Svenska företags lagring av personuppgifter på amerikanska molntjänster

En analys av CLOUD Acts förenlighet med Privacy Shield och GDPR.

Jeren Agh

Juridiska institutionen
Examensarbete 30 hp.
Inriktning: Rättsinformatik
Juristprogrammet (270 hp)
Höstterminen 2018
Grupphandledare: Johan Axhamn
Engelsk titel: The storage of personal data by Swedish Companies on US cloud services - An analysis of CLOUD Act's compatibility with Privacy Shield and the GDPR.

Stockholms universitet

Abstract

This thesis investigated and analyzed the compatibility of the law of the Unites States (US) and that of the European Union (EU) with respect to authorities obtaining personal data stored on cloud services for law enforcement purposes. The new General Data Protection Regulation (GDPR) sets rules which determine who is responsible for personal data processing and on which grounds legal data transfer to third countries can take place. The United States, which is viewed as a third country according to the regulation, does not offer an adequate level of protection that meets the standard that exists within the EU. A transfer of such data to the US can therefore only be made to companies that are affiliated with an agreement between the EU and the US. The Privacy Shield decision is based on principles that companies must comply with and implement in their policy. This allows companies within EU to transfer personal data on a legal basis. Some exceptions are regulated in Privacy Shield, where US law is applied instead. This applies if the authorities wish to access personal data for law enforcement purposes. With the adoption of the new CLOUD Act, US law entitles the collection of personal data from US cloud service providers after a court has reviewed the case and issued a warrant. This is applied regardless of whether the provider's servers are located within or outside the US. The CLOUD Act also allows the US to enter into agreements with other foreign states regarding access to personal data from US cloud service providers. This happens after an analysis by the Attorney General, who decides whether the country in question has requirements which are justifiable. This has led to a number of issues where, among other things, resulted in Privacy Shield's level of protection and validity being questioned. The extraterritorial application of the CLOUD Act has also been criticized as it may be in contradiction to the GDPR and its rules on third country data transfer. This essay has focused on making a legal inquiry into any possible contradictions between the CLOUD Act and the protection that Privacy Shield guarantees. It also included an analysis of the compatibility of the CLOUD Act and the GDPR rules on a third country transfer. An open question arose as Privacy Shield could be annulled if the executive agreements do not live up to a sufficiently higher level of protection that is satisfactory. The requirements imposed by CLOUD Act on the conclusion of the executive agreements will thus be decisive for Privacy Shield's validity. However, the CLOUD Act's extraterritorial regulation of the collection of personal data contained in servers inside the EU conflicts with Article 48 of the GDPR. Personal data controllers within the EU, therefore, should review their use of US cloud services in adopting CLOUD Act.

Nyckelord

Dataskyddsförordningen, Personuppgiftsansvarig, Artikel 48 GDPR, Privacy Shield, CLOUD Act

Förord

Det känns overkligt att det här förmodligen blir de sista orden jag skriver innan jag blir klar med 4,5 års studier. Men innan dess måste jag passa på att tacka min familj och vänner som har stöttat mig under min studietid och speciellt under mitt uppsatsskrivande.

Jag vill först börja med att tacka mina föräldrar för allt stöd jag har fått under min studietid. Jag vill också tacka mina få men underbara vänner. Ett speciellt tack till Sagar som har hjälp mig med alla mina funderingar kring den tekniska biten. Tack till Sofia och Aviva som har läst igenom uppsatsen och gett feedback. Även ett stort tack till Ulrika Kindberg Annas, min lärare i högstadiet som tog sig sin tid att läsa igenom uppsatsen.

Jag vill också tacka alla lärare på Stockholms universitet för den tid de har lagt ner på oss studenter. Framförallt min handledare Johan Axhamn för all vägledning och goda råd som jag har fått. Men också min studentgrupp, Oskar, Stella, Sara och Stellan för den konstruktiva kritiken.

Innehållsförteckning

Förkortningar

BCR	Binding Corporate Rules
CLOUD Act	Clarifying Lawful Overseas Use of Data
Dataskyddsdirektivet	Europaparlamentet och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om behandling av de fria flödet av sådana uppgifter.
Dataskyddsförordningen	Europaparlamentets och rådets förordning EU 2016/617 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (Allmän dataskyddsförordningen)
ECPA	Electronic Communication Privacy Act
ECS	Electronic Communication Service
EDPB	European Data Protection Board
EKMR	Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna
EU	Europeiska Unionen
EU-domstolen	Europeiska unionens domstolsou
FBI	Federal Bureau of Investigation
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation

ITA	International Trade Administration
LIBE	The Committee on Civil Liberties, Justice and Home Affairs
NSA	National Security Agency
NIST	National Institute of Standards and Technology
RCS	Remote Computing Service
Rättighetsstadgan	Europeiska unionens stadga om de grundläggande rättigheterna (2010/C 83/02)
Prop.	Proposition
Privacy Shield	Kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016 enligt Europaparlamentets och rådets direktiv 95/746/EG om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna.
PuL	Personuppgiftslag (1998:204)
RF	Regeringsformen (1974:152)
SCA	Stored Communications Act
SPI- modellen	Software, Platform, Infrastructure as Model

1. Inledning

1.1 Bakgrund

I ett allt mer digitaliserat samhälle lagrar företag, organisationer och myndigheter dagligen data på molntjänster som företag både inom och utanför EU tillhandahåller. Företag har i samband med att nya europeiska dataskyddsförordningen General Data Protection Regulation (GDPR) trädde i kraft i maj 2018 fått se över vad men framförallt var de lagrar data som innefattar personuppgifter.[1] GDPR ställer upp ett antal krav, vilket även den tidigare personuppgiftslagen(1998:204), PuL, gjorde för behandlingen av personuppgifter. Kraven sträcker sig till att omfatta den behandling som äger rum både inom EU och vid tredjelandsöverföringar för att säkerställa att en adekvat skyddsnivå upprätthålls hela vägen. Länder som USA med väletablerade molntjänstleverantörer som Google, Dropbox och Microsoft har enligt EU-kommissionens beslut inte en tillräckligt hög skyddsnivå.[2] För att lösa problemet ingick EU 2016 en överenskommelse om skydd för personuppgifter med USA och antog därmed ett genomförandebeslut, det så kallade Privacy Shield. Beslutet innebär inte att USA upprätthåller en adekvat skyddsnivå, utan de amerikanska företag som anslutit sig är skyldiga att följa vissa principer när de behandlar personuppgifter som överförts från EU.[3]

Det råder osäkerhet kring beslutets giltighet vilket medför konsekvenser för de många framstående amerikanska molntjänstleverantörerna som anslutit sig. Tidigare ogiltiga överenskommelser som föregångaren Safe Harbor och kritik gentemot delar av Privacy Shield har föranlett företag till att i huvudsak fokusera på att ha kontroll över var data fysiskt lagras. Många svenska företag som använder sig av molntjänster har fokuserat på GDPR och arbetat för att se till att servrarna de lagrar på faktiskt befinner sig inom EU:s gränser. Det många svenska företag inte är medvetna om är att en ny amerikansk lag har antagits vilket gör att servrarnas plats inte längre har en avgörande betydelse. Clarifying Lawful Overseas Use of Data Act (CLOUD Act) som trädde i kraft den 23 mars 2018 innebär att den amerikanska staten kan tvinga amerikanska molntjänstföretag att lämna ut data innehållande personuppgifter till amerikanska brottsbekämpande myndigheter oavsett i vilket land servrarna är belägna. Den nya lagen gör rättsläget ännu mer osäkert och på EU-nivå har det riktats kritik mot CLOUD Act. Europeiska parlamentet ifrågasätter bland annat om den nya lagen kan komma i konflikt med den unionsrättsliga lagstiftningen på området. Det ifrågasätts också om de

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

[2] Datainspektionen, *hur vet vi om ett tredje land har adekvat skyddsnivå,* https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/tredjelandsoverforing/hur-vet-vi-om-ett-tredje-land-har-adekvat-skyddsniva/, hämtad 2018-09-13.

[3] Se https://www.privacyshield.gov/list, hämtad 2018-09-13.

företag anslutna till Privacy Shield kan anses efterleva de principer som beslutet bygger på.[4] Den uppkomna situationen leder till oenigheter kring det faktiska rättsläget. Svenska företag som lagrar personuppgifter på amerikanska molntjänstleverantörer bör ifrågasätta vilka konsekvenser den nya lagen kan komma att innebära för dem.

1.2 Syfte och frågeställning

Syftet med uppsatsen är att göra en rättslig utredning om det finns någon motsättning mellan CLOUD Act och Privacy Shield inbegripet de regler om tredjelandsöverföring och personuppgiftsansvariga som följer av dataskyddsförordningen. Följande frågor kommer därför att besvaras:

- Under vilka förutsättningar får personuppgiftsansvariga enligt dataskyddsförordningen genom molntjänster överföra personuppgifter till USA?
- Vad är CLOUD Act och Privacy Shield och hur förenliga är de?
- Hur förenlig är CLOUD Act med dataskyddsförordningens regler om tredjelandsöverföring och det ansvar som åligger de personuppgiftsansvariga?

1.3 Avgränsning

EU har lagt fram ett förslag om en förordning som behandlar tillgången till e-bevisning inom och utanför EU. Det innebär att europeiska myndigheter kan få tillgång till bevisning från molntjänstföretag som lagrar information på servrar i tredje land. Det förslaget kommer dock inte att behandlas då arbetet skulle bli allt för omfattande. Inte heller själva ingåendet av ett exekutivt avtal med en utländsk stat som regleras i CLOUD Act kommer att beskrivas, utan endast de krav som CLOUD Act ställer upp på en utländsk stat. Likaså kommer inte Lag (2000:562) om internationell rättslig hjälp i brottmål att behandlas då arbetet blir allt för omfattande.

Uppsatsen kommer att belysa problematiken kring de effektiva rättsmedlen som finns tillhanda utan att göra en djupare utredning kring de olika processuella reglerna som de olika lagarna ställer upp.

1.4 Metod och material

Uppsatsen kommer i grunden att bygga på den rättsdogmatiska metoden för att fastställa gällande rätt utifrån ett svenskt perspektiv. Rättskällor som lagtext, förarbeten, rättspraxis och doktrin kommer beaktas. Ansvarsfördelning vid behandling av personuppgifter och tredjelandsöverföring reglerades i PuL som i sin tur byggde på dataskyddsdirektivet. Vägledning kommer därför att hämtas från äldre lagtext, förarbeten, och praxis som fortfarande är aktuell då ingen ny praxis tillkommit på området. Även doktrin kommer att beaktas i den mån det blir aktuellt.

[4] European Parliament, *Motion for a resolution*, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+B8-2018-0305+0+DOC+PDF+V0//EN, 2018, hämtad 2018-09-13.

Dataskyddsförordningen som är direkt tillämplig som svensk lag kommer att behandlas i enlighet med den EU-rättsliga metoden. Det kan diskuteras huruvida EU-rätten inkluderas i den rättsdogmatiska metoden då svensk rätt på många områden bygger på EU-rätten. Dataskyddsförordningen med dess artiklar och skäl är mer omfattande och komplexa än vanlig svensk lag.[5] Det gör att den traditionella rättsdogmatiska metoden med den fast vedertagna rättskälleläran inte ger en rättvisande bild. Domstolsavgöranden och generella principer som genomsyrar EU-rätten blir viktiga vid tolkningen och ett fastställande av de olika artiklarnas innebörd. Det blir dock svårt att hitta avgöranden från EU-domstolen när det gäller tolkningen av dataskyddsförordningen då den är relativt ny. EU-domstolens ändamålsenliga tolkning leder till att praxis utarbetad i och med dataskyddsdirektivet blir relevant då det materiella innehållet till viss del är densamma. I avsaknad av praxis kommer vikt att läggas på så kallad ”soft law”. Riktlinjer utarbetade av Artikel 29-gruppen som senare ersattes av Europeiska dataskyddsstyrelsen (EDPB) kommer att beaktas. EDPB som ger råd och vägledning kring hur artiklar i GDPR ska tolkas består av representanter från de olika medlemsländernas dataskyddsmyndigheter.[6] EDPBs vägledning kring undantagen för tredjelandsöverföringar är inte bindande men har ändå en normgivande funktion.[7] Även annan ”soft law” som uttalanden från datainspektionen, lagkommentarer och andra rättsutlåtanden kommer att invägas för att kunna fastställa gällande rätt.[8]

En stor del av uppsatsen kommer att behandla amerikansk rätt för att kunna granska lagarnas förenlighet med EU-och svensk rätt. Det angloamerikanska rättssystemet och den metod domstolarna använder för att fastställa gällande rätt liknar den svenska.[9] De amerikanska domstolarna börjar oftast med ”The plain meaning rule” där lagen ska tolkas så som den är skriven.[10] Skulle lagtexten vara oklar eller mångtydig så övergår domstolen till att istället granska kongressens avsikt när lagen antogs.[11] De amerikanska domstolarna kommer sedan i och med sin tolkning att skapa rätt. Det skiljer sig från det svenska rättssystemet då avsaknaden av tydlig applicerbar lag inte kan leda till att domstolarna skapar rätt. De amerikanska prejudikaten blir vägledande, dock så går det att argumentera för en annan lösning om lagtexten skulle lämna utrymme för det. Ett liknande tillvägagångssätt kommer att användas för att fastställa gällande rätt där stort fokus kommer att läggas

[5] Sjöberg Magnusson, Cecilia, Rättsinformatik, Juridiken i det digitala informationssamhället, s. 171.

[6] Datainspektionen, *Så här är dataskyddet organiserat i EU,* https://www.datainspektionen.se/om-oss/datainspektionens-internationella-arbete/sa-har-ar-dataskyddet-organiserat-i-eu/, hämtad 2018-09-13.

[7] Korling, F, Zamboni, M, (red.), *Juridisk metodlära,* 1 u, Studentlitteratur AB 2013, s 128.

[8] Sjöberg, Magnusson, Rättsinformatik, J*uridiken i det digitala informationssamhället*, s. 171.

[9] Carlson, L, American business law: A civil law perspective, Iustus,2004, s 23.

[10] CRS Report for Congress, received through the CRS Web, *Staturory Interpretation: General Principles and Recent Trends,* 2006, https://www.everycrsreport.com/files/20060330_97589_d597ae5a20af3bc9dc0711704bb2329308fd81f1.pdf, hämtad 2018-12-10.

[11] CRS Report for Congress, received through the CRS Web*, Staturory Interpretation: General Principles and Recent Trends,* 2006.

på att tolka lagtexten. För att få en djupare insikt i ämnet kommer även själva syftet med lagen och kongressens avsikt med lagens att beskrivas. I och med avsaknaden av praxis då CLOUD Act är en ny lag kommer istället artiklar och andra rättsutlåtanden kring tolkningen av lagen att granskas.

Både den EU-rättsliga och amerikanska tolkningsmetoden kommer att tillämpas vid beskrivandet av Privacy Shield då beslutet innehåller båda delarna. För att tolka innehållet i Privacy Shield kommer den EU-rättsliga metoden att användas då beslutet som inte är en lagstiftningsakt antogs i enlighet med dataskyddsdirektivet. Däremot kommer de undantagen som stadgas och där det hänvisas till amerikansk lag analyseras i enlighet med den amerikanska tolkningsmetoden.

Slutligen så kommer uppsatsen att använda sig av en rättsinformatisk metod då uppsatsen utgår från den teknik som molntjänstleverantörer har utvecklat. Molntjänsternas karaktäristiska särdrag där användare kan få tillgång till information på en plats samtidigt som data kan lagras i flera olika delar av världen gör juridiken svårapplicerad. Den rättsinformatiska metoden är då lämplig då den fokuserar på de problem som kan uppkomma när juridiken ska appliceras i de digitala miljöerna. Det handlar inte om att juridiken är ny utan miljöerna där ingen fysisk kontroll är möjlig gör rättsläget osäkert.[12] Den rättsdogmatiska metoden besvarar som bäst konkreta frågeställningar.[13] Metoden är därför inte lämplig på de områden i uppsatsen då juridiken ska tillämpas på tekniken då många svar inte går att finna i de klassiska rättskällorna. Rättsutlåtanden, myndighetsföreskrifter och artiklar kommer därför att granskas. Bland annat för att förklara den tekniska biten men också för att problematisera den ur ett juridiskt perspektiv.

1.5 Disposition

Uppsatsen inleds med att behandla vad molntjänster är för att sedan gå igenom det materiella och territoriella tillämpningsområdet. Vad en behandling av personuppgifter innefattar, ansvarsfördelningen mellan personuppgiftsansvarig och biträde samt tredjelandsöverföringar kommer därefter att utredas. I nästkommande avsnitt redogörs det för den internationella rätten där den folkrättsliga territorialprincipen och nationalprincipen till en början beskrivs. De ömsesidiga rättsliga avtalen kommer därefter att behandlas samt en introduktion av amerikansk rätt. Därefter kommer en beskrivning av det amerikanska konstitutionella skyddet och andra amerikanska lagar som CLOUD Act bygger på. Det inkluderar ett rättsfall och en beskrivning av vad CLOUD Act är. Privacy Shield kommer att beskrivas där även föregångaren Safe Harbor behandlas. Slutligen kommer CLOUD Acts förenlighet med Privacy Shield och GDPR att analyseras inkluderat de personuppgiftsansvarigas ansvar för att sedan avsluta uppsatsen med en sammanfattande slutsats.

[12] Sjöberg, Magnusson, Rättsinformatik, J*uridiken i det digitala informationssamhället*, s. 440.

[13] Korling, F, Zamboni, M, (red.), *Juridisk metodlära,* 1 u, Studentlitteratur AB 2013, s 23.

