ge vika för amerikansk lag vid en fråga om nationell säkerhet, allmänintresse eller rättsefterlevnad.[137] Undantaget var enligt EU-domstolen alltför generellt formulerat och möjliggjorde på så vis ingrepp i de grundläggande rättigheterna för europeiska medborgare vars personuppgifter fördes över till USA. I beslutet saknades hänvisning till amerikansk lag vilken skulle garantera att amerikanska staten begränsade ingrepp i de grundläggande rättigheterna för EU-medborgares personuppgifter och det fanns inte heller något effektivt rättsligt skydd mot den typen av ingrepp.[138] Sammantaget ansåg EU-domstolen att beslutet tillät amerikanska myndigheter generell åtkomst till innehållet i elektroniska kommunikationer vilket kränker den grundläggande rätten till respekt för privatlivet samt att beslutet saknade möjlighet för enskild att använda rättsmedel för att erhålla tillgång till, rätta eller radera personuppgift vilket är i strid med den grundläggande rätten till effektivt domstolsskydd.[139] För

[134] Dataskyddsdirektivet 25.1
[135] Dataskyddsdirektivet 25.6
[136] Schrems I p.67
[137] Schrems I p.85–87, *Safe Harbour Bilaga IV B*
[138] Schrems I p. 80–81
[139] Schrems I p.96–98, EU-stadgan 7, 47

att ett nytt beslut skulle kunna antas krävde EU-domstolen att kommissionen skulle fastställa och tydligt motivera att USA säkerställer en nivå på skyddet av de grundläggande rättigheterna som är *väsentligt likvärdig* med den nivå som garanteras medborgare inom EU.

4.2 Varför ogiltigförklarades Privacy Shield-beslutet i EU-domstolen?

Privacy Shield-beslutet började gälla i augusti 2016 och togs på samma grunder som Safe Harbour-beslutet.[140] Det nya beslutet skapade en mekanism för självcertifiering i USA där företag som intygade att de följde Privacy Shields krav anmälde sig till DoC där de sattes upp på en lista över certifierade företag vilka säkerställde en adekvat skyddsnivå.[141] DoC förvaltade och övervakade listan medan FTC ansvarade för dess verkställighet.[142] Om ett certifierat företag inte skötte sig kunde företaget få böter.[143] USA:s myndigheter garanterade genom beslutet att de inte skulle utöva massövervakning över EU-medborgare.[144] Efterlevnaden av Privacy Shield kunde dock inskränkas på tre grunder. Den första grunden gällde nationell säkerhet, allmänintresse eller rättsefterlevnad. Den andra grunden innebar att Privacy Shield kunde inskränkas av lagar, myndighetsföreskrifter eller rättspraxis som skapar motstridiga skyldigheter. Alternativt kunde Privacy Shield inskränkas om det till följd av EU:s medlemsstaters lagstiftning var tillåtet i jämförbara sammanhang.[145] I Schrems-II fastställde EU-domstolen att inskränkningen av Privacy Shield likt undantagen i Safe Harbour var alltför generella och gav amerikanska myndigheter oproportionerligt ingripande befogenheter.[146] Både avsnitt 702 och övervakning i enlighet med E.O 12333 tillåter insamling av data utöver vad som anses absolut nödvändigt enligt dataskyddsförordningen.[147] Visserligen

[140] Privacy Shield, 1
[141] Privacy Shield, 2.14
[142] Privacy Shield, 2.18
[143] Privacy Shield, 11.f
[144] Privacy Shield, beaktandeskäl 18
[145] Privacy Shield bilaga II 1.5(a-c)
[146] Schrems II p.165
[147] Privacy Shield, p.180

gavs hänvisning till amerikansk lag gällande övervakning enligt avsnitt 702 i garanti för EU-medborgares grundläggande rättigheter, något som saknades i Safe Harbour.[148] Hänvisningen till PPD-28 var emellertid bekräftat fruktlös av amerikanska regeringen då de medgav att direktivet inte ger utländska medborgare bindande rättigheter som kan göras gällande mot amerikanska myndigheter vid övervakning grundad på avsnitt 702.[149] Med andra ord krävs att övervakning grundad på avsnitt 702 genomförs med iakttagande av kraven enligt PPD-28 men då direktivet inte ger registrerade personer bindande rättigheter ansågs inte direktivet säkerställa en skyddsnivå i enlighet med artikel 45.2.a dataskyddsförordningen och EU-medborgare ansågs inte ha tillgång till tillräckligt effektivt rättsmedel i USA för att kunna överklaga övervakningen.[150]

