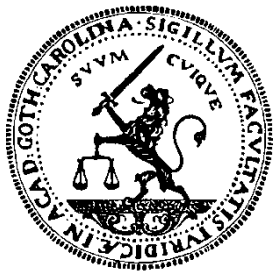

JURIDISKA FAKULTETEN
vid Lunds universitet

Julianne Ahlesten

Personuppgifter i molntjänster
Ansvarsreglering enligt GDPR

LAGF03 Rättsvetenskaplig uppsats

Kandidatuppsats på juristprogrammet
15 högskolepoäng

Handledare: Emma Ahlm

Termin: VT2018

Innehåll

Summary

In an ever more digital world, an increasing number of organizations chose, for various reasons, to move their data from local servers and into the cloud - including personal data.

Services most commonly thought of as Cloud services are Dropbox, Share-point and ICloud, but there are a vast number of different Cloud services and variants to choose from - some of which will be covered in the essay, along with giving a definition of Cloud services and the judicial responsibilities that follow such services.

In short, Cloud services store data on remote servers, accessible anywhere with an internet connection. As opposed to working locally on your company servers or laptop, you buy this external IT-resource as a service, letting you store and access information with the Internet as your platform.

This essay covers and explains the legal responsibilities under the new General Data Protection Regulation (GDPR), between suppliers of Cloud services and their customers when storing and processing personal data in the Cloud. The GDPR is directly applicable in every EU country, from 25th of May 2018 and onwards, and forms the legal grounds for processing personal data concerning EU citizens and EU visitors.

The essay also covers various variants and functions of a Cloud service, with the corresponding benefits and disadvantages. A big benefit from using Cloud services is outsourcing data storage and processing to companies more focused on IT and security than the customers organization (and removing some of the associated cost). The added benefits and cost cuts do, however, come with legal risks and demands.

Cloud services always, at a minimum, involve two parties. The parties need to make clear their respective responsibilities to the data subjects (and supervisory authorities), under GDPR by formal contract. The details of such a contract and their meaning will be further discussed in the essay.

Sammanfattning

I en värld där allt mer och mer blir digitaliserat finns det en stor användargrupp som väljer, av olika anledningar, att förflytta sin behandling av data, både persondata och annan form av data, från det lokala datacentret till en molntjänst.

Molntjänster i dagligt tal förknippas ofta med tjänster såsom Dropbox, Share-point och Icloud - molntjänster kan dock vara mycket mer än så och tekniskt komplexa varianter finns, vilket kommer att redogöras för i uppsatsen. Vad en molntjänst är samt hur det juridiska ansvaret regleras kommer också redogöras för.

Kortfattat innebär en molntjänst att du arbetar mot servrar över internet och inte lokalt på din dator, en extern IT-resurs som företag köper in som en tjänst - en teknik för att lagra information genom internet som plattform.

Uppsatsen redogör för de ansvarsregleringar som krävs gällande personuppgiftsbehandling i molntjänster mellan avtalsparterna, utifrån dataskyddsförordningen (GDPR). Dataskyddsförordningen är direkt tillämplig som lag i samtliga EU:s medlemsländer, från och med 25 maj 2018, och utgör efter detta datum grunden för personuppgiftsbehandling inom hela EU. Utifrån denna lagstiftning fokuseras det i denna uppsats på molntjänster, en digital produkt som i många fall är en komponent i behandling av personuppgifter.

I uppsatsen beskrivs även molntjänsters funktioner och egenskaper. Det finns flera för- och nackdelar med molntjänster. En fördel är att företag som specialiserar sig på lagring, backup och säker hantering av data kan ta över serverfunktionen hos många företag som inte har egen IT-kompetens. Det är således praktiskt att använda molntjänster, men det finns säkerhetsrisker och juridiska regleringar som behöver tas hänsyn till.

Vid användning av molntjänster finns det alltid flera parter inblandade. Det finns åtminstone alltid en kund och en leverantör. Dessa parter intar huvudrollerna i molntjänstavtalet och därför är relationen mellan dem i centrum när det gäller personuppgiftsbehandling i molntjänster. För att reglera ansvaret för personuppgifterna mellan parterna och sätta ramar för parternas agerande uppställs krav i GDPR på att ansvaret ska formaliseras. Hur ansvarsfördelningen ska se ut och hur detta ska regleras i enlighet med GDPR, presenteras i uppsatsen.

Förkortningar

Artikel 29-gruppen	Artikel 29-arbetsgruppen för skydd av personuppgifter, etablerad med stöd av artikel 29 i direktiv 95/46/EG
Dataskyddsdirektivet	Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter
EKMR	Europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna
ENISA	Europeiska unionens byrå för nätverks- och informationssäkerhet
EU	Europeiska unionen
GDPR	Europaparlamentets och rådets förordning 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (dataskyddsförordningen)
IaaS	Infrastructure as a Service
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
SaaS	Software as a Service

Övriga begrepp, uttryck och ord som behöver klargöras förklaras löpande i texten samt i fotnoter i uppsatsen.

1 Inledning

1.1 Bakgrund

Den 25 maj 2018, kommer den nya dataskyddsförordningen (GDPR) börja tillämpas. Förordningen trädde i kraft redan 2016 och därefter följer en implementeringsperiod på två år, för att medlemsstaterna och marknaden skulle hinna ställa om sig och anpassa sig inför den nya lagstiftningen. GDPR är den största förändringen inom dataskydd och IT-juridik i Europa på årtionden. GDPR påverkar alla företag, organisationer, myndigheter och föreningar som utför behandling[1] av personuppgifter[2]. Det är en teknikneutral lagstiftning, men i dagens samhälle använder vi många, och i flera fall, mycket avancerade system och däribland inte minst molntjänster. I en tid av stora tekniska framsteg är denna uppsats inriktad på att analysera en teknisk framställning, molntjänster eller *datamoln*[3] som de även kallas, och dess relation till juridiken. Mer specifikt hur ansvaret mellan avtalsparterna (leverantör och kund), vad gäller de personuppgifter som finns i molntjänsten, regleras i GDPR. Det finns flera komplexa aspekter kring digitalisering i kombination med skyddet av den personliga integriteten och en del av dessa avhandlas i uppsatsen.

---

[1] Artikel 4.2 GDPR. Definitionen av behandling av personuppgifter är så gott som identisk med Dataskyddsdirektivet. Det är en mycket bred definition och inkluderar allt som kan göras med personuppgifter. Något som lätt missas är att användning av molntjänster innefattas i begreppet, då det utgör lagring av personuppgifter.

[2] Artikel 4.1 GDPR. Definitionen av en personuppgift är varje upplysning som avser en identifierad eller identifierbar fysisk person. Det kan exempelvis vara namn, personnummer, postadress och telefonnummer. I uppsatsen kommer *persondata* användas som hänvisning till begreppet *personuppgift* för att variera språkbruket.

[3] Se Nationalencyklopedins definition av *molntjänst*.

1.2 Syfte

Det huvudsakliga syftet med denna uppsats är att undersöka och redogöra för hur avtalsparterna vid tillhandahållandet av molntjänster regleras i EU:s dataskyddslagstiftning. Mer specifikt är syftet att identifiera och analysera hur ansvaret för personuppgifter, mellan molntjänstkund och molntjänstleverantör, regleras i GDPR.