2. Molntjänster

För att få en bättre förståelse kring problematiken vid överföring till tredje land via molntjänster krävs en genomgång av den tekniska biten av hur molntjänster fungerar. De olika aktörerna som kunder och leverantörer spelar en viktig roll då de rent tekniskt har ansvar och kontroll över olika delarna vilket vid ett senare skede blir avgörande vid fastställandet av deras skyldigheter enligt GDPR.

2.1 Varför använder vi molntjänster?

Privatpersoner, myndigheter och företag lagrar data på olika sätt, det kan ske genom att man lagrar data på en hårddisk, fil eller andra externa lagringsobjekt. I och med utvecklingen av tekniken och digitaliseringen av samhället så har många istället valt att lagra data på molntjänster. Lagringen är effektiv och lättillgänglig då molntjänsterna bygger på en internetbaserad resurs som levereras till kunden vid behov.[14] Kunderna kan oavsett var de rent fysiskt befinner sig komma åt data så länge de via någon enhet kan koppla upp sig till internet. Det medför att kunderna inte behöver någon egen utrustning utan de betalar endast för det utrymme de använder. Leverantörerna i sin tur står för de datorhallar med servrar där data placeras.

2.2 Definition av molntjänst

Idag finns det ungefär lika många definitioner av molntjänster som leverantörer. En enhetlig och legal definition saknas. Däremot har det Amerikanska federala myndigheten, National Institute of Standards and Technology (NIST) utarbetat en teknisk definition som har följande lydelse;

”[…] en modell för att vid behov (on-demand) möjliggöra allmänt tillgängligt och behändig nätverksaccess till en delad och gemensam mängd av konfigurerbara datorresurser (exempelvis nätverk, servrar, datalagring, datorprogram och tjänster) som snabbt kan göras tillgängliga och frigöras med minimal insats och utan direkt interaktion men molntjänstleverantören”[15]

Fem grundläggande särdrag beskrivs i definitionen och dessa kriterier är avgörande för om en tjänst ska klassificeras som molntjänst.

[14] Sjöberg, Magnusson, Rättsinformatik, J*uridiken i det digitala informationssamhället*, s. 440.

[15] Mell, Grance, *The NIST Definition of Cloud Computing*, s. 2. (översatt till svenska av Edvardsson, Tobias & Frydlinger, David, *Molntjänster: juridik, affär och säkerhet*, Nordstedts Juridik AB, 2018, s. 22)

2.2.1 Molntjänsters karaktäristiska särdrag

Det finns olika kriterier som är avgörande för om en tjänst ska klassificeras som en molntjänst enligt NIST. En molntjänst ska vara *tillgänglig via självbetjäning och vid behov*. Det innebär att kunden ska vara självständig i förhållande till leverantören. Kunden ska själv kunna ansluta sig, använda och avsluta molntjänsten utan någon direkt personlig kontakt med leverantören.[16] Leverantören ska se till så att tjänsten alltid är funktionell och tekniskt tillgänglig.

Den andra egenskapen, *bred tillgänglighet via internet,* innebär att tillgängligheten ska vara geografisk obunden. Platsen ska inte vara avgörande och kunden ska ha tillgång till tjänsten oavsett vilken plattform som används (datorer, mobiltelefoner, surfplattor eller andra liknande föremål).[17]

Konsolidering av resurser som är det tredje särdraget innebär att resurserna som datorkraft, minne, lagring och bandbredd samt leverantörens infrastruktur oftast är okänt för kunden. Tjänsten ska uppfattas som ett system där kunden inte ska ha någon kännedom om hur många samt var servrarna är placerade.[18] Det är praktiskt fördelaktig för kunden att inte behöva engagera sig och förhandla kring den tekniska lösningen. Samtidigt så kan det vara till kundens nackdel då det försvårar kontrollen och efterlevnaden av dataskyddsförordningen.

Det fjärde särdraget, *omedelbar elasticitet,* syftar på att kapaciteten anpassas efter kundens användning. Kapaciteten anpassar sig omedelbart då kunden väljer att använda mer eller mindre av tjänsten vilket i princip är omärkbart för kunden.[19]

Det sista särdraget, *kontrollerad tjänsteleverans,* tar sikte på själva mätningen av nyttjandet. Det ska vara transparent för både kunden och leverantören då kunden endast betalar för det faktiska nyttjandet. Det i sig mäts i storheter där man tittar på hur mycket kapacitet som används vid lagring, användandet av bandbredd, antal aktiva konton samt processorkraftsberäkningar. Det kan dock skilja sig åt beroende på molntjänst. [20]

2.2.2 Tjänste- och leveransmodeller

Det finns tre olika tjänstemodeller enligt NIST-definitionen. Den så kallade SPI-modellen. Tjänster som faller inom definitionen är datorprogram, plattform eller infrastruktur som tjänst. Varje modell erbjuder en viss nivå av service varvid det avgörande är kundens behov och hur stort ansvar de tar för utvecklingen av tjänsten.[21] Vissa är mer tekniskt avancerade som datorprogram som tjänst medan

[16] Mell m fl, *The NIST Definition of Cloud Computing*, s. 2.

[17] Sjöberg, Magnusson, *Rättsinformatik, Juridiken i det digitala informationssamhället*, s. 442.

[18] Mell m fl, *The NIST Definition of Cloud Computing,* s. 2.

[19] Sjöberg, Magnusson, *Rättsinformatik, Juridiken i det digitala informationssamhället*, s. 443.

[20] Edvardsson m fl, *Molntjänster: juridik, affär och säkerhet,* s. 25.

[21] Kavis, Michael, *Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS),* Wiley 2014, s 37-38.

andra som infrastruktur som service erbjuder mer grundläggande tjänster. Dock så erbjuder alla de tre modellerna lagring vilket innebär att kunden kommer vara en del av ett virtuellt system.

Utöver valet av tjänstemodell så måste även kunden välja en leveransmodell, de kan enligt NIST-definitionen tillhandahållas på fyra olika sätt. Tjänsterna kan levereras i privata, gemensamma eller publika moln. Hybrider av dessa tre förekommer också. Privata moln fokuserar och levererar till den enskilda kunden genom att kunden kan bestämma om ägarskap. Det kan ägas av kunden själv, leverantören eller båda tillsammans.[22] Det skiljer sig från *gemensamma moln* där flera kunder med liknande uppdrag, mål eller krav delar gemensamt på molntjänsten.[23] Kunder avgör vem eller vilka av kunderna, leverantören eller de tillsammans som ska äga och ska driva molntjänsten. Datorhallarna kan då antingen vara hos leverantören eller kunden. De publika molnen, där datorhallarna av praktiska skäl är placerade hos leverantören, tillhandahålls tjänsten allmänheten. Kunderna har därmed ingen kontroll över servrarna annat än kunskapen om var de är placerade.[24] Amazon, Google Gmail och Dropbox utgör några exempel på publika moln som erbjuder sina tjänster till allmänheten.

De olika tjänste-och leveransmodellerna är anpassade efter kundens behov. Skulle servrarna vara ägda och placerade hos kunden så uppkommer inga svårigheter när det gäller kontrollen av var data befinner sig. Däremot uppstår problem där lagringen förekommer i leverantörens datorhallar. Uppsatsen kommer i huvudsak att fokusera på de publika molntjänsterna där lagringen förekommer i leverantörens datorhallar. Det medför att kunden har mindre kontroll, om nästan ingen alls, förutom att kunden kan få kännedom om var servrarna fysiskt befinner sig. Vilka servar viss data lagras på är inte lika enkelt att få vetskap om. Avtalet blir därför det enda sättet för kunden att få kontroll över lagringen. Dock så använder oftast leverantörer, av praktiska skäl, standardavtal vid tjänster i publika moln då det skulle vara ekonomiskt och tidsmässigt krävande att ingå enskilda avtal med alla kunder. Ansvarsfrågan blir därmed viktig att utreda. Parterna och deras ansvar för lagringen kommer att redogöras för i nästa avsnitt.

[22] Sjöberg, Magnusson *Rättsinformatik, Juridiken i det digitala informationssamhället*, s. 445.

[23] Mell m fl, *The NIST Definition of Cloud Computing*, s. 2.

[24] Kavis, Michael, *Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS),* Wiley 2014, s. 42.

3. Dataskyddsförordningen

Det är viktigt att utreda ansvarsfrågan enligt GDPR vid molntjänster då den personuppgiftsansvariga och personuppgiftsbiträdet har viktiga roller i efterlevnaden av förordningen. Även överföringen till tredje land måste vila på en laglig grund enligt förordningen, det kommer därmed att behandlas i de kommande delarna.

3.1 En ny dataskyddsförordning

GDPR som tillämpas i hela EU sedan den 25 maj 2018 har ersatt den tidigare svenska personuppgiftslagen som byggde på dataskyddsdirektivet.[25] Syftet är att på ett likformigt och enhetligt sätt skydda fysiska personer gentemot företag, myndigheter och andra organisationer som behandlar deras personuppgifter. Det fria flödet av personuppgifter inom EU främjas enlig artikel 1 GDPR då förordningen blir direkt tillämplig i alla medlemsländer. Förordningen reglerar inte endast nya och tidigare oreglerade områden då personuppgiftslagen innehöll liknande bestämmelser. Däremot har ansvaret för personuppgiftsbiträden ökat. Likaså har den personuppgiftsansvarige fler skyldigheter.[26] Även andra rättigheter för de enskilda som rätten att bli bortglömd och andra regleringar kring profilering är nya i GDPR.[27] De unika särdragen kommer dock inte att utredas, däremot är det värt att nämna de höga sanktionsavgifterna som regleras i GDPR. Avgifterna kan enligt artikel 83.5 GDPR som högst uppgå till 20 miljoner euro eller fyra procent av ett företags globala årsomsättning. De höga avgifterna leder till att förordningen får ett större genomslag. Låga avgifter skulle leda till att endast mindre företag skulle bli avskräckta medan ekonomiskt stabila företag skulle kunna överväga fördelarna.

3.1.1 Integritetsskydd vid behandling

Lagstiftaren har sedan slutet på 1900–talet uppmärksammat behovet av ett integritetsskydd i digitala miljöer.[28] Skyddet är idag fastställt både i grundlag, Europakonventionen samt EU:s rättighetsstadga. I regeringsformen 1 kap. 2 § 4 st. ska det allmänna värna om den enskildes privatliv. De enskilda är enligt 2 kap. 3 § 2 st. regeringsformen skyddad gentemot det allmänna mot betydande intrång i den personliga integriteten som skett utan samtycke och som innebär övervakning eller kartläggning av

[25] 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.

[26] Monika, Wendleby, Dag, Wetterberg, *Dataskyddsförordningen GDPR, förstå och tillämpa i praktiken*, Utbildning AB, 2018, s 25.

[27] Wendleby m fl, *Dataskyddsförordningen GDPR, förstå och tillämpa i praktiken,* s 27.

[28] Sjöberg, Magnusson, *Rättsinformatik, Juridiken i det digitala informationssamhället*, s. 149.

den enskildes personliga förhållanden. Regleringen tar endast sikte skyddet gentemot det allmänna och kan i vissa fall begränsas enligt lag.[29] En liknande reglering finns i Europakonventionen som är inkorporerad i svensk rätt.[30] Artikel 8 stadgar att var och en har rätt till respekt för sitt privat-och familjeliv, men även konventionen har vissa undantag. En nästan identisk artikel om respekten för privatlivet som konventionen reglerar finns i EU-stadgans artikel 7. Stadgan har till skillnad från konventionen ett specifikt skydd för personuppgifter i artikel 8. Både artikel 7 och 8 i stadgan kan dock inskränkas under vissa förutsättningar.[31]

Innebörden av begreppet personlig integritet kan ifrågasättas då ingen av dessa lagar eller konventioner innehåller någon definition. I förarbetena till regeringsformen, som låg till grund för det utökade grundlagsskyddet i 2 kap, menade regeringen på att det är svårt att hitta en allmänt accepterad definition.[32] Regeringen uttalade sig om vad en kränkning av den personliga integriteten kan tänkas innebära.

”[…] kränkningar av den personliga integriteten utgör intrång i den fredade sfär som den enskilde bör vara tillförsäkrad och där intrång bör kunna avvisas.”

Om uttalandet klargör eller förtydligar vad den personliga integritet egentligen innebär kan diskuteras. Uttalandet tyder på att de enskilda har någon privat sfär där intrång endast i undantagsfall får förekomma. Var gränsen går kan inte utläsas och det kan variera beroende på vilket land man befinner sig i, vilken tid samt kultur man kommer ifrån.[33] Det kan också se annorlunda ut beroende på vilka personuppgifter som behandlas, på vilket sätt samt i vilket syfte. Det kan konstateras att det värnas om den personliga integriteten då de enskilda ska skyddas mot det allmänna men också gentemot andra aktörer genom det allmännas skydd. Dataskyddsförordningen har till uppgift att stärka skyddet för den personliga integriteten i de digitala miljöerna då artiklarna sätter ramen för hur en korrekt personuppgiftsbehandling ska gå till. Trots att begreppet fortfarande är oklart och kan se väldigt olika ut även inom EU:s gränser så ska intrång inte ske i den enskildes sfär så länge dataskyddsförordningens efterlevs.

[29] Se regeringsformen 2 kap. 20-22 §§.

[30] Se Lag (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.

[31] Se artikel 52 i Europeiska unionens stadga om de grundläggande rättigheterna (2010/c 83/02)

[32] Prop. 2009/10:80 s.175.

[33] Sjöberg, Magnusson*, Rättsinformatik, Juridiken i det digitala informationssamhället,* s. 146.

3.2 Det materiella tillämpningsområdet

I artikel 2.1 GDPR framgår det att förordningen tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register. För att inte inskränka tillämpningsområdet så har begreppet personuppgift i artikel 4.1 GDPR getts en vidsträckt tolkning. En personuppgift utgör varje upplysning som avser antingen en redan identifierad eller en identifierbar fysisk person (en så kallad registrerad). Den registrerade måste antingen direkt eller indirekt kunna identifieras för att omfattas. Det kan handla om direkta uppgifter som namn, identifikationsnummer eller indirekta som onlineidentifikationer som exempelvis IP-adresser som kan härledas till en person.[34]

För att GDPR ska bli tillämplig så krävs det också att en behandling företas. I definitionen i artikel 4.2 GDPR framgår det att en behandling avser en åtgärd eller en kombination av åtgärder av personuppgifter eller uppsättningar av personuppgifter oavsett om de är automatiserade eller inte. Tillämpningen har underlättats då ingen egentlig grad av automatik krävs.[35] Insamlingar, registreringar, lagringar, bearbetningar, utlämning genom överföring eller radering är några behandlingar som artikeln tar upp.

Det som faller utanför förordningen och som bör nämnas är enligt artikel 2.2(d) behöriga myndigheters hantering av personuppgifter i syfte att förebygga, förhindra eller utreda brott. Då blir istället direktiv 2016/680 tillämplig där regler liknande de i dataskyddsförordningen uppställs för myndigheters behandling av personuppgifter och överföring till tredje land.[36] Direktivet kommer dock inte att redogöras för då uppsatsen behandlar privata aktörers behandling av personuppgifter.

3.3 Det territoriella tillämpningsområdet

I artikel 3 GDPR stadgas det att dataskyddsförordningen i första hand bygger på etableringsprincipen. Det innebär att förordningen tar sikte på de situationer då den personuppgiftsansvarige eller biträdet har sitt verksamhetsställe inom unionen. Det gäller oavsett om själva behandlingen utförs i unionen eller inte. Det inbegriper även enligt artikel 3.3 GDPR det områden där en medlemsstat nationella rätt blir tillämplig enligt folkrätten. Verksamhetsstället beskrivs som det ställe där det faktiska och reella utförandet av verksamheten med hjälp av en stabil struktur äger rum.[37] Den rättsliga formen, filial

[34] Sjöberg, Magnusson, *Rättsinformatik, Juridiken i det digitala informationssamhället*, s. 176.

[35] Sjöberg, Magnusson, *Rättsinformatik, Juridiken i det digitala informationssamhället,* s. 173.

[36] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut (2008/977/RIF)

[37] Se skäl 22 i GDPR

eller dotterbolag, ska inte vara den avgörande faktorn. Inte heller registreringen i sig är utslagsgivande, men det kan det få betydelse vid en helhetsbedömning.[38]

Skulle ett etableringsställe inte kunna fastställas så kan förordningen ändå bli tillämplig. Andra punkten i GDPR artikel 3 inriktar sig på de situationer när den personuppgiftsansvariga eller biträdet istället riktar sin handel mot eller övervakar registrerades beteenden inom unionen. Handeln måste då specifikt vara inriktad mot konsumenter samt andra registrerade inom EU.[39]

Både personuppgiftsansvarige och biträdet kan hållas ansvariga enligt GDPRs artikel 3 om de båda skulle ha sitt etableringsställe inom unionen. Skulle däremot endast den ansvarige ha sitt säte inom unionen och biträdet i tredje land så kan inte förordningen tillämpas på biträdet. Biträdet måste då rikta sin verksamhet mot den europeiska marknaden för att omfattas. Det betyder inte att den ansvariga kan slippa ansvar genom att hänvisa till biträdet som inte behandlade i enlighet med förordningen. Personuppgiftsansvarige har ett självständigt ansvar vilket medför att det åligger den ansvarige att ingå ett biträdesavtal med molntjänstleverantören. Förordningen kommer därmed indirekt även bli applicerbar på den beskrivna situationen då behandlingen ska ske i enlighet med dess stadganden.[40]

3.4 Vilka omfattas av dataskyddsförordningen

Alla företag som samlar in, bearbetar, lagrar eller på något annat sätt behandlar personuppgifter omfattas av förordningen. Det är den personuppgiftsansvariga som bestämmer hur och i vilket syfte behandlingen ska gå till medan biträde sköter själva behandlingen. I de fall lagring efterfrågas sker det endast i enlighet med instruktioner och för den ansvariges räkning.