[148] *Jämför Schrems I p.80–81*
[149] Privacy Shield, p.180
[150] Ibid

5 Komparativ analys

Fundamentalt skiljer sig dataskyddet i EU och USA åt i sin underliggande filosofi om integritet. I EU är rätten till integritet en grundläggande mänsklig rättighet medan i USA anses integriteten vara ett intresse som balanseras mot andra intressen såsom exempelvis rätten till näringsfrihet eller rätten till yttrandefrihet. Visserligen ges integriteten i USA ett visst skydd i konstitutionen men det konstitutionella skyddet är inte lika omfattande eller starkt som motsvarande skydd enligt EU-stadgan och är dessutom mer avgränsat. Det grundläggande integritetsskyddet i USA siktar främst in sig på reglering kring *statens makt* gentemot medborgaren. Motsvarande skydd inom EU reglerar snarare *statens skyldigheter* gentemot medborgaren. Vidare är det konstitutionella skyddet i USA enbart tillämpligt på amerikanska medborgare.

Dataskyddet skiljer sig även åt mellan EU och USA baserat på utifrån vilket perspektiv som har präglat lagstiftningen. I USA har dataskyddet utformats till stora delar utifrån statens perspektiv. USA har starkt präglats av de terrorattacker som nationen har utsatts för. Utformningen av dataskyddet i USA har därför till stor del syftat till nationens säkerhet. I en rättighetsavvägning har nationens säkerhets ansetts väga tyngre än individens rätt till integritet. I EU har dataskyddet istället utformats utifrån individens perspektiv snarare än ett unions- eller statligt perspektiv. EU har visserligen upplevt terrordåd men dess konsekvenser har inte lämnat ett lika starkt avtryck i samtliga medlemsländer. Att USA är en federal stat med en nationsanda och EU är en union av stater utan samma nationalistiska sidentitet kan man på så vis se bidrar till att dataskyddets utformning skiljer sig åt.

För enskilda individer är skyddet i EU starkare än i USA. Vid exempelvis konsumentköp fokuserar dataskyddet i USA på att balansera individens integritet med effektiva kommersiella transaktioner. Det kommer till uttryck i att lagstiftningen ställer upp konkreta medel som individen kan använda sig av för att skydda sin data eller själv reglera sitt samtycke. I EU är

utgångspunkten snarare tvärtom och fokus ligger på företagen och deras skyldigheter gentemot individen. Ansvaret för individens integritet ligger i högre grad på individen själv i USA än inom EU där ansvaret snarare åligger företagen att säkerställa en hög nivå av skydd för individers integritet.

Slutligen bör lagstiftningens kvantitet belysas. I EU finns en enhetlig förordning som reglerar dataskyddet för medborgare tillämplig i alla medlemsstater. I USA sprider sig dataskyddslagstiftningen ut över flera olika sektorer, tillämplig på federal- eller enbart delstatsnivå och med olika materiellt tillämpningsområde. Amerikansk dataskyddslagstiftning uppstår enbart när omständigheterna kräver det och tenderar att vara gles. I den aspekten är EU:s dataskyddslagstiftning mer förutseende och heltäckande med ett ”helikopterperspektiv” som saknas i amerikansk dataskyddslagstiftning. Ad hoc-lagstiftningen kan härledas tillbaka till den amerikanska juridiska traditionen vilken bygger på praxis. Då EU lagstiftar förutseende och brett med ambition att lagstiftningen ska täcka alla områden och besvara samtliga eventuella frågor som kan uppkomma längs vägen så lagstiftar USA snarare utefter rådande läge på en ad hoc-basis.