I uppsatsen utreds de krav som ställs på ansvarsregleringen av personuppgifter enligt GDPR samt de faktorer gällande molntjänsternas utformning som påverkar hur ansvarsregleringen ska eller bör utformas.

Fokus ligger på ansvarsregleringen av personuppgiftsbehandling, som en del i personuppgiftsbiträdeavtalet eller annat avtal med motsvarande verkan och analysera detta i ljuset av den senaste rättsutvecklingen inom dataskydd.

Ett sekundärt syfte med uppsatsen är att belysa vilka juridiska problem som kan uppstå vid tillämpning av dataskyddslagstiftning på olika sorters molntjänster vad beträffar ansvar för personuppgiftsbehandlingar.

1.3 Frågeställningar

För att uppnå syftet kommer följande frågeställningar problematiseras och utredas i uppsatsen:

- Hur regleras ansvarsförhållandet mellan en molntjänstleverantör och dess kunder vad gäller personuppgiftshantering i molntjänsten utifrån GDPR?
- Kan utformningen av molntjänsten påverka hur ansvarssituationen bedöms?

1.4 Avgränsningar

Uppsatsen är avgränsad till att omfatta den nya dataskyddsförordningen (GDPR). Dataskyddsdirektivet (95/46/EG) samt tillhörande praxis tas upp i den omfattning det utgör tolkningsunderlag för den kommande lagstiftningen, d.v.s. där lagtexten har samma ordalydelse eller innebörd. Nationell lagstiftning som hör ihop med Dataskyddsdirektivet eller dataskyddsförordningen kommer inte tas upp.

Dataskyddsförordningen är tillämplig när personuppgifter om EU-medborgare eller individer som befinner sig inom EU behandlas. Utgångspunkten för uppsatsen är att detta rekvisit är uppfyllt och kommer inte beröras ytterligare. Utgångspunkten är således att GDPR är tillämpligt på de molntjänster som diskuteras i uppsatsen.

Uppsatsen kommer inte att beröra avtalsrättsliga aspekter och regleringar, utöver de regleringar i GDPR som har direkt koppling till ansvarsfördelningen som ska regleras i ett så kallat personuppgiftsbiträdeavtal eller avtal med motsvarande verkan.

Av utrymmesmässiga skäl kommer även andra begränsningar att göras. Upphovsrättsliga aspekter samt överföring av personuppgifter till leverantörer utanför EU kommer inte att beröras. Skribenten kommer inte heller att beröra vilka konsekvenser molntjänstsanvändningen kommer att medföra för de enskilda individerna vars personuppgifter behandlas. Uppsatsen avser endast att behandla juridiska personer som kunder till molntjänsterna, eftersom GDPR huvudsakligen tillämpas på juridiska personer.

1.5 Perspektiv, metod och teori

Rättsdogmatisk metod har använts i uppsatsen för att tolka och systematisera gällande rätt på området. Utgångspunkten för den rättsdogmatiska metoden är främst användandet av de allmänt accepterade rättskällorna, vilket ä förarbeten, lagtext, praxis och doktrin.[4] Rättskällorna i denna uppsats har använts i enlighet med rättskälleläran. Med detta förstås att rättskällorna granskats och samtidigt värderats utifrån dess rättskällevärde. Lagar, förarbeten och till viss del rättspraxis har därför använts för analys av den kommande rättsliga regleringen.

En skillnad som är värt att notera vid tillämpning av EU-rätt jämfört med en traditionell svensk rättsdogmatisk metod är att förarbeten har en begränsad rättslig ställning inom EU-rätten. Istället används så kallad *soft law*, bestående av icke-bindande juridiska dokument som utarbetats av olika organ inom EU, som källa för att tolka rättsakter och fastställa deras syften.[5]

GDPR som är en EU-rättslig rättsakt har gjort att även EU-rättslig metod har tillämpats i delar av uppsatsen genom att behandla EU:s rättsakter samt rättspraxis från EU-domstolen.[6]

Det perspektiv som präglar uppsatsen mest är ett framåtblickande perspektiv eftersom GDPR inte har börjat tillämpas än. Utöver det använder skribenten delar av ett rättsutvecklingsperspektiv för att tydliggöra gällande rätt på området. Genomgående används ett kritiskt förhållningssätt till materialet för att presentera en så objektiv och tydlig bild av ämnet som möjligt.

En annan viktig källa för tolkningsdata som ersätter lagförarbeten och bör beaktas noga är den inledning, även kallad preambel, som finns i början av

---

[4] Korling, Fredric & Zamboni, Mauro (red.), *Juridisk metodlära*, s. 21.

[5] Korling, Fredric & Zamboni, Mauro (red.), *Juridisk metodlära*, s. 127.

[6] Korling, Fredric & Zamboni, Mauro (red.), *Juridisk metodlära*, s. 109.

varje förordning och direktiv.[7] I inledningen anges i punktform en kortfattad förklaring av rättsaktens syften och vilka ställningstaganden som har tagits i beaktande inför rättsaktens antagande. Inledningen är inte bindande men kan ändå bidra med viktiga tolkningsdata genom att fastställa syftet med en viss reglering. Man kan säga att inledningen påminner om den funktion som lagförarbeten fyller i svensk rätt. För att tolka vissa bestämmelsers syften har därför förordningens ingress använts i uppsatsen.[8]

1.6 Forskningsläge

Uppsatsens grundar sig på GDPR som börjar tillämpas 25 maj 2018.[9] Av denna anledning är urvalet av doktrin på området begränsat vid tidpunkten för uppsatsens författande. I det urval som finns bör doktor Axel Freiherr von dem Bussche och Paul Voigt nämnas. De har gett ut boken "*The Eu General Data Protection Regulation: A Practical Guide".* Boken är huvudsakligen ämnad att ge råd för att praktiskt tillämpa GDPR men lämnar även en analys av lagstiftningen.

Varje medlemsland i EU har en egen tillsynsmyndighet, i Sverige är det Datainspektionen. De utfärdar informationsbroschyrer och vägledningar för allmänheten. Det är tillsynsmyndigheternas uppgift att bevaka efterlevnaden av Dataskyddsdirektivet och framöver dataskyddsförordningen och de har därav en vägledande ställning.

Rätten till personlig integritet är en grundläggande mänsklig rättighet vilket medför att det är ett viktigt rättsområde som har behandlats mycket, både nationellt och internationellt.[10] Några författare som berört ämnet är David Frydlinger och Tobias Edvardsson som har mångårig erfarenhet av

---

[7] Bernitz m.fl., *Finna rätt – Juristens källmaterial och arbetsmetoder,* s. 187.

[8] Bernitz m. fl., *Finna rätt – Juristens källmaterial och arbetsmetoder*, s. 73.

[9] Artikel 99.2 GDPR.

[10] Artikel 8 EKMR.

molntjänster och personuppgiftsfrågor. Deras bok ”*Molntjänster – juridik, affär och säkerhet*” avhandlar personuppgiftsfrågor i anknytning till molntjänster och är av stor relevans för uppsatsen ämne.

Artikel 29-gruppen har utkommit med vägledningar och uttalanden gällande behandling av personuppgifter i molntjänster samt ansvarsfördelning mellan personuppgiftsansvarig och personuppgiftsbiträde.