3.4.1 Personuppgiftsansvarig

Personuppgiftsansvarige åläggs hela ansvaret vid behandling av personuppgifter oavsett om de själva utför behandlingen eller att det utförs på deras vägnar.[41] Den som verkställer behandlingen är inte alltid den som intar rollen som personuppgiftsansvarig, utan det avgörande är vem som faktiskt bestämmer ändamålen med behandlingen och hur den ska gå till.[42] Behandlingen måste ske i enlighet med förordningens stadganden och den ansvariga måste kunna visa på att förordningen följs. Enligt artikel 4.7 GDPR kan fysiska eller juridiska personer, offentliga myndigheter, institutioner eller andra organ kan inträda antingen ensamma eller tillsammans in i rollen som personuppgiftsansvarig. Det är oftast styrelsen i ett företag som är personuppgiftsansvarig även om de skulle utse en person som har

[38] Voigt, Paul, On dem Bussche, Axel, *The EU General Data Protection Regulation (GDPR),* A Practical Guide, Springer International Publishing AG s. 23.

[39] Se Skäl 23 och 24 i GDPR

[40] Voigt, m fl, *The EU General Data Protection Regulation (GDPR),* A Practical Guide, s. 25.

[41] Skäl 74 GDPR

[42] Voigt, m fl, *The EU General Data Protection Regulation (GDPR),* A Practical Guide, s. 19.

hand om personuppgiftsbehandlingen. Med fysiska personer åsyftar förordningen oftast den som bedriver näringsverksamhet i enskild firma.[43] Det kan också särskilt anges i lag eller förordning vem som är att anse som personuppgiftsansvarig.

3.4.2 Personuppgiftsbiträde och underbiträde

Personuppgiftsbiträdet har i och med ikraftträdandet av förordningen fått ett utökat ansvar i jämförelse med dataskyddsdirektivet. Biträdet har som skyldighet att föra register och tillförsäkra att en tillräckligt hög säkerhetsnivå vid behandling av personuppgifter upprätthålls. Precis som den ansvarige så kan ett biträde enligt artikel 4.8 GDPR vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. Biträdet får inte i enlighet med artikel 28.2 GDPR anlita ytterligare biträden utan den personuppgiftsansvariges godkännande. Biträdet måste inhämta ett skriftligt tillstånd av den ansvariga för att kunna använda sig av underbiträden. Vid en generell fullmakt så måste biträdet informera den ansvarige innan ett underbiträde anlitas eller ändras då den ansvarige måste ges en möjlighet att invända. Biträdet eller underbiträdet får inte behandla uppgifterna i strid med givna instruktioner, dessa framkommer i ett biträdesavtal som parterna är skyldiga att teckna 28.3(a) GDPR.

3.4.3 Ansvarsfördelning vid molntjänster

Det är oftast användaren av molntjänster som är den personuppgiftsansvarige vid molntjänstavtal. Det innebär att kunden har det huvudsakliga ansvaret för behandlingen av personuppgifter, oavsett vilken tjänste-eller leverantörsmodell som aktualiseras. Den ansvarige ska se till att den registrerade inte blir kränkt. Det sker genom att ett avtal enligt artikel 28.3 GDPR eller annan bindande rättsakt ingås med samtliga biträden. Avtalet ska reglera föremålet för behandlingen, dess varaktighet, art och ändamål, typ av personuppgifter och kategorier av registrerade och personuppgiftsansvariges skyldigheter och rättigheter. De villkor som avtalats får inte ändras utan den ansvariges godkännande.[44] Den ansvarige ska endast anlita biträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder.

Det spelar ingen någon roll vilken titel en leverantör eller kund har utan funktionen är avgörande. Den som har en självständig bestämmanderätt till varför samt hur personuppgifterna ska behandlas ska anses vara ansvarig oavsett om det skulle vara molntjänstleverantören som skulle inneha den rollen. Leverantören av en molntjänst brukar oftast inta rollen som ett biträde då leverantören oftast innehar den passiva rollen genom att endast förhålla sig till vad som är avtalat.

[43] Wendleby, m fl*, Dataskyddsförordningen GDPR, Förstå och tillämpa i praktiken* s. 29.

[44] Sjöberg, Magnusson, *Rättsinformatik, Juridiken i det digitala informationssamhället*, s. 202

3.5 Överföring till tredje land

Dataskyddsförordningen behandlar i dess femte kapitel tredjelandsöverföringar för att säkerställa att förordningens skydd inte undergrävs genom att personuppgifter överförs till tredje land. Regleringen liknar dataskyddsdirektivets samt personuppgiftslagens bestämmelser. De länder förordningen tar sikte på är de utanför EU och EES-området och de situationer då personuppgifterna skulle vidarebefordras från tredje land.[45] Syftet med själva överföringen måste enligt artikel 44 GDPR vara att personuppgifterna antingen är under behandling eller är avsedda att behandlas. I sådana fall ska behandlingen stämma överens med de bestämmelser som finns i femte kapitlet då de höga sanktionerna i artikel 83.5(c) GDPR även inbegriper dessa bestämmelser. Vad som ryms inom begreppet överföring framgår inte i förordningen. Det råder en viss osäkerhet kring vissa fall som exempelvis internetpubliceringar eller de situationer då man fysiskt bär med sig data till tredje land på en minnessticka.[46] EU-domstolens tidigare tolkning av artikel 25 i dataskyddsdirektivet vilket fortfarande är gällande klarlade att internetpubliceringar som utfördes av en person inom EU som kunde läsas över hela världen inte omfattades.[47] Vad som däremot anses vara en överföring enligt GDPR är filöverföringar från unionen till servrar i tredje land.[48] Personuppgiftsansvariga samt biträden som hanterar lagring av personuppgifter i molntjänster omfattar därmed av femte kapitlet om hela eller delar av data placeras i servrar i tredje land.

3.5.1 Adekvat skyddsnivå

En överföring till tredje land kan ske enligt artikel 45 dataskyddsförordningen utan något särskilt godkännande om kommissionen i en genomförandeakt har beslutat att det tredje landet erbjuder en adekvat skyddsnivå. Det är endast kommissionen till skillnad personuppgiftslagen, som får besluta om ett land har en adekvat skyddsnivå. Kommissionen bör med skyddet av de mänskliga rättigheterna som grund ta hänsyn till om det tredje landet respekterar rättsstatsprincipen, möjligheterna till rättslig prövning och internationella människorättsnormer. Kommissionen ska också beakta landets allmänna lagstiftning inklusive landets lagar om försvar, säkerhet, allmän ordning och straffrätt.[49] Vidare ska kommissionen enligt artikel 45 ta hänsyn till tredje landets lagstiftning kring vidarebefordran av personuppgifter till andra tredje länder, om det finns en oberoende tillsynsmyndighet och landets internationella åtaganden. Det tredje landet behöver inte uppfylla alla kriterier utan en helhetsbedömning ska göras utifrån de kriterier som förordningen stadgar.[50] Om en genomförande akt

[45] Sjöberg, Magnusson, *Rättsinformatik, Juridiken i det digitala informationssamhället*, s. 193, skäl 101 GDPR.

[46] Sjöberg, Magnusson, *Rättsinformatik, Juridiken i det digitala informationssamhället*, s. 195.

[47] EU-domstolens avgörande 2003-11-06 i mål C-101/01.

[48] Sjöberg, Magnusson, *EU:s dataskyddsförordning (EU) 2016/679, Kapitel V,* Lexino 2018-05-25".

[49] Skäl 104 GDPR.

[50] Voigt, m fl, *The EU General Data Protection Regulation (GDPR), A Practical Guide,* s. 117.

antas ska kommissionen enligt artikel 45.3 dataskyddsförordningen regelbundet kontrollera tredje landet, det bör ske minst vart fjärde år. Det ska också anges vilka myndigheter som är ansvariga för tillsynen och skulle inte landet längre uppfylla villkoren så ska genomförandeakten återkallas, ändras eller upphävas enligt artikel 45.5 GDPR. Några länder som kommissionen har godkänt är bland annat Argentina, Israel, Nya Zeeland och Schweiz.[51] Däremot är överföringen till USA villkorad genom att mottagaren har anslutit sig till Privacy Shield.

3.5.2 Överföring till tredje land utan en adekvat skyddsnivå

Det finns enligt dataskyddsförordningen andra tillåtna sätt att överföra personuppgifter till tredje land. Artikel 46 behandlar de fall då ingen adekvat skyddsnivå föreligger men där parterna emellan kan vidta lämpliga skyddsåtgärder för överföringen. Det innebär att företag kan använda sig utav standardklausuler som endast gäller parterna emellan. De ska enligt artikel 46.2 (c)(d) GDPR ha antagits av kommissionen eller en tillsynsmyndighet och därefter godkänts av kommissionen. Parterna får utan att inskränka standardklausulerna lägga till ytterligare skyddsåtgärder samt ändra i avtalet.[52]

Ett annat sätt att överföra personuppgifter till tredje land är genom bindande företagsbestämmelser. Dessa Binding Corporate Rules (BCR) tar sikte på koncerner samt företagsgrupper som deltar i en gemensam ekonomisk verksamhet.[53] Utöver dessa kan uppförandekoder godkända av en tillsynsmyndighet eller certifieringar ligga till grund för en överföring.

Skulle ett tredje land varken ha en adekvat skyddsnivå och inga lämpliga skyddsåtgärder finns tillhanda så kan en överföring ändå vara tillåten enligt artikel 49 GDPR. Det gäller då personen i fråga vars uppgifter behandlas uttryckligen har samtyckt till behandlingen. Artikel 49 reglerar även andra situationer som när det är nödvändigt för att ingå eller fullgöra ett avtal, försvara rättsliga anspråk eller i de fall det är nödvändigt för allmänintresset. Även andra undantag aktualiseras som när det görs från ett register eller de fall då en person inte kan samtycka men en behandling är nödvändig för att skydda den registrerades grundläggande intressen. Undantagen får däremot inte leda till att de grundläggande rättigheterna som dataskyddsförordningen erbjuder åsidosätts.[54] Om överföringen inte faller in under de nyssnämnda kriterierna så finns det en mer allmän bestämmelse i artikel 49.1 andra stycket GDPR som menar på att en överföring ändå är tillåten om den är nödvändig för

[51] European Commission, *Adequacy of the protection of personal data in non-EU countries,* https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_sv, hämtad 18/11-2018.

[52] Skäl 109 GDPR.

[53] Skäl 110 GDPR.

[54] EDPB, *Riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679 antagna den 25 maj 2018*, https://www.datainspektionen.se/globalassets/dokument/riktlinjer-om-undantag-enligt-artikel-49.pdf, hämtad 2018-11-18.

personuppgiftsansvariges tvingade ändamål och att den inte är repetitiv samt gäller ett begränsat antal registrerade.

De möjligheter till överföring som finns tillhanda ska tolkas restriktivt då ingen adekvat skyddsnivå föreligger. USA är ett av de länder som inte erbjuder en adekvat skyddsnivå. Det leder till att överföringen endast är tillåten om företaget är anslutet till Privacy Shield eller om något av undantagen i kapitel 5 GDPR aktualiseras. Personuppgiftsansvarige måste därför säkerställa att överföringen sker på en laglig grund.

4. Internationell rätt

De allmänt accepterade folkrättsliga jurisdiktionsprinciperna är viktiga då många länder håller sin lagstiftning inom principernas ramar. Ibland väljer vissa stater att göra avsteg från principerna vilket gör att de kan kränka andra länders suveränitet och skapa lagkonflikter. Det gäller i de fall det handlar om molntjänster då olika tolkningar finns avseende landets befogenheter att lagstifta på området. Är det landet där servrarna finns, där företaget är etablerat eller det land som har ett intresse av informationen. Det är inte lätt att avgöra, principerna blir därmed viktiga för att förstå på vilka grunder länder lagstiftar extraterritoriellt.

4.1 Folkrättens jurisdiktionsprinciper

De aktörer som är involverade i molntjänster som leverantörer och kunder kan inta rollen som, personuppgiftsansvarig och biträden. De blir då oftast skyldiga att följa olika staters lagar då flera stater samtidigt utövar jurisdiktion. Suveräna stater utövar makt genom lagstiftning, rättskipning och verkställande åtgärder i de situationer en handling har en viss anknytning till staten.[55] Den offentliga delen av folkrätten som reglerar förhållandet mellan stater har utvecklat några anknytningspunkter, vissa med större allmän acceptans än andra, som tar sikte på grunder där stater kan hävda att de har jurisdiktion i straffrättsliga situationer. Det handlar till största del om att avgränsa staternas maktutövning gentemot varandra.[56] När det gäller molntjänster så kan stater göra gällande jurisdiktion då tjänsten kan ha en anknytning till staten genom att servrarna är placerade i staten eller att företaget är etablerad i dess territorium. Det finns enligt Lotus-målet inget hinder mot att stater inom sitt eget territorium utövar jurisdiktion så länge det inte föreligger något folkrättsligt förbud mot det. [57] Däremot får inte verkställigheten ske på någon annan stats territorium av respekt till statens suveränitet.

4.1.1 Territorialitetsprincipen

Den första principen som stater kan bygga sin lagstiftning på är territorialitetsprincipen. Principen är indelad i en subjektiv samt en objektiv del som till viss mån har utvidgats. Principen tar sikte på händelser som sker inom en stats egna geografiska område. Den subjektiva avser de fall då ett brott påbörjats på en stats territorium medan det objektiva tar hänsyn till om brottet fullbordades där. Både EU samt Amerikansk rätt har i vissa situationer valt att utvidga den objektiva delen genom den så

[55] Bring, Ove, Mahmoudi, Said, Wrange, Pål*, Sverige och folkrätten*, Nordstedts Juridik 2014 s 100.

[56] Reuterswärd Reinhold, *Lagstiftningsmaktens folkrättsliga gränser*, SvJT 1977, s 1.

[57] SS Lotus (France v Turkey) (Judgement) PCIJ Rep Series A No 10 (1927).

kallade effektivitetsprincipen.[58] Jurisdiktion har då utövats på handlingar som har fått konsekvenser inom den staten, oavsett om handlingen har varit laglig i den stat där händelsen inträffa. Oavsett om en handling påbörjats eller avslutats i en stat så kan principen bli svårapplicerad på molntjänster. Information om var specifik data befinner sig är svårtillgänglig och lätt manipulerad genom att data enkelt kan byta plats.[59] Skulle platsen för data vara tillgänglig så finns det fortfarande olika uppfattningar och tolkningar om vad territorialitetsprincipen i stort innebär. Meningsskiljaktigheter aktualiserades i Microsoft fallet där USA hävdade att lagen inte applicerades extraterritoriellt då landet där företaget var etablerat var platsen där data befann sig. Microsoft menade däremot att servrarna rent fysiskt var placerade i Irland och därmed blir Irländsk lag tillämplig och amerikansk lag appliceras extraterritoriellt.

4.1.2 Nationalitetsprincipen

Den andra principen som arbetats fram tar sikte på personsambandet, den så kallade nationalitetsprincipen. Det finns, precis som territorialitetsprincipen, två grenar då principen kan åberopas. Den aktiva nationalitetsprincipen tar sikte på när statens medborgare är gärningsmän, det gäller oavsett var i världen brottet begås. Den passiva tar istället sikte på de situationer då statens egna medborgare är brottsoffer, det gäller i de fall personen blir utsatt av handlingar som sker av en annan stats medborgare utomlands.[60] Det kan handla om olika brott som krigsförbrytelser eller terrorism. Även företag kan omfattas av en stats jurisdiktion. Många amerikanska lagar omfattar amerikanska företag som är etablerade i USA. I vissa fall har lagstiftningen utvidgats till att omfatta företag som är ägda eller kontrollerade av amerikanska medborgare. Den vidsträckta tolkningen är dock inte godkänd internationellt. Skulle utvidgningen vara allmänt accepterad så skulle USA ha jurisdiktion över många företag utanför USA då de är kontrollerade eller ägda av amerikanska moderbolag eller medborgare. Det skulle då kränka andra staters suveränitet och lagstiftning och företag skulle inte veta vilket lands lagstiftning de ska prioritera.

Det har konstaterats att det finns olika principer som i stort är allmänt internationellt accepterade. Dock finns det utvidgningar som däremot inte får stöd rent internationellt. Ändå väljer vissa stater att basera sin lagstiftning på vitt tolkade principer. Frågan blir då hur andra stater ställer sig till den lagen samt hur det blir när det kommer till molntjänstleverantörer där meningarna kring principernas innebörd går isär. Slutsatser som kan dras är att folkrättsliga jurisdiktionsprinciper blir svårapplicerade när det kommer till den teknik som molntjänster omfattas av. Blir det staten där informationen kan göras tillgänglig eller staten där servrarna står. Kan det kanske vara där själva företaget är etablerat eller där det ägs av ett amerikanskt moderbolag eller medborgare. Det finns inga

[58] Bring, Ove, Mahmoudi, Said, Wrange, Pål, *Sverige och folkrätten*, s 103.

[59] Sjöberg, Magnusson, *Rättsinformatik, Juridiken i det digitala informationssamhället*, s. 45

[60] Bring, Ove, Mahmoudi, Said, Wrange, Pål, *Sverige och folkrätten*, s 103.

direkta svar och lagstiftningen ser olika ut både inom EU och USA. Det kommer att redogöras i de kommande avsnitten och analyseras samt jämföras vilka principer EU och USA baserar sin lag på.