För tillsynsmyndigheternas vidkommande är systemet likt men inte helt desamma i EU respektive USA. I EU utser varje medlemsland en eller flera tillsynsmyndigheter vilka alla ingår i europeiska dataskyddstyrelsen (EDPB) för att säkerställa en konsekvent tillämpning av förordningen. I USA övervakar istället flera olika myndigheter efterlevnaden av respektive dataskyddslag. Främst har FTC den övergripande verkställighetsbefogenheten men undantag finns.

6 Slutsats

Vad som främst skiljer dataskyddet åt mellan EU och USA är vilket perspektiv som präglat respektive lagstiftning. I EU har dataskyddet utformats utifrån individens perspektiv medan i USA är det snarare statens perspektiv som låtit utforma lagstiftningen. Skillnaden har dels en historisk förklaring men är också ett resultat av juridisk tradition och statsskick. Att USA är en federal stat till skillnad från EU som är en union av stater kan förklara varför terrorattackerna tydligare har präglat synen på dataskydd i USA än vad terrorattacker har präglat lagstiftningen i EU. I den bemärkelsen har USA som nation en starkare identitet än vad medlemsländerna i EU har tillsammans som union. Styrkan av den nationella identiteten påverkar avtrycket en terrorattack efterlämnar vilket i sin tur påverkar benägenheten att lagstifta till fördel för brottsbekämpande myndigheters befogenhet. I USA finns därför betydligt fler lagar vilka syftar till den nationella säkerheten än i EU. Säkerhetslagstiftningen ger också underrättelsetjänsten i USA betydligt större befogenheter till skillnad från motsvarande lagstiftning inom EU. I förlängningen påverkar det både enskildas rätt till integritet som statens möjlighet att bekämpa brott.
Att USA:s dataskydd lagstiftats utefter en ad hoc-basis i respektive sektor till skillnad från det enhetliga dataskyddet i EU skulle kunna förklaras av den amerikanska juridiska traditionen vilken bygger på prejudikat. Att luckor i lagstiftningen fylls i av praxis från domstolen vid behov är relevant då det i sin tur resulterar i ett mer spretigt och motsägelsefullt dataskydd i USA än i EU. Skillnaderna komplicerar dels kommissionens arbete vid utformningen av ett överföringsavtal men också utländska och amerikanska medborgares rätt- och möjlighet till effektiva rättsmedel i USA i bemärkelsen att regelverket kan vara motsägelsefullt vid utmynnandet i flera olika grenar. Den sektorsanpassade ad hoc-dataskyddslagstiftningen i USA försvårar enskildas möjlighet till effektivt rättsmedel samt myndigheternas egen möjlighet att utöva tillsyn då ansvaret är utspritt på flera olika aktörer. Med en utspridd tillsyn riskerar ansvaret för vem som ska utföra tillsynen

falla mellan stolarna och rättsläget förbli oklart. På samma sätt riskeras enskildas rättigheter att gå förlorade när rättsläget är oklart. Att synen på dataskydd skiljer sig åt mellan EU och USA samt de faktiska formella skillnaderna i dataskyddets utformning är relevant för uppsatsens slutsats då det påverkar relationen mellan USA och EU. Överföringen av data är en förutsättning för en god relation och en effektiv och blomstrande handel. Med två alltför obalanserade och ibland till och med motsägande regelverk riskerar den viktiga överföringen utebli alternativt ske olagligt till priset av enskildas rättigheter. Det vore en stor förlust för både enskilda som för företag och stat. Att dataskyddsregelverken ses över så att överföring kan ske på ett lagligt sätt utan oklarheter vore till både EU:s som USA:s fördel.