Sammantaget kan forskningsläget sägas vara på uppgång i och med det närliggande startdatumet för tillämpningen av GDPR. Det återstår att se vilken praxis och forskning som kommer på området. Stora delar av det som är skrivet kring molntjänster sedan tidigare stödjer sig på Dataskyddsdirektivet, och det finns viss bärighet i detta fortfarande. Det är dock inte en enkel avvägning för att avgöra hur mycket som fortfarande kommer vara tillämpligt efter 25 maj 2018.

Avsaknad av rättspraxis gällande ämnet, gör att det återstår tolkningsfrågor som ännu inte avgjorts av domstol eller som EU-kommissionen inte har uttalat sig om. Något som kan förväntas ske efter att GDPR börjar tillämpas.

1.7 Material

Som ovan angetts är urvalet av praxis och doktrin begränsat avseende uppsatsen ämne.

En stor del av de rättskällor som används i uppsatsen utgörs av yttranden från Artikel 29-gruppen. Artikel 29-gruppen är ett oberoende och rådgivande organ inom EU som arbetar uteslutande med frågor rörande dataskydd inom unionsrätten. Arbetsgruppen består av en företrädare för varje nationell tillsynsmyndighet i EU-medlemsstaterna, en företrädare för EU-kommissionen samt den europeiske datatillsynsmannen. Rättskällevärdet har viss begränsning och det är inte helt klart om det ska

ses som en rättskälla. Artikel 29-gruppens yttranden och utlåtanden stämmer ofta väl överens med hur EU:s institutioner tolkar EU-rätten och är i sammanhanget en lämplig källa eller åtminstone vägledande rättsligt material, då arbetsgruppens framställningar har fått ett betydande inflytande.[11]

1.8 Uppsatsens disposition

Det första kapitlet i uppsatsen är ett inledande kapitel som bland annat beskriver bakgrunden till ämnet, uppsatsens syfte och frågeställningar. I andra kapitlet presenteras molntjänster och dess definition. Vidare kommer den gällande rätten att avhandlas i det tredje kapitlet. Avslutningsvis, i det femte kapitlet, presenteras analysen av det som behandlats i uppsatsen i syfte att besvara frågeställningarna som angetts ovan.

[11] Bygrave, Lee A., *Data privacy law: an international perspective*, s. 174.

2 Molntjänster

Här presenteras hur molntjänster är uppbyggda och fungerar för att förstå vad de kan föranleda för juridiska frågor angående ansvarsfördelningen mellan personuppgiftsansvariga och personuppgiftsbiträde.

2.1 Användning av molntjänster

Molntjänster används mer och mer i vårt digitaliserade samhälle. Det finns en stor användargrupp både inom offentlig och privat sektor. På grund av den stora utvecklingen av digitala lösningar som sker finns det mängder av molntjänster på marknaden, både standardiserade likväl som hybridlösningar.

Det finns ekonomiska och affärsmässiga fördelar med molntjänster. Interna IT-resurser behöver inte vara lika avancerade samt kapaciteten för system minskar och den tekniska infrastrukturen inkluderar komponenter som lagrar data på annan plats. Molntjänster bidrar till en outsourcing av IT.[12] Det finns även säkerhetsaspekter kring molntjänster som gör att det är diskutabelt om det är till fördel eller nackdel för en kund att använda molntjänster. Samtidigt är det viktigt att molntjänsterna används på ett korrekt sätt som är förenligt med gällande lagstiftning. Här kommer regler om skydd för personuppgifter in, vilket redogörs för i avsnitt 3.

Risker som finns måste hanteras inför val av leverantör, genom beslut om vilka persondata som ska placeras i molntjänsten samt genom utformningen av avtalsrelationen.

[12] Hellström, *På molnfronten intet nytt? Vissa rättsliga aspekter på molntjänster*, s. 40.

Molntjänster är en sorts tjänst som ger tillgång till ett system utan att behöva installera hårdvara eller mjukvara. Tillgången till data som lagras i montjänster sker genom internet och lagras på servrar hos leverantören eller någon som den i sin tur anlitat. De signifikanta är att det inte kontrolleras av kunden utan det är leverantören som ger kunden tillgång genom internet, men den fysiska lagringen sker någon annanstans.

2.2 Definitionen av molntjänst

Genomgående i doktrin slås det fast att det finns ingen enhetlig definition av vad en molntjänst är. Dessutom saknas det en legal definition av vad en molntjänst är. Det finns således inte en universell definition som är gångbar, varken nationellt i Sverige, internationellt i EU eller övriga världen. En organisation som har preciserat begreppet är National Institute of Standard and Technology (NIST), som är en del av handelsdepartementet i USA och som arbetar med att stärka den amerikanska ekonomin genom att främja innovation och utveckling samt standardisera de teknologiska resultat som uppnås. Deras definition går under beteckningen *NIST-definitionen* och är den definitionen som fått störst acceptans, av denna anledning skribenten utgå från denna definition.[13]

Eftersom molntjänster är avancerade teknologiska konstruktioner, i de allra flesta fall, består *NIST-definitionen* av flera komponenter. Definitionen kan sammanfattas enligt följande;

” […] en modell för att vid behov möjliggöra allmänt tillgänglig och behändig nätverksaccess till en delad och gemensam mängd av konfigurerbara datorresurser (exempelvis nätverk, servrar, datalagring, datorprogram och tjänster) som snabbt

[13] Edvardsson, Tobias & Frydlinger, David, *Molntjänster: juridik, affär och säkerhet*, s. 21f.

kan göras tillgängliga och frigöras med minimal insats och utan direkt interaktion med molntjänstleverantören. ” [14]

De karaktäristiska drag som används som kriterier för att avgöra om en tjänst klassificeras som molntjänst, utifrån *NIST-definitionen*, redovisas närmare nedan.

Det närmsta man kan hitta en definition inom EU-rätten är Artikel 29-gruppens yttrande om molntjänster. De beskriver att molntjänster är tekniker och tjänstemodeller som fokuserar på internetbaserad användning och tillhandahållande av IT-system, processkapacitet, lagrings- och minnesutrymme.[15] Efter en omfattande genomgång av de rättsliga aspekterna kring molntjänster hänvisar Artikel 29-gruppen till delar av *NIST-definitionen.*[16]

För att vidare styrka hållbarheten i *NIST-definitionen*, kan nämnas att ENISA, EU:s nätverks- och informationssäkerhetsbyrå, hänvisar till definitionen i deras framställning gällande molntjänster inom den offentliga sektorn.[17]

2.2.1 Kännetecken för molntjänster

Enligt *NIST-definitionen* har en molntjänst fem karaktäristiska drag, som bedöms för att kunna avgöra om en tjänst utgör en molntjänst.
Kännetecknen för molntjänster är följande:

- tillgänglig genom självbetjäning vid behov,
- bred tillgänglighet via internet,

---

[14] Mell, Grance, The NIST definition of cloud computing, s. 2 (översättning till svenska av Edvardsson, Tobias & Frydlinger, David, *Molntjänster: juridik, affär och säkerhet*, s. 22).
[15] Artikel 29-gruppen, Yttrande 05/2012 om molntjänster (Cloud computing), s. 4.
[16] Artikel 29-gruppen, Yttrande 05/2012 om molntjänster (Cloud computing), s. 25.
[17] ENISA, *Security & Resilience in Governmental Clouds – Making an informed decision*, s. 46.