4.2 De internationella ömsesidiga avtalen avseende rättshjälp

Ibland uppkommer det situationer där vissa länder anser att de har jurisdiktion och därmed kan göra myndighet eller domstolsbeslut gällande i andra länder. Dessa situationer regleras i artikel 48 i GDPR där det stadgas att överföring i och med sådana beslut inte är legitima om de inte uppfyller kraven i kapitel 5. Personuppgifter får överföras efter domstolsbeslut eller beslut från myndighet i de fall de grundar sig på en internationell överenskommelse så som ett avtal om ömsesidig rättslig hjälp mellan det tredje landet och EU alternativt med en medlemsstat. De avtal som avses är de som arbetats fram genom samarbete mellan olika länder för att inhämta och utbyta information om kriminella samt andra liknande situationer.[61] Företag kan inte enbart hänvisa till artikel 48 GDPR och ett ömsesidigt avtal för att på ett lagligt sätt överföra personuppgifter. Det måste också vara förenligt med övrig reglering kring tredjelandsöverföring i dataskyddsförordningen.[62] Det kan vara då utlämnandet är nödvändigt enligt artikel 49 GDPR med hänvisning till ett viktigt allmänintresse inom unionen eller nationell rätt.[63] Företag inom EU ska avvisa förfrågningar från tredje land och istället hänvisa till befintliga avtal.[64]

Det finns för tillfället tre befintliga avtal som Sverige är bundna av, dels de två avtalen mellan EU och USA som ingicks efter 11 septembers terrorattack mot USA samt det som Sverige har ingått med USA.[65] Syftet är att förbättra samarbetet med USA samt att tillhandahålla rättslig hjälp i vissa situationer. De uppställs en del formkrav gällande framställningen och staters rätt att villkora själva användandet av uppgifterna.[66] I artikel 9 i avtalet om ömsesidig rättslig hjälp mellan Europeiska unionen och Amerikas förenta stater begränsas användningen för att skydda personuppgifter. Där uppställs ett antal krav när den ansökande staten får använda bevismaterialet från den anmodade staten. Brottsutredningar, rättsliga förfaranden, förebygga ett överhängande eller allvarliga brott mot den allmänna säkerheten, rättsliga eller administrativa förfaranden som inte gäller brottmål men ändå

[61] European Commission, *Mutual legal assistance and axtradition,* https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en, hämtad 2018-11-20.

[62] Se Magnusson Sjöberg, *Artikel 48 Överföringar och utlämnanden som inte är tillåtna enligt unionsrätten,* Lexino 2018-09-03".

[63] Se skäl 115 GDPR.

[64] EDPB:s riktlinjer 2/2018 s. 5.

[65] Prop. 2004/05:46 s. 110-145.

[66] Prop. 2004/05:46 s. 129.

har någon koppling samt annat ändamål om informationen offentliggjorts eller samtycke har lämnats av den givande staten. Enligt 9.2(a) så får den givande staten ställa upp villkor som är nödvändiga, dock så får det enligt (b) inte vara fråga om allmänna begränsningar när de gäller ansökande statens rättsliga standarder för personuppgiftsbehandlingen. De avtalsslutande parterna var medvetna om att deras reglering kring behandlingen kunde se annorlunda ut, därför får det inte ensamt utgöra en grund för vägran att lämna ut uppgifter.[67] Dock så kan en stat efter en intresseavvägning där allmänintresset ställs mot skyddet av personuppgifter vägra lämna ut personuppgifter. En vägran får då ske med hänvisning till att det skulle kunna ge upphov till vissa grundläggande svårigheter i statens skydd av väsentliga intressen. En hänvisning till att landet i fråga inte uppställer en tillräckligt hög skyddsnivå får inte utgöra den enda anledningen till en vägran.

I de fall ett avtal inte har ingåtts blir reglerna om tredjelandsöverföring i kapitel 5 GDPR att utgå från. Skulle däremot en internationell överenskommelse finnas så kan enligt artikel 48 inte överenskommelsen självständigt ligga till grund för en tillåten överföring. Överföringen måste då, precis som i de fall ett avtal inte föreligger, ändå grunda sig på någon annan bestämmelse i kapitel 5. En fråga som uppkommer är då om avtalen underlättar inhämtningen då kapitel 5 ändå måste efterlevas med eller utan avtal.

En begäran om att få ut personuppgifter med hänvisning till de internationella avtalen kan vara krångliga då de är reglerade i detalj om hur en framställning ska ske. Kostnader och andra begränsningar måste också beaktas. De amerikanska domstolarna och organisationerna har riktat kritik mot de ömsesidiga avtalen då de anser att processen tar för lång tid.[68]

[67] Council of the European Union, *Handbook on the practical application of the EU-U.S. Mutual Legal Assistance and Extradition Agreements,*2011, s. 33, http://www.statewatch.org/news/2011/mar/eu-council-eu-usa-mla-handbook-8024-11.pdf, hämtad 2018-11-19.

[68] Report and Recommendations of the President's Review Group on Intellifence and Communication Technologies, *Liberty and security in a changing world,* 2013, s 227, https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf, hämtad 2018-11-20.

5. CLOUD Act

CLOUD Act grundar sig på redan befintlig amerikansk rätt vilket gör att amerikansk rätt samt Microsoft-målet som var en av anledningarna till antagandet av CLOUD Act måste utredas. Det krävs att läsaren förstår amerikansk rätt då även kommissionen i och med antagandet av Privacy Shield hänvisar till det konstitutionella skyddet samt de andra lagarna.

5.1 En inblick i USAs personuppgiftsreglering

Skyddet för behandlingen av personuppgifter regleras på federal och statlig nivå. Till skillnad från EU så finns det ingen generell federal lag som behandlar skyddet av personuppgifter i den privata sektorn. Däremot har en del stater som exempelvis Kalifornien valt att lagstifta på området.[69]

Trots avsaknaden av en generell lag så finns det vissa kategorier av personuppgifter som är reglerade på federal nivå. Det handlar om information som försäkringsföretag, banker, kreditgivare och andra inom den finansiella sektorn behandlar.[70] Lagstiftning finns också då vårdgivare handskas med uppgifter kring en persons hälsa och vissa e-post meddelanden som skickas med kommersiella syften.[71]

USA har, jämfört med EU, valt en annan metod då den privata marknaden i stort är självreglerad när det kommer till behandlingen av personuppgifter. Statliga myndigheter och olika företagsgrupper har utarbetat riktlinjer som företag kan välja att följa. Det sker genom att företagen utarbetar en policy som är förenlig med anvisningarna. Individerna ansvarar sedan för att de förstått och accepterat företagets policy innan de börjar använda deras tjänster. Skulle det visa sig att ett företag inte håller sig till det som står i policyn eller ändrar dessa utan ett godkännande så kan konsumenterna vända sig till den federala självständiga myndigheten, Federal Trade Commission (FTC). Myndigheten har som syfte att skydda konsumenterna. FTC kräver inte att företag har en policy, men de som har måste handla utifrån den. Skulle ett företag misslyckas med efterlevnaden eller skyddet för inhämtade uppgifter så kan FTC under sektion 5 i Federal Trade Commission Act ta ut en sanktionsavgift.

[69] Jolly, Ieuan, Loeb, Loeb, *Data protection in the United States: overview*, https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1, 2018, hämtad 2018-11-18.

[70] Se Gramm Leach- Biley Act 15 U.S.C § 6802 (a), The Fair Credit Act § 15 U.S.C. § 1618.

[71] Se Health information Portability and Accountability Act 42 U.S.C. § 1301, CAN-SPAM Act 15 U.S.C. § 7701-7713.

5.1.1 Konstitutionellt skydd för den personliga integriteten

Det finns ingen direkt uttryckligt konstitutionellt skydd för den personliga integriteten i USA. Det som behandlar liknande intrång i en fysisk miljö är det fjärde tillägget i den amerikanska konstitutionen som ratificerades på slutet av 1700-talet i samband med de andra nio tilläggen i the Bills of Rights. Regleringen tillhandahåller ett skydd för de enskildas privatliv gentemot staten genom att förhindra orättfärdiga intrång. Tillägget stadgar:

”Folkets rätt att vara säkra i sina personer, hus, dokument och ägodelar mot oskälig husrannsakan och gripande ska ej överträdas och inga rannsaknings- eller arresteringsorder ska utgå, utom på skälig grund […]”

Konstitutionen ska skydda individerna mot oskälig husrannsakan, gripanden och beslagtagning av egendom som utövas av statliga aktörer. Det får endast ske efter att utredaren visar att de har tillförlitlig information kring personen och att ett brott har eller kommer att äga rum.[72] Domaren ska därmed, om det är rimligt, medge sitt tillstånd för att minimera effekten av intrånget. För att undvika att utredaren söker i annat irrelevant material ska det i husrannsakningsordern specificeras vad som omfattas. Om inget tillstånd inhämtas ska all bevisning som tillhandahållits inte beaktas vid en rättegång.[73] Enskilda skyddas därmed gentemot genomsökningar då utredaren måste uppfyllda två krav, i första hand att få ut själva ordern och i andra hand att det är rimligt.

Det har diskuterats huruvida inhämtning av personuppgifter digitalt, utan någon fysiskt kontakt, också faller under fjärde tilläggets skydd. I målet Katz v. United States behandlades frågan om avlyssning av en misstänkt då samtal ägt rum via en offentlig telefonkiosk omfattades av fjärde tilläggets skydd. USAs högsta domstol fastslog år 1967 att tillägget tar sikte på personer och inte platser. Domaren John Marshall som höll med majoriteten utvecklade den så kallade ”rimliga förväntan” testet. Individer skyddas därmed av fjärde tillägget oavsett var de befinner sig om de har en subjektiv rimlig förväntan att det ska hållas privat samt att den rimliga förväntan rent objektivt är accepterad.[74] Högsta domstolarna i USA har sedan dess tillämpat testet genom att dela upp det i två steg.[75] Det tillämpades bland annat i fallet Smith v. Maryland då polisen inhämtade information om en

[72] Solove, Daniel, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, SSRN Electronic Journal, 2002, Brinegar v. United States, 338 U.S. 160 (1949).

[73] Solove, Daniel, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, (2002) SSRN Electronic Journal, 2002, s.1120.

[74] Katz v. United States, 389 U.S. 347 (1967) s. 361.

[75] Scolnik, Alexander, Protection for Electronic Communications: Stored Communications Act and the Fourth Amendment, 78 Fortdham L. Rev. 349 (2009) s. 353, https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4471&context=flr, hämtad 2018-11-22.

misstänkts telefonsamtal.[76] När rimlighetstestet diskuterades så kom majoriteten, fem mot tre domare, framtill att frivillig information som överlämnats till tredje part inte föll under det konstitutionella skyddet. De menade på att individer inte rimligen kan förvänta sig att information om de nummer man ringt inte ska hållas privat då telefonföretagen har den informationen. Tredje parts doktrinen etablerades och flera domstolar hänvisade till den då brottsbekämpande myndigheter ville begära ut information. Det frångicks under år 2018 då USAs högsta domstol i målet Carpenter v. United States då domstolen fastslog att individer, även då uppgifterna om var personen befinner sig genom mastrar som har gjorts tillgängliga för tredje part, ändå förväntar sig att det ska vara privat.[77] De uppgifter som inhämtades omfattades därmed av fjärde tilläggets skydd. USAs högsta domstol valde att öppna upp dörrarna för en större tolkning av vad som faller inom konstitutionens skydd. Dock är det fortfarande inte klarlagt vad som omfattas av det konstitutionella skyddet och inte.

5.1.1.2 The Electronic Communications Privacy act

I och med utvecklandet av tredjepartsdoktrinen och för att reglera de fall som föll utanför det konstitutionella skyddet för personlig integritet så antogs lagen om brevhemlighet (Electronic Communication Privacy Act- ECPA). Lagen består av tre delar, en av de tre är lagen om lagrade meddelanden (Stored Communication Act -SCA) som CLOUD Act bygger på. SCA reglerar under vilka villkor privata aktörer, som lagrar trådbunden och annan elektronisk kommunikation som e-post meddelanden, får tillhandahålla sådan information till andra privata aktörer eller statliga brottsutredande enheter.

I ECPA görs det, till skillnad från det konstitutionella skyddet, en åtskillnad på leverantörerna ”Electronic Communication Service” (ECS) och ”Remote Computing Service” (RCS). Skillnaden stadgas i 18. U.S.C. § 2510(12) och (14) där ECS tillhandahåller tjänster som medför att man kan skicka och ta emot elektronisk kommunikation medan RCS genom ett elektroniskt kommunikationssystem erbjuder tjänster som lagring och hantering. 18 U.S.C. § 2703 SCA uppställer krav för när en utredare kan få ut uppgifter. Skulle informationen som ECS tillhandahåller vara inom 180 dagar gammal så ska utredaren först ansöka om en rannsakningsorder hos en domare. Skulle det däremot vara information som är äldre än 180 dagar eller lagrad i RCS så krävs det ingen order utan det räcker med att det är skäligt. Data får då inhämtas genom ett administrativt föreläggande eller via ett domstolsbeslut. Det räcker då med att en utredare inför en domstol gör gällande att det på sannolika skäl finns uppgifter som är relevanta för en pågående brottsutredning. Kravet är lägre ställt än det konstitutionella skyddet vilket medför att fysiska intrång i en persons egendom där uppgifter samlas in anses vara mer skyddsvärt än de som lagras elektroniskt.

[76] Smith v. Maryland, 442 U.S. 735, 743 (1979).

[77] Carpenter v. United States, 484 U.S. 19 (1987).

Huruvida SCA strider mot konstitutionen genom att tillåta ett lägre skydd för information lagrad under en längre tid är omdiskuterat.[78] Fjärde tillägget som skrevs i slutet av 1700-talet kan omöjligen ha förutsett framtiden och den digitala utvecklingen som skett. Det skulle i dagens samhälle vara orimligt att argumentera för att lika integritetskränkande intrång skulle behandlas annorlunda beroende på om det förvarades fysiskt eller digitalt. Inte heller är det längre hållbart att fortsätta applicera tredje parts doktrinen då majoriteten av människors vardag är integrerad med den digitala världen.

5.2 Microsoft vs USA

Teknikens utveckling och molntjänsternas funktioner att lagra data på olika servrar som kan vara placerade i olika delar i världen har lett till en viss del problematik. En fråga som uppkommer är vilket land som ska anses ha ‚jurisdiktion över data när data är placerad på datorhallar i ett land men kan kommas åt på datorskärmar i ett annat land. Frågan aktualiserades i fallet mellan företaget Microsoft Corporation och Amerikanska staten.

5.2.1 Bakgrund

Företaget Microsoft Corporation som är baserad i Washington har sedan flera år tillbaka erbjudit kostnadsfria internetbaserade e-mail tjänster. De kunder som har ett e-mail konto kan skicka och ta emot e-mail som lagrats på en publik molntjänst. I samband med att en användare uppger information om var han eller hon bor så kommer det på grund av nätverkets latens att lagras i de datorhallar som finns närmast det land användaren anger. Efter att överföringen är klar så raderas all data, förutom icke informativ data, från de Amerikanska servrarna. Icke informativ data består av grundläggande information kring kontot som exempelvis e-postrubriker utan ämnesrad.[79]

Microsoft fallet handlade i grunden om en förundersökning kring ett fall om narkotika smuggling. Den Amerikanska staten hade genom en rannsakningsorder som en domare i U.S District Court of the Southern District of New York hade utgett, försökt få ut data som förvarades på servrar i Irland. Tillståndet utgavs med hänvisning till 18 U.S.C. §§ 2703 SCA, vilket gav order till Microsoft att utlämna både informativ och icke informativ data. Microsoft vägrade med hänvisning till att den amerikanska lagen inte kunde sträcka sig till att omfatta data som var lagrad i Irland.

[78] Scolnik, Alexander, Protection for Electronic Communications: Stored Communications Act and the Fourth Amendment, 78 Fortdham L. Rev. 349 (2009) s. 383. Tillgänglig på:

[79] 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, bilaga VII s 2, (Privacy Shield)

5.2.2 U.S District Court of the Southern District of New York

Microsoft överklagade till United States District Court of New York och hävdade att de skulle ogilla rannsakningsordern som domaren hade utgett. Microsoft menade på att de kunde utge endast icke informativ data medan data som var lagrad utanför USA inte föll inom SCAs tillämpningsområde. Det skulle enligt Microsoft vara en extraterritoriell utövning av lagen. Microsofts begäran att ogilla rannsakningsordern nekades av en federal domare då, precis som den amerikanska staten argumenterade, att en order i SCA var likt en administrativt föreläggande. Det innebar att även elektroniskt lagrat material ska tillhandahållas domstolen. Domaren hänvisade till tidigare praxis på området där företag i samband med en stämning har varit tvungna att utge all information som varit i deras vårdnad eller kontroll, även det som funnits utanför USAs gränser. Domaren menade på att kongressens avsikt var platsen där informationen kunde göras tillgänglig och inte stället där det förvarades.[80]

Microsoft krävde att en överdomare skulle ompröva fallet. Domaren stod fast vid ordern och höll Microsoft ansvariga för domstolstrots då de vägrade anpassa sig. Microsoft valde därmed att överklaga domen till U.S Court of Appeals for the Second Circuit.

5.2.3 U.S Court of Appeals for the Second Circuit

Domstolen som bestod av tre domare upphävde den tidigare domen. Domstolen började med att hänvisa till Morrision fallet där Supreme Court of the United States fastslagit att finns en presumtion mot att applicera lagar extraterritoriellt. Domstolen ansåg att SCA inte reglerade hur långt lagen sträckte sig, därmed skulle en tvåstegsprövning göras för att se om lagen ska appliceras extraterritoriellt.