Med adekvat skyddsnivå kan förstås en standard vilken är *väsentligt likvärdig* det skydd som ges EU-medborgare enligt dataskyddsförordningen och artikel 7–8 och 47 i EU-stadgan. Med det sagt behöver skyddet i tredjelandet inte vara desamma som skyddet i EU men de grundläggande rättigheterna som ges EU-medborgare enligt EU-stadgan måste tillgodoses för att överföringen ska anses uppfylla kravet på adekvat skyddsnivå.
I praxis från EU-domstolen har mekanismen för skyddet vid dataöverföring till USA ogiltigförklarats två gånger då mekanismerna inte har uppfyllt kravet på adekvat skyddsnivå. Skyddsnivån har inte bedömts väsentligt likvärdig på främst tre grunder. För det första brister mekanismen för överföring till tredjeland i de båda fallen på grund av de *undantag* som möjliggör inskränkningar i skyddet. EU-domstolen har bedömt att undantagen är alltför generellt utformade för att uppnå kravet på adekvat skyddsnivå. Vidare har mekanismen även brustit i rätten till integritet och skydd av privatliv för EU-medborgare då USA:s underrättelsetjänst genom undantagen ges alltför inskränkande befogenheter. Slutligen saknas möjlighet för individer att tillvarata sin rätt till effektivt rättsmedel i USA då PPD-28 inte medger utländska medborgare en faktisk rättighet att nyttja gentemot amerikanska myndigheter. Sammanfattningsvis har mekanismerna då inte uppnått kraven för adekvat skyddsnivå. Slutsatsen blir att undantag måste vara mer tydliga och precisa än vad som tidigare har gällt för att

uppnå kravet på adekvat skyddsnivå. Inskränkningar på grund av brottsbekämpande åtgärder måste undantas mer restriktivt och EU-medborgare måste ges bättre möjligheter till att tillvarata sin rätt till effektivt rättsmedel genom tydligare regler och bättre tillsyn. För att överföra data från EU till USA på ett lagligt och effektivt sätt krävs att EU och USA kommer fram till ett bättre överföringsavtal i bemärkelsen att det är tydligare och inte lika generellt utformat, och som ger EU-medborgare en faktisk möjlighet till effektivt rättsmedel, samt är mer restriktivt vid inskränkningar på individers privatliv i brottsbekämpande syften. Förslagsvis bör PP2-28 inkorporeras i avsnitt 702 FISA och US CLOUD Acts inverkan på datsskyddsförordningen ses över före ett nytt beslut fattas.

Käll- och litteraturförteckning

Offentligt tryck (EU)

Beslut

Kommissionens beslut 2000/520/EG 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 Harbour Privacy Principles) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat

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 privatliv i EU och Förenta staterna

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

Europaparlamentet och rådets förordning 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

Vägledning

Artikel 29-gruppens vägledning (EDPB) *”Guidelines on transparency under Regulation 2016/679”,* antagen 29 november 2017

EDPB, *Recommendations on the European Essential Guarantees for surveillance measures,* 10 november 2020

Offentligt tryck (Sverige)

Propositioner

Proposition 1997/98:44

Proposition 2017/18:105

Lagar och förordningar

Personuppgiftslag (1998:204)

Datalag (1973:289)

Förordning (2007:975) med instruktion för Datainspektionen

Litteratur

Black's Laws Dictionary 1627, 2014 (10e upplagan)

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

Steenken, Beau; Brooks, Tina M, *Sources of American Law: An Introduction to Legal Research* (andra upplagan)*,* eLangdell Press, 2016

Elektroniska källor

Amerikanska kongressens forskningsservice, *Data Protection Law: An Overview,* 25 mars 2019, tillgänglig på: https://fas.org/sgp/crs/intel/IF11451.pdf (hämtad 2020-11-19)

Amerikanska kongressens protokoll; *Data Security: the discussion draft of data protection legislation hearing protocoll before the sucbommittee on commerce trade and consumer protection*, 28 juli 2005
Tillgänglig på: https://www.govinfo.gov/app/search/ (hämtad 2020-11-20)

Amerikanska konstitutionen, *US Constitution 4th Amendment,* tillgänglig på: https://constitution.congress.gov/constitution/amendment-4/ (hämtad 2020-11-25)

California Civil Code, tillgänglig på: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (hämtad 2020-11-28)