- sammanslagning av resurser,
- omgående (eller nästintill omgående) anpassning, och
- mätbar användning.[18]

Att molntjänsten är *tillgänglig genom självbetjäning vid behov* innebär att molntjänstanvändaren kan starta och stänga av de tjänster som finns i molntjänsten, för att smidigt anpassa utefter sin verksamhet, utan att kontakta en fysisk person.[19] En följd av att det råder utebliven kommunikation vid självbetjäning är att det finns begränsade möjligheter till avtalsförhandling, något som kan föranleda juridiska frågeställningar gällande ansvarsreglering mellan parterna.[20]

Bred tillgänglighet via internet avser de accesspunkter som en molntjänst kan nås genom. Det omfattar olika plattformar såsom bärbara datorer, surfplattor och mobiltelefoner samt stationära datorer. Det ska vidare innefatta att informationen är geografiskt obunden, d.v.s. tillgänglig oberoende av var du befinner dig.[21]

Sammanslagning av resurser går ut på att tillgodose flera användares behov genom samma infrastruktur. Mer konkret betyder det att kunder delar på kapaciteten och leverantören kan fördela resurserna dynamiskt, något som kunden inte märker av eller har kontroll över.[22] Den juridiska problematiken kring att kunden inte har vetskap kring var personuppgifterna lagras och hur det sker, aktualiseras tydligt här då det är svårt för kund att kontrollera att leverantören uppfyller instruktionerna samt att säkerhetsåtgärder vidtas.

Att en molntjänst har *omgående (eller nästintill omgående) anpassning* inbegriper att den automatiskt justerar sig efter kundens faktiska nyttjande,

---

[18] Edvardsson, Tobias & Frydlinger, David, *Molntjänster: juridik, affär och säkerhet*, s. 22.

[19] Mell, Grance, *The NIST definition of cloud computing*, s.2.

[20] Edvardsson, Tobias & Frydlinger, David, *Molntjänster: juridik, affär och säkerhet*, s. 23.

[21] Mell, Grance, *The NIST definition of cloud computing*, s.2.

[22] Edvardsson, Tobias & Frydlinger, David, *Molntjänster: juridik, affär och säkerhet*, s. 24.

med andra ord ökar och minskar resurserna direkt efter kundens behov. Detta möjliggör snabb skalbarhet utefter de resurser kunden disponerar.[23]

Mätbar användning betyder att molntjänstleverantören övervakar och dokumenterar automatiskt, i realtid, kundens faktiska förbrukning, vilket bidrar till en transparens för parterna och möjliggör att kunden enbart betalar för utnyttjade resurser.[24]

2.2.2 Molntjänstmodeller

Det finns en etablerad uppdelning av molntjänster som utgår ifrån vad det är som tillhandahålls. Metoden för kategoriseringen går under namnet SPI-modellen och delar in molntjänsterna i tre underkategorier:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Ovanstående uppdelning är en distinktion som även används inom EU.[25] I följande stycke kommer respektive del av SPI-modellen beskrivas närmare.

Software as a Service (datorprogram som en tjänst) är när kunden direkt använder molntjänstleverantörens datorprogram, system eller andra applikationstjänster som molntjänst.

Platform as a Service (platform som tjänst) är den formen av molntjänst som karaktäriseras av att kunden erhåller en utvecklingsplattform, där kunden själv kan utveckla och integrera program och applikationer. Denna variant kan användas av företag som vill utveckla viss programvara, men inte utveckla alla komponenter som behövs.

---

[23] Edvardsson, Tobias & Frydlinger, David, *Molntjänster: juridik, affär och säkerhet*, s. 24.

[24] Edvardsson, Tobias & Frydlinger, David, *Molntjänster: juridik, affär och säkerhet*, s. 25.

[25] Artikel 29-gruppen, Yttrande 05/2012 om molntjänster (Cloud computing), s.25ff.

Infrastructure as a Service (infrastruktur som tjänst) är när molntjänstleverantören tillhandahåller datorkapacitet vilket innefattar servrar, nätverksteknologi, lagring och datahallsutrymme. Kunden behöver därmed inte köpa in infrastruktur utan kan få tillgång till detta via en molntjänstleverantör. Utifrån infrastrukturen bygger sedan kunden upp sina egna program, nätverk och system.[26]

Det kan konstateras att det finns olika nivåer av molntjänster i form av komplexitet, beroende på vilket resursbehov kunden har. Det är inte ovanligt att molntjänstleverantörer är kunder till andra molntjänstleverantörer, av den enkla anledningen att de kan använda en molntjänst i form av *PaaS* eller *IaaS* för att ta fram och erbjuda program och applikationer genom *SaaS.* Faktum är att det leder till komplicerade partsförhållanden med flera inblandade aktörer. Att molntjänsten kan ha olika modeller, påverkar hur ansvaret ska regleras mellan parterna samt vilken roll de inträder, utifrån dataskyddslagstiftningens titlar, som redogörs för nedan.

Det florerar andra begrepp gällande modeller av molntjänster, dessa förefaller dock inte att tillföra något nytt, därav utesluts de i denna uppsats.

2.2.3 Molntjänsters distrubutionsmodeller

Utöver att molntjänster kan konstrueras på olika sätt går det dessutom att leverera dem på olika sätt. *NIST-definitionen* inkluderar fyra olika tillvägagångssätt genom vilka en molntjänst kan levereras och de kommer redogöras för nedan.

[26] Edvardsson, Tobias & Frydlinger, David, *Molntjänster: juridik, affär och säkerhet*, s. 25ff.

I det *publika molnet* (offentliga molntjänster) erbjuder en leverantör IT-resurser till allmänheten direkt via internet. Resurserna kan bestå av lagring eller program som kunderna, eller användarna, delar på. Offentliga molntjänster är exempelvis Facebook och Gmail. Det publika molnet kan erbjudas både kostnadsfritt och mot betalning.[27]

Privat moln kallas det leveranssätt som är utformat för att tillgodose en specifik kunds behov av IT-resurser. Molntjänsten som levereras som ett *privat moln* kan ägas av kunden, en extern leverantör eller en kombination av de föregående. Denna leveransmetod är anpassad för att kunna placeras antingen i kundens egna serverhall eller i leverantörens, beroende på vilken variant kunden efterfrågar.[28]

Gemensamma molntjänster eller *gemenskapsmoln* är en leveransmodell för en gemenskap av kunder, som delar på ett moln för sina molntjänster. Detta kräver att kunderna har likartade mål och syfte avseende användningen av molnet. Precis som privata moln kan molnet ägas av en av kunderna, gemensamt av alla kunderna, av en extern leverantör eller kombinationer av föregående.[29]

Hybrider av leveransmodeller eller *hybridmoln* är den leveransmodell som blir resultatet om man kombinerar två eller tre av de andra leveransmodellerna. De olika leveransmodellerna sätts upp separat och hålls intakta, för att integreras genom ett övergripande hybridmoln.[30]

---

[27] Edvardsson, Tobias & Frydlinger, David, *Molntjänster: juridik, affär och säkerhet*, s. 29.

[28] Liu m.fl, *NIST cloud computing reference architecture*, s. 10.

[29] Liu m.fl., *NIST cloud computing reference architecture*, s. 11.

[30] Liu m.fl, *NIST cloud computing reference architecture*, s. 12.