Det första steget var att se om Kongressen, när lagen antogs, ville att rannsakningsordern skulle nå utanför USA. Det måste enligt Morrisson fallet finnas en klar indikation på att det ska appliceras extraterritoriellt.[81] Domstolen gjorde en bokstavstolkning av hur en order tillkommer enligt SCA. Enligt § 2703 (a), (b)(1)(a) ska en order utges av en statlig domstol under samma villkor som Federal Rules of Criminal Procedur utger. Domstolen kom fram till att varken SCA eller Federal Rules of Criminal Procedur benämner något om en extraterritoriell tillämpning. Domstolen avstod från argumentationen att en order enligt SCA skulle vara en blandning mellan en order och ett föreläggande då dessa termer i sektion 2703 stadgas separat från varandra.[82] Vidare menade domstolen på att ett föreläggande om att ett företag ska tillhandahålla kommunikation lagrad utanför USA endast gäller information om det mottagande företaget och inte dess kunder. Domstolen

[80] United States v. Microsoft Corp., F.Supp. 3d 466 (S.D.N.Y. 2014), s 473.
[81] Morrison v. National Australia Bank Ltd., 561 U.S. 247 (2010), s. 5-12.
[82] Microsoft vs US., 892 F.3d 197 (2nd Cir. 2016), s. 18.

påpekade att Microsoft lagrar data åt andra personer vilka har ett intresse av att informationen är skyddad. SCA kan därmed inte tillämpas extraterritoriellt.

Det andra steget var att undersöka om lagens fokus skulle leda till en extraterritoriell tillämpning. Skulle lagen tar sikte på händelser som sker i USA även fast det utspelar sig utanför territoriet så har det en inhemsk tillämpning av lagen fast med extraterritoriella konsekvenser. Domstolen började med en bokstavstolkning och kom fram till att lagen fokuserar på att rent processuellt skydda personers privatliv mot intrång. Intrång får endast ske under vissa villkor stadgade i U.S.C § 2703. Även om lagen tar sikte på hur staten ska få ut information så är det syftet sekundärt jämfört med skyddet för privatliv. Förvaltningen skulle ske utanför USA, oavsett var personen ifråga befinner sig och oavsett om företaget är baserat i USA. Domstolen menade därmed på att en amerikansk domstol inte genom en order kan tvinga Amerikansk baserade tjänsteleverantörer att utge informativ data kring en kunds elektroniska kommunikation som är lagrat på servrar utanför USA.

Den amerikanska staten ansökte därmed om att domstolen skulle höra fallet på nytt vilket blev avslaget i januari 2017 med 4 av 8 röster. Den amerikanska staten valde därmed att överklaga fallet till the Supreme Court of the United States i juni 2017.

5.2.4 The Supreme Court of the United States

Den amerikanska staten ansåg att den tidigare domstolen tolkat SCA felaktigt och att lagen inte behövdes tillämpas extraterritoriellt då Microsoft skulle utge information som de hade kontroll över. Staten argumenterade för att Second Circuits tolkning inte skulle funka i praktiken samt hindra förundersökningar då det inte finns något processuellt tvångsmedel för att framtvinga information. EU-kommissionen inkom i fallet med ett utlåtande där de inte tog någon av parternas ståndpunkt. Kommissionen ansåg däremot att internationell rätt och territorialitetsprincipen blev involverat i fall där företaget är beläget på en plats och servarna i ett annat. Kommissionen hävdade att domstolen måste ta hänsyn till andra suveräna länders lagar och intressen för att undvika konflikter avseende jurisdiktion. Vidare så hänvisade kommissionen till artikel 48 dataskyddsförordningen där det stadgar att utländska domar i sig inte utgör en laglig överföring. Det måste grunda sig på ömsesidiga internationella överenskommelser samt någon annan laglig grund i det kapitlet. Kommissionen citerade skäl 115 GDPR där det står att en extraterritoriell tillämpning av lagar kan, förutom att strida mot internationell rätt, skada skyddet av fysiska personer som säkerställs inom unionen.[83]

The Supreme Court valde att pröva fallet i oktober 2018, dock så hade en ny lag redan i mars 2018 antagits av Kongressen och skrivits under av Presidenten. Lagen, The Clarifying Lawful Overseas Use of Data Act, valde att bygga på samt ändra vissa delar i den tidigare föråldrade SCA. Lagen stadgar i 18 U.S.C. § 2713, som ett tillägg i SCA, att elektroniska kommunikationstjänstleverantörer ska utge data som de innehar, vårdar eller kontrollerar oavsett om data finns på servrar i eller utanför

[83] The European Commission, *In the Supreme Court of the United States in the matter of a warrant to search a certain E-mail account controlled and maintained by Microsoft Corporation*, s. 13.

USA. Den amerikanska staten begärde efter att lagen antogs en ny fullmakt och Microsoft valde att rätta sig efter fullmakten. The Supreme Court uttalade att det inte längre fanns något fall eftersom parterna var överens, domstolen skickade därmed tillbaka fallet till de lägre domstolarna med instruktioner om att det skulle frångå sina tidigare domslut.

5.2.5 Uppmaning till en ny lag

I och med att lagen antogs så prövades aldrig den problematik som uppstod kring den extra territoriella tillämpningen av lagen. Redan efter att fallet behandlats av the Second Circuit så uppmanade en av domarna i domen, Gerard E. Lynch, den lagstiftande makten till att modernisera området genom att reglera det. Domaren höll med majoriteten men påpekade att ingen lag hindrade Kongressen till att lagstifta på området när det gäller Amerikanska eller utländska subjekt utanför USA. Enligt Lynch så kunde inte kongressen år 1986 när SCA antogs ha förutsett teknologin bakom molntjänster. Domaren ansåg att domen skulle medföra att utländska kunder samt de amerikaner som falskeligen klickar i att de bor utomlands skulle komma att omfattas av ett absolut skydd. Amerikanska staten skulle därmed vara förhindrad till att ta in information, även i de fall det handlar om terrorism. Enligt Lynch var det därmed viktigt att avgöra om kunden var en amerikansk person eller inte.

Liknande resonemang anfördes av José Cabranes, en av domarna i U.S District Court of the Southern District of New York, som röstade för en omprövning. Han menade på att domen brände statens lagfulla framtvingande av information och istället skapat en karta som främjade kriminella aktiviteter. Han ansåg att domen hindrade den nationella säkerheten i USA.[84]

Andra har varit kritiska gentemot fallet och ansett att Second Circuit rent tekniskt inte har tagit hänsyn till att data kan vara icke territoriellt och istället sett det som ett fysiskt objekt.[85] De frågor som kan uppstå kring Second Circuit domen är vad som händer om data delvis är placerad på servar i ett land och resterande i andra länder. Eller vad händer om man beslagtar någons telefon och information är lagrad på molntjänster som kanske använder sig av servrar placerade i andra länder. Kongressen såg problemet med åtkomst åt data i dessa situationer och antog därmed CLOUD Act för att reglera luckorna i lagen som SCA medför.

5.3 CLOUD Acts rannsakningsorder oavsett var data befinner sig

Kongressen valde att uppdatera SCA efter att luckorna i lagen och det problem det medförde uppmärksammades i Microsoft fallet. Lagen röstades igenom den 23 mars i samband med den 2232

[84] Microsoft Corp. v. United States, No. 14-2985 (2d Cir. 2017) s. 2-3.

[85] Privacy- Stored Communications Act- Second Circuit Holds that the Government Cannot Compel an Internet Service Provider to Produce Information Stored Overseas- Microsoft Corp. v. United States, 829 F .3d 197 (2d Cir.2016) [130 Harv .L. Rev. 769] s. 774.

sidor långa Omnius Spending Bill. Syftet med lagen är enligt sektion 102 att skydda den allmänna säkerheten och bekämpa allvarliga brott vilket inkluderar terrorism. Kongressen ansåg att den amerikanska staten hindrades från att upprätthålla säkerheten då de inte kunnat komma åt data som är lagrad utanför USA.[86] Detta trots att data är i besittning, vårdnad eller kontroll av amerikanska tjänsteleverantörer av kommunikation som USA har jurisdiktion över. Ändamålet med lagen är att den amerikanska staten, genom de bestämmelser som finns i SCA, ska kunna få tillgång till data som hålls av leverantörer av kommunikationstjänster som omfattas av amerikansk jurisdiktion. Kongressen valde att i kapitel 121 av titel 18 U.S.C. lägga till § 2713 som stadgar:

”En leverantör av elektronisk kommunikationstjänst eller fjärrdators tjänster ska uppfylla de förpliktelser som kapitlet stadgar för att bevara, säkerhetskopiera eller avslöja innehållet i en tråd eller elektronisk kommunikations och annat register eller annan information som gäller en kund eller abonnent inom en sådan leverantörs besittning, vårdnad eller kontroll, oavsett om sådan kommunikation, register eller annan information är lokaliserad inom eller utanför USA.”[87]

Den tillagda sektionen utökar SCAs territoriella tillämpning rent geografiskt genom att även inkludera information som finns lagrad utanför USA. Själva subjektet som lagen tar sikte på står oförändrat. De som omfattas är som tidigare behandlat elektroniska kommunikationstjänster som definieras i 18 U.S.C. § 2510(15) och fjärrdatorstjänster i 18 U.S.C. § 2711. CLOUD Act ändrar inte heller vilken typ av data som omfattas. Förutom självaste innehållet i elektronisk kommunikation och lagring som definieras i 14 U.S.C. § 2510(8) så innefattar stadgandet också icke informativ data. Då är det inte själva kommunikationen som går att utläsa utan annan information kring själva kontot.[88] Processen att få ut information, som tidigare behandlats, är också densamma. Däremot har andra processuella regler tillkommit i och med CLOUD Act där kommunikations tjänsteleverantörer kan kräva att rannsakningsordern ogillas.

5.3.1 Tjänsteleverantörers möjlighet att invända

Det görs en åtskillnad mellan en rannsakningsorder samt en administrativt föreläggande. De behandlar data olika beroende på datum samt har olika krav som måste vara uppfyllda innan en domstol medger en sådan ansökan. Skillnaden är dock nödvändig då en ansökan om en order ställer högre krav eftersom det handlar om nyare kommunikation som skett inom 180 dagar medan äldre data kan utkrävas genom ett föreläggande. En annan distinktion mellan dessa var att föreläggande, tillskillnad

[86] Section 102 (2) CLOUD Act.

[87] Se U.S.C. § 2713, den engelska versionen lyder: *A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.".*

från en order, processuellt kunde utmanas innan de skulle verkställas. Det enda sättet att utmana en rannsakningsorder var att inte rätta sig efter den och därmed riskera att bli dömd för domstolstrots. CLOUD Act introducerade en lösning på problemet genom att införliva nya processuella regler kring när och vilka orsaker som får ligga till grund för en talan om att ogilla en order. Den första grunden i 18 U.S.C. § 2703(h)(1)(A) handlar om att kunden eller abonnenten inte är en amerikansk person och inte bor i USA medan den andra grunden tar sikte på eventuella lagkonflikter som kan uppstå. De måste båda vara uppfyllda för att domstolen ska kunna ogilla en fullmakt.

Det första stadgandet tar sikte på om personen ifråga som informationen gäller är en amerikansk person, alternativt bor i USA. I 18 U.S.C. § 2523(a)(2) definieras en ”United States person” som en medborgare eller en person som har amerikansk nationalitet eller en utländsk person som lagligen uppehåller sig i USA. Likaså faller företag som är inkorporerade i USA eller inte inkorporerade, men har många medlemmar som är amerikanska medborgare eller utländska med amerikanska uppehållstillstånd inom definitionen. En leverantör av kommunikation eller lagring kan därmed göra invändningar om det skulle handla om personuppgifter kring en svensk medborgare som lagras på servrar antingen inom eller utom USAs gränser. Precis som Lynch uppmärksammade för egen del i Microsoft målet så skulle nog den irländska staten och EU inkomma med klagomål om den Amerikanska staten ville få ut information kring en medborgare i Irland.[89] Däremot menar Lynch på att fallet skulle se annorlunda ut, vilket han hoppades att Irland och EU håller med om, ifall det skulle handla om en Amerikan. Lynch tog särskilt sikte på de situationer då amerikaner felaktigt påstått att de bor utanför EU för att undkomma den amerikanska lagen.[90] Trots att en leverantör som omfattas av lagen kan invända så betyder det inte leverantören alltid gör det. CLOUD Act lämnar inget utrymme för enskilda att överklaga ett sådant beslut utan de får förlita sig på att leverantören gör det. Den enskilde kanske inte är medveten om att en insamling efterfrågats då inget besked om att information utlämnats inom en viss tid ges till den enskilde enligt SCA 18 U.S.C. § 2703(b)(1)(A). Det leder till att information kan samlas in utan att EU-medborgaren är medveten om det eller kan invända.

Den omständigheten att det handlar om en Amerikansk person utgör inte i sig självt en anledning till att ogilla ordern. Det andra kravet är att problem kan uppstå då andra länders lagar blir tillämpliga. Den problematiken uppmärksammas redan i inledningen i sektion 102(5). De leverantörer som erbjuder kommunikationstjänster kan hamna i kläm då lagarna står i konflikt med varandra, USA kan kräva att få ut data samtidigt som det andra landet förbjuder en överföring. Enligt § 2703 (h)(2)(A)(ii) kan en sådan anledning, att leverantören bryter mot lagen i ett annat land, läggas till grund för att en domstol ska ogilla en fullmakt. Det får dock inte ske på någon annan grund än den verkliga lagkonflikten med en kvalificerad stats lagar. Det ska dock påpekas att det är domstolen som avgör om en order ska ogillas. Det faktum att det strider mot ett annat lands lagar kan för domstolen väga

[89] Microsoft Corp. v. United States, No. 14-2985 (2d Cir. 2017) s. 2-3, s. 230.

[90] Microsoft Corp. v. United States, No. 14-2985 (2d Cir. 2017) s. 2-3, s. 230.

mindre än den kriminella aktiviteten som ska utredas. Domstolen måste därför göra en analys för att bedöma om den grunden leverantören åberopar väger tyngre eller inte.

5.3.2 Domstolens analys

En ansökan om att domstolen ska ogilla en rannsakningsorder måste ha skickats inom 14 dagar efter att leverantören fått del av ordern oavsett vilken utav dessa två grunder som åberopas, 18 U.S.C. § 2703(h)(2). Domstolen får enligt U.S.C. § 2703 (h)(2)(B) ändra eller ogilla ordern om domstolen finner att avslöjandet av information skulle leda till att leverantören bryter mot lagen i ett kvalificerat land. En helhetsbedömning ska göras där intresset för rättvisa ska beaktas och beroende på omständigheterna får beslutet ändras eller upphävas. Domstolen ska då också beakta om personen ifråga som informationen gäller är en amerikansk person eller annars bor i USA.

Vid helhetsbedömningen enligt 18 U.S.C. § 2703 (h)(2)(B)(ii) ska domstolen inväga några faktorer som § 2703 (h)(3) uppräknar. Domstolen ska i enlighet med § 2703 (h)(3)(B) beakta intresset som USA har av rannsakningsordern och den utredande statliga enhetens intresse av avslöjandet. Likaså ska även det andra landets intresse av att förhindra att ett avslöjande äger rum enligt § 2703 (h)(3)(B) inbegripas i analysen. Det innefattar också att utreda de legala påföljder en leverantör eller anställda hos leverantören kan utsättas för vid ett avslöjande, § 2703(h)(3)(D). De första punkterna börjar därmed med att analysera USAs, det andra landet och de lagliga kraven en leverantör är belastad med. Enligt § 2703(h)(2)(B)(i) ska även nationaliteten och var kunden befinner sig vägas in, dock endast om information finns att tillgå. Det inbegriper en analys av kundens koppling till USA och skulle information begäras av en annan stat så är det relationen med den staten som ska granskas. Även leverantörens kopplingar till och närvaro i USA ska undersökas samt hur viktigt det är för förundersökningen att informationen kommer fram, § 2703(h)(2)(A)(iii). Skulle det vara en utländsk myndighet som söker information så ska den myndighetens utredningsintresse vägas in i bedömningen. Slutligen ska domstolen kontrollera ifall det finns andra effektivare sätt att tillgå information för att förhindra negativa konsekvenser. Innan en domstol tar ett beslut eller efter en överklagan inkommit så är inte leverantören skyldig att utge någon information utan det ska bevaras tills målet är avgjort, 18 U.S.C. § 2703(h)(4). Domstolen får dock enligt samma bestämmelse omedelbart kräva ut information om någon av de situationerna uppräknade i § 2705(a)(2) skulle bli aktuella. Det handlar om att förhindra situationer där individers liv eller hälsa är i fara eller att misstänkta försöker fly från åtal, förstöra bevisning, hota vittnen eller på annat sätt skada en utredning.

Domstolen ska i sin helhetsbedömning ta hänsyn till alla de uppräknade faktorerna. USAs och utländska länders intresse ska tas med i analysen samt även andra lagar som kan stå i konflikt med den amerikanska. Med detta sagt så finns det dock inte garantier på att de amerikanska domstolarna då en lagkonflikt uppstått kommer att ogilla rannsakningsordern då utredningsintresset kan spela en viktigare roll. Utan någon närmare analys så kommer dataskyddsförordningens artikel 48 som

uttryckligen hänvisar till de ömsesidiga rättsliga avtalen, då domar inte kan ligga till grund för en överföring, att stå i strid med CLOUD Act.