Datainspektionen, *Förtydligande med anledning av Privacy Shield-domen (Schrems II)*, tillgänglig på: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/tredjelandsoverforing/hur-vidtar-vi-lampliga-skyddsatgarder/ (hämtad 2020-11-22)

Department of Homeland Security Office of Intelligence and Analysis, *Policy Instruction; IA-2002*, 16 januari 2015
Tillgänglig på: https://www.dhs.gov/sites/default/files/publications/office-of-intelligence-and-analysis-intelligence-oversight-program-and-guidelines.pdf (hämtad 2020-11-29)

Federal Trade Commission, *Data Security Update 2019,* tillgänglig på: https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf (hämtad 2020-11-20)

Foreign Intelligence Surveillance Court: *About Us,* tillgänglig på: https://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court (hämtad 2020-12-09)

Fortune, *Fortune 500,* tillgänglig på: http://fortune.com/global500/ (hämtad 2020-11-21)

FTC, *Pressmeddelande 2012-12-19,* tillgänglig på: https://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over (hämtad 2020-11-27)

Hartzog, Woodrow, Solove, Daniel J., *The Scope and Potential of FTC Data Protection,* tillgänglig på: https://www.gwlr.org/wp-content/uploads/2016/01/83-Geo-Wash-L-Rev-2230.pdf (hämtad 2020-12-07)

Hartzog, Woodrow, Solove, Daniel J., *The FTC and the New Common Law of Privacy,* 114 Columbus Law Review, revisionssummer 583 (2014), tillgänglig på: https://columbialawreview.org/content/the-ftc-and-the-new-common-law-of-privacy/ (hämtad 2020-12-07)

HHS, *Summary of HIPAA Security Rule,* tillgänglig på: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (hämtad 2020-11-30)

Holtz, Hajo Michael & Ledendal, Jonas, *Överlappning mellan dataskydd och marknadsrätt,* Svensk Juristtidning 2020, tillgänglig på: https://svjt.se/content/overlappningen-mellan-dataskydd-och-marknadsratt (hämtad 2020-12-08)

House of Representatives, *US CLOUD Act,* tillgänglig på: https://www.congress.gov/bill/115th-congress/house-bill/4943/text (hämtad 2020-12-09)

Lane Scott, Kristi, *Overview of the Privacy Act of 1974*, United States Department of Justice (2015 års upplaga), tillgänglig på: https://www.justice.gov/opcl/file/793026/download (hämtad 2020-11-19)

Larsson, Stefan & Ledendal, Jonas, *Personuppgifter som betalningsmedel* (4e upplagan), tillgänglig på: https://www.konsumentverket.se/globalassets/publikationer/produkter-och-tjanster/gemensamt/rapport-2017-4-personuppgifter-som-betalmedel-konsumentverket.pdf (hämtad 2020-12-04)

Linden, Oliver; Dahlberg, Erik, *Data Flows – a fifth freedom for the internal market?,* tillgänglig på: https://www.kommerskollegium.se/en/publications/reports/2016/data-flows---a-fifth-freedom-for-the-internal-market/ (hämtad 2020-11-19)

Magnusson Sjöberg, Cecilia, *lagkommentar nr. 239 till dataskyddsförordningen,* tillgänglig på: https://juno.nj.se/b/documents/2514469?st=karnov&t=annotations (hämtad 2020-11-20)

McAdams, James G., *Foreing Intelligence Surveillance Act (FISA): An Overview*, 10 mars 2020, tillgänglig på: https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeingIntelligenceSurveillanceAct.pdf (hämtad 2020-11-17)

Office of the Director of National Intelligence, *Section 702 Overview,* tillgänglig på: https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf (hämtad 2020-12-09)

Office of the Director of National Intelligence, *Status of Implementation of PPD-28,* oktober 2018, tillgänglig på: https://fas.org/irp/offdocs/pclob-ppd28-response.pdf (hämtad 2020-12-09)