3 EU:s dataskyddslagstiftning

3.1 Rättsutveckling

Att reglera hantering av personuppgifter är en central fråga inom EU-rätten och de grundläggande syftena är att skydda medborgarnas personliga integritet, säkerställa en hög skyddsnivå för personuppgifter och samtidigt se till att underlätta överföring av data på EU:s inre marknad.[31]

Gällande rätt på dataskyddslagstiftningens område är Dataskyddsdirektivet, som infördes år 1995. Den 25 maj 2018, kommer dataskyddsförordningen (GDPR) börja tillämpas i samtliga EU-länder och därmed kommer Dataskyddsdirektivet upphävas.[32]

Båda rättsakterna har till syfte att harmonisera dataskydd och säkerställa enskildas personliga integritet. Då nivåerna av dataskydd har varierat inom EU och Dataskyddsdirektivet har införlivats med skilda tolkningar och tillämpningar inom unionen, ska GDPR säkra en enhetlig och hög skyddsnivå för personer i EU.[33]

Det följer av artikel 288 i Fördraget om europeiska unionens funktionssätt (FEUF) att en rättsakt i form av ett direktiv är endast bindande i den omfattningen att medlemsstaten ska uppnå det resultat som direktivet stadgar. Hur resultatet ska åstadkommas överlåter EU till varje enskild medlemsstat att avgöra, d.v.s. att implementera lagstiftningen i nationell rätt. Detta har lett till att Dataskyddsdirektivet, som ovan redogjorts för, inte har uppnått önskad harmoniseringseffekt.

---

[31] Ingresspunkt 2 och 10 Dataskyddsdirektivet samt skäl 1, 2 och 6 GDPR.

[32] Artikel 94 och artikel 99 GDPR.

[33] Skäl 3, 9 och 10 GDPR.

EU-domstolen har uttalat följande i mål C-101/01 *Bodil Lindqvist:*

”Harmoniseringen av de nämnda nationella lagstiftningarna inskränker sig således inte till en minimiharmonisering, utan leder till en i princip fullständig harmonisering. Det är i detta perspektiv som man skall se direktiv 95/46, som syftar till att säkerställa det fria flödet av personuppgifter och att samtidigt garantera en hög skyddsnivå för rättigheter och intressen för de personer som dessa uppgifter avser.”.[34]

Samma uttalande återfinns i de förenade målen C-468/10 *ANSEF* och C-469/10 *FECEMD*.[35] Båda rättsfallen rörde tolkning av Dataskyddsdirektivet. Det är tydligt att ett syfte med Dataskyddsdirektivet, som EU-domstolen uttalar, är att harmonisera personuppgiftsskyddet i EU. Att så inte har blivit fallet kan tydligt utläsas ur inledningen till GDPR.[36]

Skyddet av den personliga integriteten är också en del av rätten till privatliv i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR).[37]

3.2 GDPR

GDPR antogs den 27 april 2016 av Europaparlamentet och rådet. Förordningen trädde i kraft i samband med att den offentliggjordes i Europeiska unionens tidning, 25 maj samma år. Samtliga medlemsstater i EU fick således en implementeringsperiod på ungefär två år för att anpassa sig inför den nya lagstiftningen.[38] GDPR är till skillnad från direktivet

[34] C-101/01, Bodil Lindqvist mot Sverige, p.96.

[35] C-468/10 (ASNEF) och C-469/10 (FECEMD) mot Administración del Estado, p.29.

[36] Se skäl 7 GDPR.

[37] Artikel 8 EKMR.

[38] Artikel 99 GDPR.

bindande till hela sin omfattning och direkt tillämplig som lag i medlemsstaternas rättsordningar.[39]

Terminologin och begreppen som finns i Dataskyddsdirektivet kommer i stor utsträckning förbli samma i GDPR. De begrepp som är relevanta att klargöra för fortsättningen av denna uppsats är *personuppgiftsansvarig* och *personuppgiftsbiträde*. Det är benämningar på olika ansvarsroller som parterna kan inträda i, vilket kommer utredas i följande avsnitt.

Det huvudsakliga syftet med GDPR är att ytterligare harmonisera och effektivisera skyddet av personuppgifter för att förbättra den inre marknadens funktion i EU samt att öka den enskildes kontroll över sina personuppgifter.

3.3 Parterna

En molntjänst har minst två inblandade parter i avtalsförhållandet. Det är leverantören och kunden. Vad gäller de personuppgifter som behandlas i molntjänsten kan man ur ett personuppgiftsrättsligt perspektiv identifiera olika ansvarsroller. Det finns två olika ansvarsfunktioner som stadgas i GDPR. Den första är *personuppgiftsansvarig* och den andre är *personuppgiftsbiträde.*[40] Hur dessa roller förhåller sig till molntjänster ska redovisas närmare i följande avsnitt.

3.3.1 Personuppgiftsansvarig

Personuppgiftsansvarig är ett nytt begrepp i GDPR i förhållande till Dataskyddsdirektivet, där benämningen *registeransvarig* används.
I artikel 4.7 GDPR definieras begreppet *personuppgiftsansvarig* och det är en av två möjliga positioner som en avtalspart, vid tillhandahållande av

[39] Artikel 288 FEUF.

[40] Se Artikel 29-gruppen, Yttrande 05/2012 om molntjänster (Cloud computing).

molntjänst, kan inträda i. I artikel 24 GDPR stadgas ytterligare vad som innefattas i den personuppgiftsansvariges ansvar.

Artikel 4.7 GDPR lyder enligt följande:

”[…] en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt, […].”

Det som kännetecknar en *personuppgiftsansvarig* är att det är den part som bestämmer *ändamål* och *medel* med personuppgiftsbehandlingen. Det som avses med *ändamål* är syftet med behandlingen av personuppgifterna d.v.s. varför uppgifterna behandlas. Detta är något som inte kan delegeras vidare utan hänför sig till den personuppgiftsansvariges kompetens. Styr inte parten över ändamålet betyder det att den inte är personuppgiftsansvarig.

Med *medel* avses det tillvägagångsätt som personuppgifterna behandlas på. Det är något som kan delegeras genom avtal utan att ansvarsfördelningen förändras. Det kan exemplifieras genom att en molntjänstkund (personuppgiftsansvarig) kan överlåta till molntjänstleverantören att bestämma hur personuppgiftsbehandlingen ska ske rent tekniskt, utan att det för den delen gör leverantören till personuppgiftsansvarig. Tekniskt tillvägagångssätt inverkar inte på behandlingens ändamål. [41]

[41] Artikel 29-gruppen, Yttrande 1/2010 om begreppen registeransvarig och registerförare, s.13ff.

Den som bestämmer *medlen* för behandlingen blir endast ansvarig om det rör sig om väsentliga delar som avgör om behandlingen är tillåten, såsom vilka uppgifter som ska behandlas och under vilket tidsintervall.[42]

Enligt Artikel 29-gruppens yttrande finns det tre bedömningsgrunder som utvärderas för att avgöra om en part är personuppgiftsansvarig.
Det första är *uttrycklig behörighet* – det innebär att kompetensen att bestämma över en personuppgiftsbehandling följer uttryckligen av lag. Exempel på detta kan vara en myndighet som enligt registerförfattningar har krav på sig att utföra vissa personuppgiftsbehandlingar.