5.3.3 Exekutiva avtal med utländska länder om tillgång till data

Kongressen fokuserar förutom på den amerikanska statens intresse även på andra staters intresse av att motarbeta allvarlig kriminalitet. Sektion 104 i CLOUD Act ändrar i 18 U.S.C. kapitel 119 genom att i slutet av § 2511(2)(a) lägga till att det inte ska vara olagligt för publika elektronisk kommunikationstjänst leverantör eller fjärrdatorstjänster att utge information kring trådbunden eller elektronisk kommunikation till en utländsk stat. Det får utlämnas i samband med en utländsk order av ett land som justitiekanslern har ett exekutivt avtal med och som har uppfyllt villkoren i § 2523 och därmed certifierats till kongressen. De villkoren som är uppställda i § 2523 (b) kräver att landet ifråga uppställer ett skydd för den personliga integriteteten och respekterar mänskliga rättigheter. I § 2523 (b)(1) ska bland annat den inhemska lagen i det begärande landet ha ett robust materiellt och processuellt skydd för integritet och medborgerliga friheter i samband med datainsamlingen.

Det begärande landet måste också tillämpa mänskliga rättigheter där en rättvis rättegång, rätten att uttrycka sig och förbudet med tortyr samt andra rättigheter räknas upp. Uppfyller ett land alla dessa krav så kommer ett exekutivt avtal ingås vilket leder till att även utländska stater kan komma åt data. Dock så ställer 18 U.S.C. § 2523(4) upp ett antal krav för behandlingen där den utländska staten inte medvetet får sikta sig in på en Amerikansk person eller en person som bor i USA. Inte heller icke-amerikanska personer som bor utanför USA om själva syftet är att få ut information om ett amerikanskt subjekt eller en person som bor där. En order från utlandet att kräva ut information får endast ske i det syfte att införskaffa information för att förhindra, utreda, lagföra, upptäcka allvarligare brott som inkluderar terrorism.

Skulle justitiekanslern och utrikesministern måste vara eniga om att ett land uppfyller dessa villkor så kan ett avtal ingås. Kongressen behöver inte godkänna avtalet för att det ska träda i kraft men kan göra invändningar om de skulle krävas. En domstol kan inte granska lagenligheten av avtalet i sig utan domarna får endast beakta om ordern att lämna ut data står i förenlighet med SCAs uppställda krav, § 2523(c). Det finns därmed ingen möjlighet för leverantörer av elektronisk kommunikation eller enskilda kunder att göra en invändning mot ett avtal med ett land de anser inte uppfyller alla villkor.

6. EU-US Privacy Shield

6.1 Inledning

EU och USA är stora aktörer på marknaden och överföring av data från EU till USA måste kunna ske utan att den personliga integriteten kränks. Den rätt till privatliv som artikel 8 EKMR och artiklarna 7 och 8 i stadgan reglerar till EU-invånares fördel måste upprätthållas även i de fall då personuppgifter lämnar EU:s territorium. Likaså måste stadgans artikel 47 upprätthållas där de enskilda har rätt till ett effektivt domstolsskydd för att tillvarata sina rättigheter.[91] Kommissionen kan enligt artikel 45 GDPR besluta att ett land uppfyller villkoren för att klassificeras som ett land med adekvat skyddsnivå. Bland annat ska relevant lagstiftning i landet beaktas, ifall det finns en oberoende tillsynsmyndighet, dataskyddsregler samt granska reglerna för vidare överföring. Som tidigare behandlats har inte USA på det federala planet ett lika starkt generellt skydd för behandling av personuppgifter. Endast vissa kategorier och vissa situationer är reglerade genom lag medan privatpersoner annars hänvisas till företagens policy. Det krävs inte att ett land erbjuder en skyddsnivå av grundläggande fri-och rättigheter som är identisk med den som garanteras inom EU. Det räcker med att nivån är väsentligen likvärdig den som finns inom EU.[92]

6.2 Föregångaren Safe Harbors ogiltighet

USA erbjöd vid dataskyddsdirektivets antagande inte en adekvat skyddsnivå, beslutet Safe Harbor arbetades då fram mellan EU och USA.[93] Amerikanska företag kunde därmed ansluta sig till beslutet och ta emot personuppgifter från EU då landet i sig inte hade en tillräckligt hög skyddsnivå.

I och med Edward Snowdens avslöjande om de amerikanska underrättelsetjänsternas övervakning, mer specifikt på den verksamhet som National Security Agencys (NSA) bedrev, ledde till att organisationer och enskilda blev mer uppmärksamma och måna om den personliga integriteten. NSAs granskning var inte olaglig då den baserade sig på The Patriot Act som tillkom efter den 11 september 2011 som gav brottsbekämpande myndigheter en möjlighet att vid terrorbrott använda samma processuella regler som vid annan brottslighet.[94]

---

[91] Privacy Shield, skäl 124.

[92] Mål C-362/14 Maximillian Schrems mot Data Protection Commissioner, p. 73.

[93] Kommissionens beslut av den 26 juli 2000 enligt Europaparlamentet och rådets direktiv 95/46/EG 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.

[94] Department of Justice, *The USA PATRIOT Act: Perserving Life and Liberty (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism),* https://www.justice.gov/archive/ll/highlights.htm, hämtad 2018-11-24.

Maximilian Schrems en österrikisk medborgare gjorde en anmälan till ombudsmannen i Irland där han krävde att ombudsmannen skulle förbjuda Facebook Irland från att överföra personuppgifter till USA. Alla EU-medborgare som var Facebook användare var tvungna att ingå ett avtal med Facebook Irland där de accepterade att deras personuppgifter helt eller delvis skulle överföras till moderbolaget Facebook Incs servrar i USA. Schrems begäran avslogs av ombudsmannen med motiveringen att Facebook var anslutet till Safe Harbor vilket kommissionen beslutat uppfyller en adekvat skyddsnivå. Ombudsmannen var därmed inte tvungen att utreda lagenligheten av överföringen till tredje land. Schrems överklagade till High Court som skickade frågan vidare till EU-domstolen som tog upp fallet. EU-domstolen behandlade inte endast High Courts frågor kring ombudsmannens befogenheter utan valde att ogiltigförklara Safe Harbor beslutet i sin helhet. EU-domstolen ansåg att beslutet inte levde upp till det skydd för privatliv och personuppgifter som reglerades i artikel 7 och 8 rättighetsstadgan.

Domstolen började med att klargöra ombudsmannens befogenheter vilket följande avsnitt inte kommer att behandla. Domstolen granskade därefter artikel 1 i Safe Harbor och vad som avsågs med begreppet adekvat skyddsnivå som varken definierades i artikel 25.2 dataskyddsdirektivet eller någon annan bestämmelse. Domstolen kom fram till att en adekvat skyddsnivå inte kräver att tredje landet har en skyddsnivå identisk med EU, men det krävs i vart fall att tredjelandet erbjuder ett skydd som är väsentligen likvärdig med det skydd som garanteras inom EU.[95] Vidare konstaterade domstolen att ett företag ansluten till Safe Harbor var tvungna att följa amerikansk lag om de skulle stå i strid med principerna. Ett särskilt undantag reglerades i bilaga I fjärde stycket Safe Harbor där principerna fick ge vika för de krav som gällde den nationella säkerheten, allmänintresset eller rättsefterlevnaden.[96] Safe Harbor hänvisade inte heller till amerikanska lagar vilket kunde begränsa användningen då undantaget var av generell beskaffenhet.[97] Domstolen hänvisade därefter till kommissionens granskning av Safe Harbor där samma problematik uppmärksammades. Kommissionen ansåg att de amerikanska myndigheterna kunde erhålla och behandla personuppgifter som gick strängt över vad som var nödvändigt och proportionerligt för att skydda den nationella säkerheten.[98] En lagstiftning som tillåter generell åtkomst till innehållet i elektroniska kommunikationer ansågs enligt domstolen kränka rätten till privatliv. Det fanns inte heller någon möjlighet för de enskilda att använda effektiva rättsmedel för att gå tillgång till, rätta eller radera uppgifter som kränkte deras rätt till privatliv vilket garanteras av artikel 47 rättighetsstadgan.[99] Artikel 1 var därmed enligt EU-domstolen inte förenlig med kravet på en adekvat skyddsnivå som artikel 25.6 direktiv 95/46 kräver.

Slutligen påpekade domstolen att artikel 3 i beslutet varvid en tillsynsmyndighet fick begränsa överföringen till USA stred mot kommissionens befogenhet som stadgades i artikel 25.6 direktivet.

[95] Mål C-362/14, p. 74.
[96] Mål C-362/14, p. 84.
[97] Mål C-362/14, p. 87.
[98] Mål C-362/14, p. 90.
[99] Mål C-362/14, p. 90.

Då artiklarna 1 och 3 i beslut 2000/520 inte kunde avskiljas från de andra två artiklarna valde EU-domstolen att underkänna beslutet i sin helhet.

6.3 Privacy Shield den nya lösningen

I samband med att Safe Harbor avtalet ogiltigförklarades, utarbetade EU och USA ett nytt avtal, med beaktande av de synpunkter EU-domstolen hade på avtalet. I juli 2016 beslutade EU-kommissionen att godkänna Privacy Shield avtalet vilket började tillämpas redan i augusti 2016. Trots att beslutet grundade sig på det tidigare dataskyddsdirektivet 95/46/EG så är det fortfarande giltigt enligt artikel 45.9 dataskyddsförordningen. Precis som Safe Harbor så bygger Privacy Shield ett självcertifierings system där amerikanska företag kan välja att ansluta sig.[100] Företagen förbinder sig då att följa principer om integritetsskydd samt andra kompletterande principer. De har utfärdats av USAs handelsministerium som ansvarig för hanteringen av avtalet och övervakningen av att anslutna företag följer principerna.[101] Principerna, som måste implementeras i deras policy, blir enligt skäl 17 Privacy Shield omedelbart tillämpliga med vissa undantag då företag redan har existerande kommersiella förbindelser med tredjeparter.

6.3.1 Privacy Shields principer

Företagen förbinder sig att efterleva de principer som avtalet stället upp. Dessa principer hade redan utarbetats i och med antagandet av Safe Harbor men har efter EU-domstolens dom förbättrats. Den första principen tar sikte på meddelande då företag ska utlämna information kring dess personuppgiftsbehandling. Tidigare så krävdes det enligt Safe Harbor endast att företag lämnade övergripande information kring behandlingen av personuppgifter.[102] I och med Privacy Shield införande så ska mer detaljerad och specifik information kring behandlingen lämnas. Det kan enligt skäl 20 Privacy Shield handla om vilken typ av uppgifter som samlas in, ändamålet, åtkomst och valmöjlighet, ansvarsskyldighet samt förutsättningar för att föra uppgifterna vidare. Den andra principen om dataintegritet och ändamålsbegränsning omöjliggör för företag att samla in uppgifter baserat på ett falskt syfte. Ändamålen måste vara tillförlitliga, riktiga och stämma överens med det syfte företaget hade från början för att förhindra att det samlas in för ett ändamål som sedan ändras. Skulle det ändras så ger den tredje principen om valmöjlighet den registrerade rätten att invända. Skulle det däremot handla om känsliga personuppgifter så krävs det ett uttryckligt samtycke.[103]

Personlig information som lagras så personen ifråga kan identifieras får endast, enligt principen om dataintegritet och ändamålsbegränsning i skäl 23, behandlas så länge det tjänar de ändamål för vilket

[100] Skäl 14 Privacy Shield, Se listan på; https://www.privacyshield.gov/list, hämtad 2018-10-20.
[101] Bilaga II Privacy Shield.
[102] Voigt, m fl, *The EU General Data Protection Regulation (GDPR),* A Practical Guide, s. 123.
[103] Privacy Shield, skäl 22.

uppgifterna insamlades. Principen om säkerhet kräver att de som lagrar, använder, skapar eller sprider personuppgifter måste vidta lämpliga och rimliga skyddsåtgärder.[104] Enskilda måste enligt den sjätte principen om tillgång kunna ta bort, rätta eller ändra oriktig eller felbehandlad information som ett företag innehar om det inte skulle vara oproportionerligt. Rättsmedel, genomförande och ansvar är en viktig princip som utarbetades i och med kritiken av Safe Harbor där begränsningarna för enskilda att åberopa sina rättigheter kritiserades. Anslutna företag ska därmed tillhandahålla rättsmedel för den registrerade vars personuppgifter blivit behandlade. Det sker genom att frivilligt inrätta en effektiv prövnings mekanism för att hantera klagomål.[105] Den sista principen om ansvar för vidare överföring stadgar de villkor då en vidare överföring är tillåten. Det krävs enligt skäl 28 att det ska ske för begränsade och specificerade ändamål, på grundval av ett avtal och att sådant avtal i sig ger samma skyddsnivå som principerna garanterar.

Företag ska som tidigare nämnt implementera dessa principer i deras policy och de måste enligt skäl 22 årligen åter certifiera sig till Privacy Shield. Även om principerna i sig inte motsvarar alla bestämmelser i GDPR så liknar det väsentligen det som uppställs inom EU.

6.3.2 Brottsbekämpande ändamål

I Privacy Shield undantas vissa situationer från principerna. Det gäller de fall då offentliga myndigheter i USA behöver tillgång till personuppgifter i situationer som rör den nationella säkerheten, allmänintresset eller rättsefterlevnanden.[106] Under vilka omständigheter personuppgifter får inhämtas och användas regleras däremot i amerikansk lag. Själva möjligheten för myndigheter att framtvinga information ska framgå i företagens policy. Kommissionen har i och med Privacy Shields genomförande granskat den amerikanska lagen som reglerar de situationerna och dragit slutsatsen att dessa ingrepp begränsas till vad som är absolut nödvändigt.[107] Till skillnad från Safe Harbor så säkerställer Privacy Shield att undantagen tillämpas i de fall då det är absolut nödvändigt och proportionerligt.[108]

I Privacy Shield görs en distinktion mellan de regelverk som tar sikte på nationell säkerhet och de som inriktar sig på brottsbekämpande ändamål.[109] De regelverk som behandlar brottsbekämpande ändamål blir relevanta vid en analys då även CLOUD Act fokuserar på de ändamålen. Privacy Shield benämner både i skäl 126 och bilaga VII integritetsskyddet i fjärde tillägget i den amerikanska konstitutionen. De krav på ”sannolika skäl” för en husrannsakningsorder och skälighetstestet i de fall husrannsakningsordern inte gäller motsvarar enligt kommissionen unionens krav på nödvändighet och

[104] Skäl 24 Privacy Shield.

[105] Skäl 26 Privacy shield.

[106] Skäl 64 Privacy Shield, Calder, Alan, *EU GDPR & EU-US Privacy Shield- A Pocket Guide,* IT Governance Publishing 2017, s. 55-56..

[107] Skäl 123, 153 Privacy Shield.

[108] Skäl 8 Privacy Shield.

[109] Se Privacy Shields skäl under avsnitt 3.1 och 3.2.

proportionalitet.[110] Skyddet omfattar enligt kommissionen tredjelands personer indirekt genom att de brottsbekämpande myndigheterna måste ansöka om en rannsakningsorder, alternativt respektera skälighetstestet för att inhämta information från Amerikanska företag.[111] Det hindrar därmed amerikanska myndigheter från att gränslöst och utan befogande anledningar tillgå personuppgifter.[112] De myndigheter som har befogenhet att tvinga amerikanska företag att lämna ut personuppgifter via olika rättsprocesser är federala utredare och federala åklagare som är tjänstemän vid justitieministeriet. Även tjänstemän från Federal Bureau of Investigation (FBI) och myndigheter som är brottsbekämpande inom justitieministeriet har rätt att kräva ut personuppgifter.[113] Som tidigare behandlats så sträcker sig inte alltid fjärde tilläggets skydd till att även omfatta all tekniskt lagrad information. I Annex VII och skäl 132 behandlas därför specifikt ECPA och SCA som ger ett ökat integritetsskydd. Kommissionen menar på att lagen ger personer vars personuppgifter inhämtats en möjlighet till att vid en federal domstol väcka en civilrättslig talan där skadestånd kan krävas eller att den enskilde väcker en fastställelsetalan mot en statstjänsteman eller mot USA.[114] Utöver den möjligheten så påpekade kommissionen att det i annat fall finns en allmän bestämmelse i den amerikanska förvaltningslagen (Administrative Procedure Act) där den enskilda kan kräva en rättslig prövning i de fall den enskilda felaktigt drabbats eller skadats av rättsliga åtgärder.[115] Man kan ifrågasätta ifall de rättsmedel som finns de enskilda tillhanda motsvarar de krav som artikel 47 i stadgan uppställer. Kommissionen nämner också andra lagar som ger enskilda en rätt att väcka talan som exempelvis avlyssningslagen. De blir dock inte aktuella då de inte ger enskilda en rätt att väcka talan för de åtgärder som vidtagits av brottsbekämpande myndigheter i enlighet med CLOUD Act. Vidare finns det riktlinjer som utfärdats av justitieministern för hur brottsbekämpande myndigheter vid utredningar ska inkräkta så lite som möjligt, de kommer dock inte att diskuteras i denna uppsats.

Personuppgiftsbehandlingen som utförs av brottsbekämpande myndigheter är ett undantag från de principer som regleras i Privacy Shield och därmed även de mekanismer som beslutet erbjuder. Den enskilde måste därmed tillvarata sin rätt genom att använda sig av de amerikanska processuella reglerna. Det är inte alltid lätt för enskilda från tredje land att veta hur de ska gå till väga och rättslig rådgivning kan vara dyrt. Det är inte alltid heller så att den enskilde vet om att brottsbekämpande myndigheter i USA har framtvingat personuppgifter. En annan fråga som uppstår är de fall då USA har ingått exekutiva avtal med utländska länder. Kan enskilda väcka talan gentemot ett sådant avtal då de inte är föremål för judiciell prövning. Man kan ifrågasätta om Privacy Shields nödvändighet och

[110] Skäl 126 Privacy Shield.