Office of the Director of National Intelligence Civil Liberties and Privacy Office, *Civil Liberties and Privacy Information Paper: Description of Civil Liberties and Privacy Protections Incorporated in the 2008 Revision of Executive Order 12333,* tillgänglig på: https://www.dni.gov/files/documents/CLPO/CLPO_Information_Paper_on_2008_Revision_to_EO_12333.pdf (hämtad 2020-12-02)

Perry, James M., *Watergate Case Study,* Columbia Law School, tillgänglig på:http://www.columbia.edu/itc/journalism/j6075/edit/readings/watergate.html (hämtad 2020-11-26)

Poindexter, John M., *Finding the Face of Terror in Data,* New York Times 10 september 2003, tillgänglig på: https://www.nytimes.com/2003/09/10/opinion/finding-the-face-of-terror-in-data.html (hämtad 2020-11-18)

Risen, James; Lichtblau, Eric, *"Bush lets U.S spy on callers without courts: secret order to widen domestic monitoring",* tillgänglig på: https://www.pulitzer.org/winners/james-risen-and-eric-lichtblau (hämtad 2020-12-06)

Schwartz, Paul M., Solove, Daniel J., *Reconciling Personal Information in the United States and the European Union*, 13 maj 2013 https://fpf.org/wp-content/uploads/Schwartz-Solove_Reconciling-Personal-Information-in-the-US-and-EU.pdf (hämtad 2020-12-07)

Schwartz, Paul M. & Solove, Daniel J., *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 5 december 2011, tillgänglig på: https://ssrn.com/abstract=1909366 (hämtad 2020-12-08)

Senator Kirsten Gillibrand, *Pressmeddelande*,12 februari 2020, tillgänglig på: https://www.gillibrand.senate.gov/news/press/release/confronting-a-data-privacy-crisis-gillibrand-announces-landmark-legislation-to-create-a-data-protection-agency (hämtad 2020-12-09)

Solove, Daniel J.,*"I've Got Noithing to Hide" and Other Misunderstandings of Privacy*, San Diego Law Review, vol. 44. 2007, GWU School Public Law Research Paper nr. 289, tillgänglig på: http://ssrn.com/abstract=998565 (hämtad 2020-11-11-22)

United States Code, tillgänglig på: https://www.govinfo.gov/app/details/USCODE-2011-title15/USCODE-2011-title15-chap94-subchapI-sec6809/context (hämtad 2020-12-07)

US Department of Health and Human Services, *Summary of the HIPPA Security Rule,* tillgänglig på: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (hämtad 2020-11-23)

US Department of Health and Human Services Office for Civil Rights, *About us,* tillgänglig på: https://www.hhs.gov/ocr/about-us/index.html (hämtad 2020-11-23)

US Department of Justice, *Promoting Public Safety, Privacy and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act,* tillgänglig på: http://www.diva-portal.se/smash/get/diva2:1302856/FULLTEXT01.pdf (hämtad 2020-12-09)

William H. Cooper, *EU-US Economic Ties: Framework, Scope and Magnitude,* Kongressens forskningsservice, 2 april 2013, tillgänglig på: https://www.hsdl.org/?view&did=750742 (hämtad 2020-12-07)

Rättsfallsförteckning

EU-domstolen

C-101/01 av den 6 november 2003, *brottmål mot Bodil Lindqvist*, begäran om förhandsavgörande från Göta Hovrätt (Sverige)

C-131/12 av den 13 maj 2014, *Google Spain SL och Google Inc. Mot Agencia Espanola de Protección de Datos (AEPD) och Mario Costeja González*

C-362/14 av den 6 oktober 2015, Maximillian Schrems mot Data Protection Commissioner begäran om förhandsavgörande från High Court (Irland), punkt 28 och Kommissionens beslut 2000/520/EG av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat

C-434/16 av den 20 december 2017, *Nowak mot Data Protection Commissioner*, begäran om förhandsavgörande från Supreme Court (Irland)

C-311/18 av den 16 juli 2020, *Data Protection Commissioner mot Facebook Irland Limited och Maximillian Schrems,* begäran om förhandsavgörande från High Court (Irland)

Högsta domstolen i USA

United States v. Verdugo-Urquidez, 494 U.S. 259 (1990)