Den andra är *underförstådd behörighet* – rätten att kontrollera personuppgiftsbehandlingar följer indirekt av rättsliga bestämmelser eller rättspraxis.

Den tredje är *faktiskt inflytande* – kontrollen grundar sig i avtal eller annan dokumentation som rör aktörernas ansvarsförhållande. Verkligt personuppgiftsansvar kan vara skäl för kontroll även om det inte framgår av avtal, individernas förväntningar och uppfattning av personuppgiftsbehandlingen kan också ha betydelse för bedömningen.

3.3.2 Personuppgiftsbiträde

Den andra ansvarsrollen som en avtalspart kan inträda i är *personuppgiftsbiträde* vars definition återfinns i artikel 4.8 GDPR. Det är också ett nytt begrepp i förhållande till Dataskyddsdirektivet där begreppet *registerförare* används.

[42] Artikel 29-gruppen, Yttrande 1/2010 om begreppen registeransvarig och registerförare, s.14.

Artikel 4.8 GDPR har följande lydelse:

”[…] en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning […]”.

Personuppgiftsbiträdet ska således behandla personuppgifter för den personuppgiftsansvariges räkning, men har viss möjlighet att själv bestämma tekniska och organisatoriska *medel* för behandlingen.

I artikel 28 GDPR finns detaljerade beskrivningar av personuppgiftsbiträdets roll. En nyhet i GDPR är det självständiga ansvaret som faller på biträdet, något som inte finns i Dataskyddsdirektivet.

Den personuppgiftsansvarige ska enbart utse biträden som kan ge tillräckliga garantier för att personuppgiftsbehandlingen uppfyller GDPR:s krav. Dessutom krävs det ett skriftligt avtal mellan den personuppgiftsansvarige och biträdet innan personuppgifter delas. Detta avtal heter *personuppgiftsbiträdesavtal*.[43] Detta reglerar ansvaret mellan parterna gällande personuppgiftsbehandling och styr därför parternas agerande.

3.3.3 Gemensamt personuppgiftsansvariga

I det fall båda parterna, innefattande molntjänstens leverantör och kund, rättsligt betecknas som enskilda personuppgiftsansvariga – kommer de ses som *gemensamt personuppgiftsansvariga*. Denna ansvarskonstellation har till syfte att visa på att båda parterna besitter en roll som personuppgiftsansvarig.[44]

[43] Artikel 28 GDPR.

[44] Artikel 26 GDPR.

Det som är unikt för denna situation, när parterna är gemensamt personuppgiftsansvariga, är att de tillsammans fastställer *ändamål* och *medel* med personuppgiftsbehandlingen.[45]

Gemensamt personuppgiftsansvar kan exempelvis vara när ett moderbolag och ett dotterbolag (två enskilda juridiska personer) har ett gemensamt personalsystem (en molntjänst). Där sätter de gemensamt upp målen med behandlingen av personuppgifterna och det sker genom ett system (vilket ses som ett medel) som båda parterna styr över.

Ett *inbördes arrangemang* är GDPR:s uttryck för den reglering som ska ske av parternas personuppgiftsansvar. Det finns inga formkrav på det inbördes arrangemanget men det som kan utläsas i GDPR är att det ska vara ett tydligt ställningstagande angående personuppgiftsansvar som uppfyller GDPR:s krav.[46] En tolkning som har gjorts är ”[…] att ett sådant arrangemang bör dokumenteras och regleras inom ramen för ett skriftligt avtal.”. Ett sådant avtal kan benämnas *datadelningsavtal.*[47]

För att visa hur ansvaret för personuppgifter förhåller sig till molntjänster, kommer nästa avsnitt redogöra för molntjänsters funktioner i relation till ansvar för personuppgiftsbehandling.

3.4 Ansvarsreglering

Datainspektionen har uttalat att en molntjänstkund som använder en molntjänst för sin personuppgiftsbehandling är personuppgiftsansvarig och molntjänstleverantören, inklusive dennes underleverantörer, är personuppgiftsbiträden.[48] Att kunna särskilja ansvarsrollerna på detta sätt är inte helt oproblematiskt. Artikel 29-gruppen har i ett yttrande uttalat att för

[45] Skäl 79 GDPR.

[46] Skäl 79 GDPR.

[47] Juridisk publikation 2/2017 s.281.

[48] Datainspektionen, *Molntjänster och personuppgiftslagen,* s.1.

att avgöra om en part är ansvarig eller biträde måste man titta på omständigheterna i varje enskilt fall för att se vem som faktiskt bestämmer ändamål och medel för personuppgiftsbehandlingen.[49] Vem eller vilka av parterna som har rätt att bestämma över personuppgiftsbehandlingen avgörs av de faktiska omständigheterna i varje enskilt fall.[50]

3.4.1 Gemensamt personuppgiftsansvariga

Det är de personuppgiftsansvariga som har ansvar för att behandling av personuppgifter följer GDPR, både i relationen mellan parterna men också i de led där personuppgifterna lämnas vidare till andra parter. Det är upp till båda parterna att se till de skyldigheter som en personuppgiftsansvarig har enligt GDPR efterlevs.

Som nämnts ovan finns inget krav på avtal utan använder definitionen ”inbördes arrangemang” för att strukturera upp den gemensamma personuppgiftsbehandlingen.[51]

Datadelningsavtal är ett exempel på inbördes arrangemang för ansvarsreglering för gemensamt personuppgiftsansvariga.

3.4.2 Biträdessituation

Vid personuppgiftsbehandlingar utanför den egna organisationen ställer GDPR krav på den personuppgiftsansvarige att reglera sådan outsourcad[52]

---

[49] Artikel 29-gruppen, Yttrande 1/2010 om begreppen registeransvarig och registerförare, s.8ff.

[50] Kahn, Johan & Gustafsson, Fredrik, Juridisk publikation 2/2017, *Gemensamt personuppgiftsansvar – vanligare under GDPR?*, s.275.

[51] Artikel 26 GDPR.

[52] Det svenska begreppet är *uppdrag på entreprenad* d.v.s. en leverantör tillhandahåller en tjänst som tidigare sköttes internt.

behandling ”[…] genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt.”.[53] I detta avtal, även kallat *personuppgiftsbiträdesavtal* ska ”[…] föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter […]” anges.[54] Vidare ställs en rad krav på organisatoriska och tekniska säkerhetsåtgärder som måste finnas på plats och fastställas genom avtalet. Dessa krav motsvarar de krav som den personuppgiftsansvarige haft om behandlingen skett inom organisationen.[55]

Den personuppgiftsansvariga har huvudansvar för att behandling av personuppgifter följer GDPR samt ska ge instruktioner personuppgiftsbiträdet. Biträdet får inte behandla personuppgifter som inte följer av instruktionerna från den ansvarige. Biträdets ansvar ska regleras i ett så kallat *personuppgiftsbiträdesavtal.* Personuppgiftsbiträden kommer kunna hållas ansvariga gentemot individer de behandlat data om samt åläggas administrativa sanktionsavgifter.[56]

Om biträdet går utöver sina instruktioner, behandlar de inte längre personuppgifter för någon annans räkning och ses i den situationen som egna personuppgiftsansvariga och dessutom kan behandlingen vara otillåten om det inte finns en laglig grund för behandlingen.[57]

En molntjänstleverantör har i många fall underleverantörer som underhåller och sköter driften av vissa komponenter i molntjänsten för att kunna effektivisera molntjänsten. Underleverantörerna kallas för underbiträden och ansvar för personuppgifter de tar del av behöver även regleras. Det kan

[53] Artikel 28.3 GDPR.