[111] Skäl 126 Privacy Shield.

[112] Annex VII stycke 2 Privacy Shield.

[113] Annex VII stycke 3 Privacy Shield.

[114] Skäl 132 Privacy Shield.

[115] Skäl 130 Privacy Shield, 5 U.S.C. § 706(2)(A).

proportionerlighetskrav efterlevs då möjligheten till rättslig prövning, speciellt i de fall exekutiva avtal har ingåtts verkligen upprätthålls.

7. Förhållandet mellan CLOUD Act och Privacy Shield

Amerikanska molntjänsteföretag som lagrar personuppgifter åt kunder på molntjänster som innefattar elektronisk kommunikation eller annan information blir i och med CLOUD Act tvungna att lämna ut uppgifterna. Det sker efter en rannsakningsorder eller ett administrativt föreläggande beroende på om information är äldre än 180 dagar. De amerikanska molntjänstföretagen anslutna till Privacy Shield måste även behandla personuppgifter i enlighet med dess principer så länge de behandlar personuppgifter som överförts från EU. Det krävs då att företagen i sin policy implementerar de olika principerna. Privacy Shield gör ett undantag i de fall brottsbekämpande myndigheter vill få ut personuppgifter. Det regleras som tidigare behandlats i amerikansk lag. Där behandlas, förutom själva utlämnandet av personuppgifter, även de processuella reglerna varvid molntjänsteföretag samt enskilda kan använda sig av vid ett rättsstridigt utlämnande.

7.1 Europaparlamentets kritik

Utskottet i Europaparlamentet för medborgerliga fri- och rättigheter samt rättsliga och inrikesfrågor (LIBE) är kritiska till Privacy Shield. En av de flera anledningar som utskottet påpekar är CLOUD Act. I sin resolution som röstades igenom i Europaparlamentet i juni 2018 med 303 röster mot 252 varvid 29 blanka menade utskottet att Privacy Shield skulle upphävas.[116] Resolutionen ansåg att upphävandet skulle ske den 1 september 2018 om inte USA skulle följa de skyddsregler för personuppgifter som EU uppställde.[117] I punkt 27 uttrycker utskottet sin oro för de amerikanska och de utländska myndigheternas möjligheter att inrikta sig på och tillgå personuppgifter som befinner sig utanför USAs gränser. Resolutionen hänvisar till de ömsesidiga rättsliga avtalen i artikel 48 GDPR där en överenskommelse om ett utlämnande kan ske. Utskottet ansåg att CLOUD Acts extraterritoriella tillämpning skulle kunna kränka andra länders jurisdiktion samtidigt som det skulle strida mot EU:s skydd för personuppgifter. Varken principerna enligt Privacy Shield eller utfästelserna av den amerikanska administrationen i bilagorna visar på eller försäkrar en processuell förbättring för de enskilda. Utskottet jämförde det med det föregående beslutet Safe Harbor som underkändes av EU-domstolen och menade på att Privacy Shield inte gjort några direkta framsteg. De

[116] Nyheter Europaparlamentet, *Suspend EU-US data exchange deal, unless us complies by 1 september, say MEPs,*2018, http://www.europarl.europa.eu/news/hu/press-room/20180628IPR06836/suspend-eu-us-data-exchange-deal-unless-us-complies-by-1-september-say-meps, hämtad 2018-12-23.

[117] European Parliament, *Motion for a resolution,* 2014, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+B8-2018-0305+0+DOC+PDF+V0//EN, hämtad 2018-12-23.

processuella reglerna som den amerikanska lagen uppställde då brottsbekämpande myndigheter fick tillgång till personuppgifter upplevde inte kraven som säkerställs av artikel 47 stadgan.

7.2 Är rättsläget oförändrat?

Kommissionen valde att inte rätta sig efter resolutionen som inte har en rättslig verkan utan endast uttrycker politiska uppfattningar.[118] Kommissionen uttryckte sig i sin andra granskning av Privacy Shield som ägde rum i december 2018 där kommissionen bedömde att CLOUD Act inte har en påverkan på Privacy Shield. Enligt kommissionen tog Privacy Shield endast sikte på de situationer då personuppgifter behandlas i USA efter att de blivit överföra från EU. Personuppgifter befinner sig då på amerikanska servrar och de brottsbekämpande myndigheterna kan då tillgå personuppgifter enligt Privacy Shield som hänvisar till amerikansk lag. Rättsläget är därmed oförändrat då den amerikanska konstitutionens skydd och SCA reglerar området. Det nya med CLOUD Act är däremot den extraterritoriella tillämpningen vilket belystes i Microsoft fallet. Problematiken låg i de fall då data var placerad på servrar utanför USAs territorium. Kommissionen uttryckte sin oro över framtiden i de fall USA skulle ingå exekutiva avtal med utländska stater som inte är med i EU. Det skulle då påverka de företag anslutna till Privacy Shield som lagrar personuppgifter på amerikanska servrar. Inga avtal har i dagsläget ingåtts men kommissionen var ändå tveksam till om ett exekutivt avtal med utländsk stat skulle påverka Privacy Shield. Kommissionen ansåg att de krav som CLOUD Act ställer upp innan ett avtal ingås och en överföring äger rum kan motsvara de uppställda av Privacy Shield. I U.S.C § 2523 (b) krävs det att landet respekterar mänskliga rättigheter och uppställer ett skydd för den personliga integriteten. Den inhemska lagen måste ha ett materiellt och processuellt skydd för integriteten och medborgerliga friheter. Informationen får endast inhämtas för vissa ändamål som att utreda, förhindra, lagföra eller upptäcka allvarlig brottslighet. Kongressen kan, om de skulle anse att avtal inte uppfyller alla villkor, göra invändningar. Kommissionen bedömde i sin granskning att de krav som CLOUD Act uppställer för att ingå ett avtal med utländsk stat kan stå i överensstämmelse med Privacy Shields krav. Dock så kommer kommissionen att göra en ny bedömning i och med ett avtal har ingåtts för att försäkra sig om att Privacy Shields skydd upprätthålls. Även International Trade Administration (ITA) som är en del av U.S. Department of Commerce som har hand om anslutningen till Privacy Shield har liknande ståndpunkter som kommissionen. ITA ansåg att CLOUD Act inte står i konflikt med Privacy Shield då det endast är en mekanism för överföring av personuppgifter från EU.[119]

[118] Europeiska rådet Europeiska unionens råd, *Rådets slutsatser och resolutioner,* https://www.consilium.europa.eu/sv/council-eu/conclusions-resolutions/, hämtad 2018-12-23.

[119] Privacy Shield Program, *FAQs – General,* https://www.privacyshield.gov/article?id=General-FAQs, hämtad 2018-12-23.

Frågan om det uppstår en konflikt mellan CLOUD Act och Privacy Shield är omdiskuterad. Slutsatser som kan dras är att CLOUD Act inte har en påverkan på företag anslutna till Privacy Shield när det gäller den extraterritoriella tillämpningen. CLOUD Act har inte heller en påverkan på de personuppgiftsansvariga som väljer att överföra personuppgifter i enlighet med Privacy Shield då beslutet fortfarande är giltigt. Däremot kan det ifrågasättas om inte CLOUD Act försvårar de processuella rättigheterna som de enskilda är garanterade. Antingen genom de exekutiva avtalen eller då det endast är molntjänstleverantörer kan göra invändningar mot en inhämtning av uppgifter. En fråga är om det avtalande utländska landet uppfyller både ett materiellt och processuellt skydd som motsvarar det i Privacy Shield. Brottsbekämpande myndigheters insamling är undantagen i Privacy Shield men endast på de villkoren att den amerikanska lagen garanterar ett materiellt och processuellt skydd likvärdigt det som EU uppställer.[120]

Kommissionen har granskat det fjärde tillägget, ECPA och SCA och därmed dragit slutsatsen att en insamling endast kan ske i de fall det är nödvändigt eller proportionerligt. Kommissionen tror att CLOUD Act med dess uppställda krav på en utländsk stat kan upprätthålla Privacy Shields skydd som hänvisar till amerikansk lag. En fråga som uppkommer då är om enskilda ska väcka talan i den utländska staten eller i USA om de känner sig kränkta. Det är också problematiskt att en amerikansk domstol inte kan granska lagenligheten av avtalet. Skulle kommissionen eller ett annat EU organ anse att avtalet inte uppfyller de villkor uppställda i CLOUD Act så kan de inte begära en ogiltigförklaring av avtalet utan endast själva överföringen i sig kan prövas. Det återstår att se om kommissionen intar samma ståndpunkt efter att ett avtal har ingåtts.

7.3 Förlita sig på Privacy Shield?

I de fall amerikanska molntjänstleverantörer lagrar personuppgifter åt kunder inom EU på servrar inom USA och direkt riktar sin verksamhet gentemot EU ska även GDPR tillämpas. Leverantören kan då inträda i rollen som biträde eller personuppgiftsansvarig vilket kommer att behandlas i nästa avsnitt. Rättsläget blir däremot svårare då ett moderbolag är beläget i USA med ett dotterbolag som erbjuder molntjänster inom EU. Moderbolaget blir då inte skyldigt att följa GDPR i och med ett överförande av personuppgifter men däremot Privacy Shield som gör ett undantag för brottsbekämpande myndigheters begäran av personuppgifter. Ett biträde som är etablerad inom EU samt personuppgiftsansvariga får därmed förlita sig på att Privacy Shield som hänvisar till amerikansk rätt uppställer en adekvat skyddsnivå.

[120] Mål C-362/14, p. 74.

8. Förhållandet mellan CLOUD Act och GDPR

CLOUD Act tar sikte på amerikanska molntjänstföretag med servrar både inom och utanför USA. Det territoriella tillämpningsområdet som stadgas i artikel 3 GDPR gör att GDPR blir tillämpligt. Det kan ske antingen genom att ett företag etablerat inom EU eller riktar sina tjänster gentemot EU erbjuder enskilda molntjänster. Det finns dock två situationer som måste skiljas åt. Det första fallet avser de situationer då ett amerikanskt molntjänstföretag genom ett dotterbolag är etablerat inom EU med dess servrar inom EU:s gränser. Det andra fallet avser de situationer då ett dotterbolag till ett amerikanskt molntjänstföretag är etablerat i tredje land utanför EU och USA och inte riktar sin service gentemot EU. Både GDPR och CLOUD Act kommer genom deras extraterritoriella tillämpning i viss mån att omfatta de båda situationerna.

8.1 CLOUD Acts extraterritoriell tillämpning

En omdiskuterad fråga är om CLOUD Act verkligen tillämpas extraterritoriellt. Är det servrarna eller platsen där informationen kan inhämtas som är avgörande eller är det båda två? Liknande frågor med en del meningsskiljaktigheter uppkom även i Microsoft fallet. The U.S District Court of the Southern District of New York fastslog i målet att SCA inte tillämpades extraterritoriellt då informationen kunde inhämtas via datorer i USA. Den andra instansen, U.S. Court of Appeals for the Second Circuit, hävdade motsatsen då servrarna rent fysiskt var belägna i ett land utanför USA och förvaltades där. Man kan hävda att CLOUD Act tillämpas extraterritoriellt då den antogs för att lösa det problem som uppstod då SCA begränsade de brottsbekämpande myndigheternas åtkomst. Det gällde så länge servrarna fysiskt var placerade i utlandet. Det stadgas också i CLOUD Act att hänsyn ska tas till eventuella lagkonflikter som kan uppstå, även det tyder på att lagen tillämpas extraterritoriellt. Även kommissionen uttryckte sin oro till eventuella lagkonflikter om SCA skulle tillämpas extraterritoriellt i sitt utlåtande till the Supreme Court innan CLOUD Act antogs. De slutsatser som kan dras är att servrarnas position blir det avgörande för vilket lands lag som ska tillämpas. Både EU och USA utgår till viss del från servrarnas plats vilket även skapar en del andra problem. En fråga som kan uppkomma är i de fall brottsbekämpande myndigheter får tillgång till ett företags mobiltelefon som är aktiv världen över. Ska de då undersöka på vilka servrar data är lagrad för att sedan få åtkomst till informationen via det landet eller är telefonens plats avgörande? Det finns flera situationer där liknande problematik uppkommer vilket många brottsbekämpande myndigheter inte alltid är medvetna om. Användare av molntjänster begriper sig inte alltid på tekniken bakom molntjänster och var den riktiga förvaltningen egentligen sker.

En stor vikt har lagts på servrarnas position och både CLOUD Act och GDPR har en extraterritoriell tillämpning varvid CLOUD Act sträcker sig längre än GDPR. De bygger på effektivitetsprincipen vilket är en utvidgning av territorialitetsprincipen. Landets inhemska lagar appliceras på handlingar som får konsekvenser i det landet. GDPRs artikel 3 fokuserar till skillnad från CLOUD Act på de fall ett företag som inte är etablerad inom EU ändå riktar sina tjänster eller övervakar beteenden inom EU. Det måste då ha någon koppling till EU för att GDPR ska bli tillämplig. CLOUD Act som reglerar endast brottsbekämpande myndigheternas åtkomst till personuppgifter går steget längre. Även dotterbolag eller andra företagsformer etablerade inom EU omfattas av CLOUD Act då ägaren, moderbolaget, faller inom begreppet ”United States person” 18 U.S.C. § 2523. Dotterbolaget eller de andra företagsformerna som inte riktar sin verksamhet mot USA eller inte är etablerade i USA omfattas ändå av CLOUD Act. Det gäller även i de fall servrarna skulle finnas på platser i hela världen så länge företaget fallet in under begreppet ”United States person”. Dock så kan den extraterritoriella tillämpningen vid domstolens helhetsbedömning efter en invändning ändå begränsas. Då ska förutom eventuella lagkonflikter också enligt 18 U.S.C § 2703(3)(d) leverantörens koppling och närvaro i USA undersökas men även nationalitet och position av den registrerade. Det finns ingen garanti för att de amerikanska domstolarna vid en invändning bedömer att de olika begränsningarna lagen uppställer väger tyngre än de brottsbekämpande myndigheternas intresse vid en avvägning som sker i enlighet med U.S.C. § 2703(2)(b)(ii). En leverantör vet inte alltid vilken identitet en enskild person eller aktör har vilket även var okänt i Microsoft fallet.[121]

Trots att rannsakningsorder i enlighet med CLOUD Act kan ogillas så är det problematiskt då det endast kan ske efter att leverantören har gjort en invändning. I och med GDPRs extraterritoriella tillämpning blir leverantörer av molntjänster i princip alltid skyldiga att invända för då inhämtningen med hänvisning till en domstolsorder måste vara förenlig med artikel 48 GDPR. Skulle en molntjänstleverantör inte invända så finns det enligt artikel 83.5 GDPR en risk för att företaget blir tvungna att betala en sanktionsavgift.

8.2 I enlighet med artikel 48 GDPR

En tredjelandsöverföring får inte enbart grunda sig på ett domstolsbeslut från tredje land enligt artikel 48 GDPR. Företag inom EU ska enligt EDPB:s riktlinjer avvisa förfrågningar från tredjeland och istället hänvisa till de ömsesidiga rättsliga avtalen. Som tidigare beskrivits i avsnitt 4.2 så krävs det att det förutom avtalet även grundar sig på någon annan omständighet i kapitel 5. Det kan bland annat hänvisas till allmänintresset eller för att försvara rättsliga anspråk som behandlas i artikel 49. Det krävs då att det rättsliga anspråket gäller företaget själv och inte deras kunder. En eventuell konflikt kan då uppstå med CLOUD Act där det stadgas att brottsbekämpande myndigheter med hänvisning till den allmänna säkerheten kan inhämta ett beslut om rannsakningsorder från en amerikansk

[121] Microsoft vs US., 892 F.3d 197 (2nd Cir. 2016), s. 220.

domstol. Både USA och EU kan tolka allmän säkerhet på olika sätt. Myndigheten måste enligt amerikansk lag visa på sannolika skäl för att ett brott har begåtts eller kommer att begås. CLOUD Act öppnar upp en genväg från GDPRs stadgande för de amerikanska brottsbekämpande myndigheterna. Det underlättar för USAs myndigheter som har en negativ syn på de ömsesidiga rättsliga avtalen och de regler som krävs för att få ut personuppgifter. Det framgår bland annat av Microsoft målet där både första instansen kritiserar avtalen och den långsamma processen som måste företas.[122] En tredjelandsöverföring utan något stöd i kapitel 5 får därmed inte ske i enlighet med GDPR medan CLOUD Act reglerar det motsatta då de bortser från GDPRs krav.

Ett annat problem som också kan skapa eventuella konflikter med GDPR är de exekutiva avtalen som stadgas i U.S.C § 2523. I artikel 44 GDPR krävs det att en personuppgiftsansvarig uppfyller villkoren i kapitel 5 och det gäller även i de fall en vidare överföring ska ske från tredjeland. Det innebär att USA inte kan inhämta uppgifter på ett sätt som är oförenligt med GDPR för att senare överföra uppgifterna. Det innebär också att USA inte i enlighet med artikel 48 skulle kunna inhämta uppgifter på ett lagligt sätt och senare överföra de till tredje land. Det tredje landet måste också uppfylla de villkor som finns stadgade i kapitel 5 då förordningens skydd i annat fall skulle undergrävas. Man kan ifrågasätta om CLOUD Acts krav som uppställs på en utländsk stat i U.S.C. § 2523 (b) kan leva upp till det skydd som finns inom EU? Skulle det vara acceptabelt om USA ingick ett exekutivt avtal med ett annat land som kommissionen redan anser har en adekvat skyddsnivå. Det finns inga direkta svar på de frågor som uppkommer, man kan däremot dra slutsatsen att CLOUD Act inte kommer i konflikt med GDPR så länge en leverantör invänder och att lagkonflikter blir en avgörande faktor i amerikanska domstolens analys. Huruvida man ska förlita sig på att ett biträde eller underbiträde invänder och att domstolen respekterar staters suveränitet kan inte anses vara rättssäkert för de enskilda. Den omständigheten att avtalen inte får underkännas av domstolen gör att inga EU-institutioner eller enskilda skulle kunna vända sig till domstol för att få avtalet underkänt.

8.3 Amerikanska molntjänstföretag som omfattas av artikel 3 GDPR

Så länge servrarna ligger inom EU blir artikel 3 GDPR tillämpligt då företaget antingen genom ett dotterbolag är etablerat i EU eller att biträdet riktar sin handel mot EU. Den vidsträckta tolkningen har en extraterritoriell tillämpning i vissa fall då företaget som riktar sin handel eller sina tjänster till kunder inom EU omfattas. Det innebär att amerikanska molntjänstleverantörer enligt artikel 3 GDPR blir skyldiga att följa förordningen. Många företag inom EU och Sverige har i och med införandet av GDPR fokuserat på att ha kontroll över var data befinner sig och att det lagras säkert. Den personuppgiftsansvarige har ett självständigt ansvar och det spelar egentligen ingen roll vilken tjänste-

[122] United States v. Microsoft Corp., F.Supp. 3d 466 (S.D.N.Y. 2014), s 474.

eller leveransmodell som kunden använder sig av. Då ett av de karaktäristiska särdragen är att kunden blir en del av ett virtuellt system där tekniken i princip är okänd för kunden gör det inte lättare. Avtalet blir det avgörande vilket inte alltid kan ingås under kundens villkor när det gäller publika molntjänster. CLOUD Act tar inte hänsyn till tjänste- eller leveransmodeller. De brottsbekämpande amerikanska myndigheterna kan framtvinga information så länge amerikanska företag är etablerade i USA och har kontroll över servrarna som kan befinna sig i olika delar av världen.

Problemet som uppstår för de amerikanska företagen är att de omfattas av både GDPR samt CLOUD Act. Enligt EDPBs riklinjer ska företag som är skyldiga att följa GDPR hänvisa till artikel 48 och de befintliga avtal som finns mellan staterna. Molntjänstleverantören får inte utlämna personuppgifter endast på den grunden att en rannsakningsorder utfärdats av en domstol. Skulle leverantören göra det så finns det en risk för att leverantören får betala sanktionsavgifter i enlighet med artikel 83.5 GDPR. Både den personuppgiftsansvarige och biträdet kan hållas ansvariga i de fall de båda har sitt etableringsställe i EU. Biträdet kan inte hållas ansvarig om biträdet skulle befinna sig i tredje land och inte inrikta sig verksamhet till EU. Skulle däremot servrarna finnas i EU så kan slutsatserna dras att företaget i vart fall riktar sin verksamhet gentemot EU. Oavsett var biträdet befinner sig så har den personuppgiftsansvariga ett självständigt ansvar enligt 28.1 GDPR och ska genom biträdesavtalet se till så att lagringen sker i enlighet med GDPR.

8.4 Amerikanska molntjänstföretag som inte omfattas av artikel 3 GDPR

I den andra situationen, där ett företag inom EU använder sig av dotterbolag till amerikanska molntjänstleverantörer med servrar i tredje land, är rättsläget mer osäkert. Skulle inte dotterbolaget rikta sin verksamhet gentemot EU så blir GDPRs artikel 3 inte tillämplig.[123] Ansvaret ligger då på den personuppgiftsansvariga som enligt 28.1 GDPR ska se till att endast biträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder ska anlitas. Biträdet måste också uppfylla kraven i förordningen samt säkerställa de registrerades rättigheter. Skulle ett underbiträde anlitas måste ett biträde inom EU när de ingår ett avtal i enlighet med artikel 28.3 GDPR informera personuppgiftsansvariga om det. Varken biträdet eller underbiträdet får då behandla personuppgifterna i strid med den ansvariges instruktioner vilka framkommer i avtalet 28.3 (a) GDPR.

Den fråga som uppkommer är om personuppgiftsansvariga som är medvetna om CLOUD Act och dess extraterritoriella tillämpning kan påstå att det anlitat ett biträde eller ett underbiträde som uppfyller kraven i förordningen. Överföringen sker då inte till USA utan till ett dotterbolag i ett tredje land vilket gör att Privacy Shield inte blir tillämpligt. Svenska företag som anlitat amerikanska dotterbolag som befinner sig i tredje land måste därför se till att överföringen sker i enlighet med

[123] Voigt, m fl, *The EU General Data Protection Regulation (GDPR), A Practical Guide*, s. 25.

någon av de grunderna som benämns i kapitel 5. Kommissionen kanske redan har beslutat om att landet har en adekvat skyddsnivå alternativt att företagen använder sig av standardklausuler eller bindande företagsbestämmelser i enlighet med artikel 46.2(c)(d). Skulle ett beslut om adekvat skyddsnivå ligga till grund, som kommissionen tagit, kan den personuppgiftsansvarige förlita sig på att en överföring är tillåten. Skulle inget beslut om en adekvat skyddsnivå ha antagits kan man ifrågasätta om en personuppgiftsansvarig kan förlita sig på att standardklausulerna eller de bindande företagsbestämmelserna lever upp till GDPRs krav. Det gäller i de fall dotterbolagen omfattas av CLOUD Act i med den breda tolkningen av en ”United State person” i U.S.C. § 2523. Skulle dotterbolaget göra en invändning så kan det inte hänvisa till någon lagkonflikt om inte landets inhemska lag skulle reglera området. Däremot finns det andra omständigheter som den amerikanska domstolen kan ta hänsyn till. Personen ifråga som informationen gäller kanske inte enligt § 2703(2)(i) faller under definitionen av en amerikansk person. Den amerikanska domstolen tar då hänsyn till i enlighet med § 2703(3)(d) var personen ifråga befinner sig och personens koppling till USA. Även leverantörens koppling till USA beaktas, § 2703(3)(e). Domstolen ska då göra en helhetsbedömning av de omständigheterna för att se om rannsakningsorder ska ogillas. Men som tidigare påpekats så krävs det att företaget i fråga som rannsakningsordern riktar sig mot invänder.

8.5 Effektiva rättsmedel

Det krävs enligt rättighetsstadgans artikel 47 att de enskilda tillhandahålls effektiva rättsmedel. Enskilda kan i enlighet med ECPA, 18 U.S.C. § 2702 väcka en civilrättslig talan vid en rättsstridig tillgång. Den kan ske i de fall inhämtningen är otillåten eller inte har godkänts av en domstol. En nyhet med CLOUD Act är att leverantörerna har fått en möjlighet att invända innan själva framtvingandet av uppgifter. En invändning kan ske på två grunder, antingen att det inte är en ”United States person” eller att en eventuell lagkonflikt kommer att uppstå. Domstolen får därefter göra en helhetsbedömning där olika intresseavvägningar görs. Det som kan ifrågasättas är de enskildas möjlighet att invända då de i vissa fall inte ens vet om att information har begärts av en myndighet 18 U.S.C. § 2703(b)(1)(a), Anledningen till varför information inte alltid lämnas till den enskilde är förståeligt då bevisning lätt kan manipuleras genom att förflyttas eller manipuleras. Däremot blir det rättsosäkert för den enskilde som endast kan förlita sig på att biträdet kommer att invända mot rannsakningsordern. Skulle leverantören invända så kan analysen som den amerikanska domstolen ska företa diskuteras. Är analysen tillräcklig för att tillvarata skyddet av den personliga integriteten av de enskilda?

8.6 Risker för personuppgiftsansvariga

I de fall en personuppgiftsansvarig har överfört personuppgifter till företag anslutna till Privacy Shield utgör ingen risk i sig. Däremot kan företaget vid en ogiltigförklaring av Privacy Shield vara tvunget att flytta över all data vilket kan vara tidskrävande och kostsamt. Det som personuppgiftsansvariga kunder till molntjänster bör uppmärksamma är de situationer då de lagrar på servrar inom EU men som ägs av amerikanska företag. Den omständigheten att CLOUD Act endast inriktar sig på ”United States person” har ingen avgörande betydelse då integritetsskyddet inte baserar sig på medborgarskap eller andra liknande faktorer. Anknytningen till EU är avgörande, antingen då företaget är etablerat i EU eller riktar sina tjänster till EU. Det kan vara ett dotterbolag till ett amerikanskt moderbolag, det kan också vara amerikanska företag som erbjuder sina molntjänster till personer inom unionen. Då rättsläget är oklart ska personuppgiftsansvariga iaktta stor försiktighet då personuppgifter vid en brottsmisstanke kan begäras ut utan den ansvariga eller enskildes kännedom. Rätten till att invända innan personuppgifter krävs ut är begränsad då den enskilde oftast får kännedom om inhämtningen i efterhand. Likaså kommer även de garantier som har lämnats i samband med ingåendet av molntjänstavtalet att få ge vika då CLOUD Act inte begränsar tillämpningen med hänvisning till något avtal. Molntjänstleverantörer kommer hamna i situationer där både GDPR och CLOUD Act reglerar samma situation, dock så har de till skillnad från de enskilda en rätt samt en skyldighet att invända innan ett utlämnade av uppgifter.

9. Sammanfattande slutsats

Tekniken bakom molntjänster kan vara komplicerad. Avsaknaden av faktisk kontroll över var data befinner sig annat än en hänvisning till avtalet underlättar inte situationen. De olika principerna som territorialitet och nationalitet som folkrätten reglerar för att avgränsa en stats jurisdiktion i straffrättsliga sammanhang blir svårapplicerade. Meningsskiljaktigheter förekommer kring vad som är själva platsen där data befinner sig då det inte avser något fysiskt.

Rättsläget är oklart då CLOUD Acts förhållande till Privacy Shield och GDPR lämnar en rad öppna frågor. Privacy Shield står i och med antagandet av CLOUD Act på en ostadig grund då även kommissionen i sin andra granskning skulle följa utvecklingen med särskild hänsyn till de exekutiva avtalen. Även de amerikanska företagen står inför ett dilemma då kunder inom EU som inträder rollen som personuppgiftsansvarig kommer avstå från att lagra på deras servrar. Man kan ifrågasätta om inte amerikanska företag som erbjuder molntjänster kommer att konkurreras ut av europeiska molntjänstleverantörer i och med antagandet av CLOUD Act.

Inom EU är det för tillfället endast de internationella ömsesidiga rättsliga avtalen som berättigar ett överförande i och med en utländsk order. Det medför att personuppgiftsansvariga riskerar att betala en sanktionsavgift i de fall amerikanska brottsbekämpande myndigheter krävde ut personuppgifter lagrade på servrar inom EU. Slutsatser som kan dras är därmed att personuppgiftsansvariga som lagrar på molntjänster bör vara medvetna om det osäkra rättsläget och göra det de kan för att minimera risken att amerikanska brottsbekämpande myndigheter med hänvisning till CLOUD Act tvingar fram personuppgifter på ett sätt som strider mot GDPR.

Källförteckning

Offentligt tryck

Propositioner

Prop. 2009/10:80, *En reformerad grundlag,* Stockholm: Justitiedepartementet.
Prop. 2004/05:46, *Avtal med Amerikas förenta stater om utlämning och om internationell rättslig hjälp i brottmål,* Harpsund: Justitiedepartementet

Litteratur

Bring, Ove, Mahmoudi, Said, Wrange, Pål, *Sverige och folkrätten,* Nordstedts Juridik 2014.

Calder, Alan, *EU GDPR & EU-US Privacy Shield- A Pocket Guide,* IT Governance Publishing 2017.

Carlson, Laura, *American business law: A civil law perspective*, Iustus 2004.

Edvardsson, Tobias & Frydlinger, David, *Molntjänster: juridik, affär och säkerhet,* Nordstedts Juridik AB 2018.

Kavis, Michael, *Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS,PaaS, and IaaS),* Wiley 2014.

Monika, Wendleby, Dag, Wetterberg, *Dataskyddsförordningen GDPR, förstå och tillämpa i praktiken*, Utbildning AB 2018.

Sjöberg Magnusson, Cecilia, Rättsinformatik, *Juridiken i det digitala informationssamhället*, Studentlitteratur, Lund 2018.

Voigt, Paul, *The EU General Data Protection Regulation (GDPR), A Practical Guide*, Springer International Publishing AG.

Rättsfall

EU-domstolen

Dom den 6 november 2003, *konfirmandlärarfallet*, mål C-101/01.
Dom av den 6 oktober 2015, *Maximillian Schrems mot Data Protection Commissioner,* Mål C-362/14, ECLI:EU:C:2015:650

USA

United States Supreme Court

Carpenter v. United States, 484 U.S. 19 (1987).
Katz v. United States, 389 U.S. 347 (1967).
Morrison v. National Australia Bank Ltd., 561 U.S. 247 (2010).
Smith v. Maryland, 442 U.S. 735, 743 (1979).

Microsoft v. US., 584 U.S (2018)

Federala domstolar

Microsoft vs US., 892 F.3d 197 (2nd Cir. 2016).
United States v. Microsoft Corp., F.Supp. 3d 466 (S.D.N.Y. 2014).

Internationella domstolen i Haag

SS Lotus (France v Turkey) (Judgement) PCIJ Rep Series A No 10 (1927).

Artiklar

Reuterswärd Reinhold, *Lagstiftningsmaktens folkrättsliga gränser,* SvJT 1977.

Solove, Daniel, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, SSRN Electronic Journal, 2002, Brinegar v. United States, 338 U.S. 160 (1949).

Privacy- Stored Communications Act- Second Circuit Holds that the Government Cannot Compel an Internet Service Provider to Produce Information Stored Overseas- *Microsoft Corp. v. United States,* 829 F .3d 197 (2d Cir.2016) [130 Harv L Rev. 769] s. 774.

Elektroniska källor

EU

Council of the European Union*, Handbook on the practical application of the EU-U.S. Mutual Legal Assistance and Extradition Agreements,*2011, s. 33, http://www.statewatch.org/news/2011/mar/eu-council-eu-usa-mla-handbook-8024-11.pdf, hämtad 2018-11-19.

EDPB, *Riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679 antagna den 25 maj 2018,* https://www.datainspektionen.se/globalassets/dokument/riktlinjer-om-undantag-enligt-artikel-49.pdf, hämtad 18-11-2018.

European *Commission, Mutual legal assistance and axtradition,* https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en, hämtad 2018-11-20.

European Parliament*, Motion for a resolution,* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+B8-2018-0305+0+DOC+PDF+V0//EN, 2018, hämtad 2018-09-13.

Europeiska rådet Europeiska unionens råd, *Rådets slutsatser och resolutioner,* https://www.consilium.europa.eu/sv/council-eu/conclusions-resolutions/, hämtad 2018-12-23.

USA

CRS Report for Congress, received through the CRS Web*, Staturory Interpretation: General Principles and Recent Trends*, 2006, https://www.everycrsreport.com/files/20060330_97589_d597ae5a20af3bc9dc0711704bb2329308fd81f1.pdf Hämtad 2018-12-10.

Department of Justice*, The USA PATRIOT Act: Perserving Life and Liberty (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism),* https://www.justice.gov/archive/ll/highlights.htm, hämtad 2018-11-24.

Jolly, Ieuan, Loeb, Loeb, *Data protection in the United States: overview,* https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1, 2018, hämtad 20-11-18.

Mell, Grance, *The NIST Definition of Cloud Computing*, http://delivery.acm.org/10.1145/2210000/2206223/SP800-145.pdf?ip=213.113.187.229&id=2206223&acc=OPEN&key=4D4702B0C3E38B35%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35%2E6D218144511F3437&__acm__=1546815210_81204dc019b5c7839d82dea9b347daaa, (2011) hämtad 2018-09-13,

Privacy Shield framework, https://www.privacyshield.gov/list, hämtad 2018-09-13.
Privacy Shield Program*, FAQs – General*, https://www.privacyshield.gov/article?id=General-FAQs, hämtad 2018-12-23.

Report and Recommendations of the President's Review Group on Intellifence and Communication Technologies, *Liberty and security in a changing world*, 2013, https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf , hämtad 2018-11-20.
Scolnik, Alexander*, Protection for Electronic Communications: Stored Communications Act and the Fourth Amendment*, 78 Fortdham L. Rev. 349 (2009) s. 353, https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4471&context=flr, hämtad 2018-11-22.

Svenska myndigheter

Datainspektionen, *hur vet vi om ett tredje land har adekvat skyddsnivå,* https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/tredjelandsoverforing/hur-vet-vi-om-ett-tredje-land-har-adekvat-skyddsniva/, hämtad 2018-09-13.

Datainspektionen, *Så här är dataskyddet organiserat i EU,* https://www.datainspektionen.se/om oss/datainspektionens-internationella-arbete/sa-har-ar-dataskyddet-organiserat-i-eu/, hämtad 2018-09-13.

Lagkommentarer

Magnusson Sjöberg, Artikel 48 Överföringar och utlämnanden som inte är tillåtna enligt unionsrätten, *Lexino 2018-09-03.*

Stockholms universitet
Juridiska institutionen
SE-106 91 Stockholm
Telefon/Phone: 08 – 16 20 00
www.su.se

Stockholms universitet