[54] Artikel 28.3 GDPR.

[55] Se Artikel 28.3 a-c och e-h GDPR.

[56] Artikel 82.1 GDPR.

[57] Artikel 6 GDPR.

därför i många fall bli kedjor av avtal i olika led för att varje aktör utför viss personuppgiftsbehandling åt en annan.[58]

I slutändan är det tillsynsmyndigheterna i medlemsstaterna och ytterst EU-domstolen som avgör hur rollerna som personuppgiftsbiträde och personuppgiftsansvarig ska tolkas. De uppstramade kraven och höga sanktionsavgifterna är tydliga incitament för att uppfylla GDPR.

3.5 Molntjänstens utformning påverkar ansvarsregleringen

Det finns situationer där molntjänstleverantören inte styr ändamål och medel med personuppgiftsbehandlingen i molnet och därav ses som personuppgiftsbiträde. I verkligheten kan det vara så att utformningen av molntjänsten d.v.s. vilken molntjänstmodell som används kan inverka på vilken ansvarsroll som leverantören får.

Det går att ifrågasätta om alla molntjänstleverantörer verkligen är biträden. Beroende på vilken molntjänstmodell används har leverantören olika inflytande över den data som kunden för in i molntjänsten och det är det som styr vilken ansvarsposition leverantören får. Skillnaden kan illustreras med följande exempel:

En leverantör av en IaaS-molntjänst i form av en digital infrastruktur och processorkraft har liten, om ens någon, kontakt med kundens data i molntjänsten. Däremot har en SaaS-molntjänstleverantör tillgång till och möjlighet att styra över kundens data i större utsträckning p.g.a. att leverantören hanterar tjänsten mer ingående. I dessa olika scenarion kommer ansvarsrollen för leverantören troligen bedömas olika. I det första fallet där inflytandet över datan är liten ses leverantören med stor sannolikhet som ett

[58] Artikel 28 GDPR.

biträde, medan i det andra fallet är det mer tydligt att leverantören kan kontrollera data och eventuellt ska ses som ansvarig.[59]

För att klargöra en del av problematiken är svårigheten att avgöra hur ansvarsrollerna ska tilldelas när flera aktörer är inblandade i samma eller närliggande behandlingar av personuppgifter, i ljuset av denna uppsatsen är ett sådant typexempel molntjänster.

Det kan i många fall bli komplexa utredningar för att avgöra vilken ansvarsroll en part har, eller vill ha för den delen. Avtalssituationen är inte oproblematisk.

3.6 Molntjänster och GDPR

Det kan konstateras att GDPR har ett stort territoriellt tillämpningsområde, vilket medför att alla molntjänstleverantörer vars kunder behandlar data om EU-medborgare eller personer som vistas inom EU:s gränser kommer behöva anpassa sig och se till att det finns ett *personuppgiftsbiträdesavtal* eller *datadelningsavtal* på plats som reglerar ansvaret för persondata.[60]

I många fall är personuppgiftsbehandling nödvändig för att upprätthålla åtaganden gentemot en avtalspart. Däremot medför all personuppgiftsbehandling dock samtidigt risker för intrång i den enskildes personliga integritet. Med anledning av det finns det ett behov av reglering för vilka personuppgifter som får behandlas och mer specifikt under vilka förutsättningar.[61]

---

[59] Hon m.fl., *Who is responsible for "personal data " in cloud computing? – The cloud of the unknowing*, s.11.

[60] Artikel 3 GDPR.

[61] SOU 2016:65, s 33.

Molntjänster, som det ovan har redovisats om, används mer frekvent hela tiden. Det finns en hel del juridiska ställningstaganden att fundera kring vid inköp och tillhandahållande av molntjänster.[62]

Grunden i GDPR är att individer ska få stärkt skydd för sin integritet och det ska förverkligas genom att de aktörer som behandlar deras personuppgifter behöver bland annat följa instruktioner och vidta säkerhetsåtgärder, för att behandla uppgifterna på ett lagligt och säkert sätt.

Personuppgiftsregleringen i EU kräver att aktören som behandlar personuppgifterna behåller kontrollen över dessa även om de används i en molntjänst, för att säkerställa skydd för den personliga integriteten.

Definitionen av personuppgifter, som omnämns i inledningen, har utökats något i förhållande till Dataskyddsdirektivet. Det som har tillkommit är att lokaliseringsuppgifter och onlineidentifikationer uttryckligen har angetts falla inom definitionen av vad en personuppgift är. Det visar på att lagstiftningen har försökt anpassa sig för den tekniska utvecklingen som skett sedan Dataskyddsdirektivet introducerades.[63]

[62] Edvardsson, Tobias & Frydlinger, David, *Molntjänster: juridik, affär och säkerhet*, s. 105.

[63] Artikel 4.1 GDPR.

4 Analys

För att återkoppla till uppsatsen frågeställning kan jag konstatera att det finns en gråzon gällande ansvarsregleringen mellan parterna för personuppgifter som behandlas i en molntjänst. På grund av att det finns en gränsdragningsproblematik gällande de begrepp som tillämpas. Här åsyftar jag särskilt begreppen medel och ändamål. Dessa begrepp har ingen uttömmande definition och får därför tolkas utifrån sammanhanget i varje enskilt fall.

Att skriftligt reglera ansvaret för personuppgifter i molntjänster är i vissa fall ett krav, när det gäller biträdessituationer, och andra fall, vid gemensamt personuppgiftsansvar, rekommenderat.

Det personuppgiftsansvar som ska regleras mellan ett personuppgiftsbiträde och en personuppgiftsansvarig får inte delegeras. Det finns ett krav på att enbart godkända underbiträden får anlitas, detta för att ytterligare behålla skyddet för personuppgifterna och inte missta kontroll. Personuppgiftsbiträden har samma juridiska ansvar som den personuppgiftsansvariga gentemot den enskilda individen och tillsynsmyndigheten.

Det som har visats är att det finns två olika sätt att reglera ansvaret beroende på vilken form av personuppgiftsutbyte som sker mellan parterna. Å ena sidan, ska en ansvarig lämna över uppgifter till en annan part som ska behandla dessa för den ansvarigas räkning, detta kallas biträdessituation. Denna avtalsreglering ska enligt GDPR regleras genom ett personuppgiftsbiträdesavtal. Å andra sidan finns situationen där en personuppgiftsansvarig tillsammans med en annan part bestämmer ändamål och medel för personuppgiftsbehandlingarna och därav ses som gemensamt personuppgiftsansvariga. Där krävs ett inbördes arrangemang där parterna reglerar ansvaret gällande den persondata som behandlas i molntjänsten.

Det uppstå oklara situationer huruvida molntjänstens leverantör är biträde eller ansvarig. För även om utgångspunkten är att leverantören är personuppgiftsbiträde och kunden är personuppgiftsansvarig, finns det undantag till denna utgångspunkt.

Beroende på vilken sorts molntjänst det handlar om kommer utfallet att se annorlunda ut. Molntjänsten utformning spelar en avgörande roll för vilken ansvarsposition som leverantören hamnar i. Molntjänstkunden är alltid personuppgiftsansvarig för den data den lägger in i molntjänsten. Molntjänstleverantörens ansvarssituation är beroende av hur mycket kontroll denne har över personuppgifterna som finns i molntjänsten. Exempel på olika sorters kontroll är radering, analysering och ändring av personuppgifterna. Därav anser jag att det är visat genom denna uppsats att molntjänstens sammansättning och funktion påverkar utfallet av ansvarssituationen gällande personuppgifterna i molntjänsten.

Det som är komplext är att montjänstleverantören kan ha visst inflytande över personuppgiftsbehandlingen i molntjänsten, men det är inte klart var gränsen går för när dennes faktiska kontroll bedöms utgöra grund för att juridiskt anses som personuppgiftsansvarig. En annan aspekt som är värd att belysa är att det finns de molntjänstleverantörer som inte vill bli beordrade eller instruerade av personuppgiftsansvarig för hur data i molntjänsten ska hanteras. Samtidigt finns det en säkerhetsaspekt i att kunden bestämmer mål och medel för personuppgiftsbehandlingen och leverantören kan inte påverka detta. För det kan kännas otryggt, både för individer och molntjänstkunden, om molntjänstleverantörer kan anses personuppgiftsansvariga i alla situationer och det inte har reglerats eller reflekterats kring.

Ett biträde kan i viss utsträckning enskilt bestämma de tekniska och organisatoriska medlen som ska gälla för personuppgiftsbehandlingen. Om så inte hade varit fallet hade det nästintill varit omöjligt att reglera ansvaret

mellan biträdet och den ansvarige p.g.a. att det skulle kräva en enorm detaljnivå på informationen i avtalet mellan parterna.

Det är inte självklart hur gränsdragningen ska ske gällande vilken ansvarsroll en leverantör ska inträda vid tillhandahållande av molntjänster. Det går inte att sortera olika molntjänster i olika fack och kategorisera ansvarspositionen utifrån det utan det som krävs är en bedömning av molntjänstens faktiska funktion och parternas kontroll av personuppgifterna i det enskilda fallet.

Den som en gång varit personuppgiftsansvarig för en viss personuppgiftsbehandling kan inte sluta vara ansvarig för detta, det kan endast ske om personuppgiftsbehandlingen helt avslutas i verksamheten. I det fall en personuppgiftsansvarig lämnar över personuppgifter till en annan aktör kommer denne därför inte sluta vara personuppgiftsansvarig. Den mottagande parten inträder antingen i rollen som biträde, och behandlar personuppgifterna åt den ansvariges räkning vilket ska regleras med ett personuppgiftsbiträdesavtal, eller rollen som ansvarig och då kommer parterna ses som gemensamt personuppgiftsansvariga och det ska regleras genom ett inbördes arrangemang.

Innehållet i avtalet mellan parterna är därför viktigt och kan få stor påverkan på parternas avtalsrelation samt hur molntjänsten ska användas. Av betydelse för hur avtalsrelationen ska utformas är kraven på att den ansvarige ska se till att biträdet ställer tillräckliga garantier att GDPR:s regler uppfylls innan denne lämnar över personuppgifter till biträdet.

Det kan spekuleras i om det är eftersträvansvärt att rättsligt ses som ansvarig för att bibehålla större kontroll vad gäller personuppgiftsbehandlingen. Min egna tolkning av detta är att det skiljer sig från fall till fall, utefter vilken sorts molntjänst som det rör.

En återkommande sak som jag harförsökt belysa är att det finns en kvarstående oklarhet huruvida den lagstiftning som finns på området är tillräcklig eller om det finns det för stort tolkningsutrymme för att göra lagstiftningen och dess tillämpning effektiv. I och med förordningens utökade territoriella tillämpningsområde anser jag att förordningen är bättre anpassad för molntjänster än tidigare lagstiftning.

Ett effektivt skydd av personuppgifter i molntjänster förutsätter att parternas ansvar är utrett. Det som står klart är att det är en viktig del att reglera ansvaret för personuppgifterna i molntjänstavtalet för att uppfylla kraven i GDPR, vilket inte ter sig vara så enkelt i alla situationer.

Jag kan se ett tydligt mål i GDPR att strama upp kraven och se till att ansvarsregleringarna hanteras under ordnade former. Det är vad som krävs för att personuppgifter ska behandlas med respekt och försiktighet.

Att avgöra ansvarsrollerna kan vara både tidsödande men också juridiskt och tekniskt komplext. Det kräver både juridiska och tekniska kunskaper för att reda ut hur en molntjänst fungerar och hur den använder sig av personliga data. Uppsatsen påvisar att lagstiftningen inte ger mycket vägledning kring hur aktörer ska reglera ansvar och inte heller hur en molntjänst ska tolkas.

Käll- och litteraturförteckning

Källor

Tryckta källor

Offentligt tryck

Sverige

Utredningsbetänkanden

SOU 2016:65 Ett samlat ansvar för tillsyn över den personliga integriteten.

EU

Vägledning, yttranden och rekommendationer

Artikel 29-gruppen, Yttrande 1/2010 om begreppen registeransvarig och registerförare (on the concepts of "controller" and "processor"), WP 169, antagen 16 februari 2010.

Artikel 29-gruppen, Yttrande 05/2012 om molntjänster (on Cloud Computing), WP 196, antagen 1 juli 2012.

ENISA; Catteddu, Daniele, *Security & Resilience in Governmental Clouds – Making an informed decision*, 2011.

Mell, Grance, The NIST definition of cloud computing, 2011.

Elektroniska källor

Datainspektionen, *Molntjänster och personuppgiftslagen,* oktober 2016, https://www.datainspektionen.se/Documents/faktablad-molntjanster.pdf (hämtad 2018-05-10).

Nationalencyklopedin, *datamolnet,* http://www.ne.se.ludwig.lub.lu.se/uppslagsverk/encyklopedi/lång/molnet (hämtad 2018-04-22).

Litteratur

Bygrave, Lee A., *Data privacy law: an international perspective*, First edition., Oxford, United Kingdom, 2014.

Edvardsson, Tobias & Frydlinger, David, *Molntjänster: juridik, affär och säkerhet*, 1. uppl., Norstedts juridik, Stockholm, 2013.

Hellström, Roger, *På molnfronten intet nytt? Vissa rättsliga aspekter på molntjänster,* Ny juridik 2:2011 s.37.

Hon, W K, Millard, C, Walden, I, *Who is responsible for 'personal data' in cloud computing? – The cloud of the unknowing*, Part 2, International Data Privacy Law, vol. 2, nr. 1, februari 2012.

Liu m.fl, *NIST cloud computing reference architecture,* 2011.

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

Korling, Fredric & Zamboni, Mauro (red.), *Juridisk metodlära*, 1. uppl., Studentlitteratur, Lund, 2013.

Voigt, Paul & von dem Bussche, Axel, *The EU general data protection regulation (GDPR): a practical guide,* Cham, 2017.

Rättsfallsförteckning

EU-domstolen

C-101/01, Bodil Lindqvist mot Sverige, EU:C:2003:596.

C-468/10 och C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) och Federación de Comercio Electrónico y Marketing Directo (FECEMD) mot Administración del Estado, EU:C:2011:777.