



LUNDS UNIVERSITET

Ekonomihögskolan

Institutionen för informatik

Personuppgifter i molnet

Utmaningar ur ett tekniskt och juridiskt perspektiv

Kandidatuppsats 15 hp, kurs SYSK02 i informationssystem
Framlagd 25 maj 2016

Författare: Fredrik Lindahl
Olof Kindblad

Handledare: Odd Steen

Examinatorer: Björn Johansson
Anders Svensson

Personuppgifter i molnet: Utmaningar ur ett tekniskt och juridiskt perspektiv

Författare: Fredrik Lindahl och Olof Kindblad

Utgivare: Inst. för informatik, Ekonomihögskolan, Lund universitet

Dokumenttyp: Kandidatuppsats

Antal sidor: 59

Slutseminarium: 25 maj 2016

Nyckelord: Datormoln, personuppgifter, informationslagring, databehandling, utmaningar

Sammanfattning:

Med en växande global infrastruktur blir det allt vanligare att verksamheter använder olika typer av molntjänster för att underlätta sitt dagliga arbete. För myndigheter, kommuner och andra verksamheter som utnyttjar dessa tjänster till personuppgiftslagring finns det en komplexitet kring hur de ska förhålla sig till lagstiftning och teknik. I den här studien behandlas detta problemområde genom att undersöka legala och tekniska utmaningar förenade med att lagra personuppgifter i molntjänster för svenska verksamheter. En kvalitativ studie har genomförts där resultatet visade på att behandling av personuppgifter i molntjänster för med sig komplikationer eftersom det är en geografiskt gränsöverskridande teknik som lagstiftningen ännu inte hittat en tillfredsställande lösning på. Vår studie fann att den största juridiska utmaningen främst är att kunna navigera inom en föråldrad lagstiftning samt lösa problematiken kring lagring i tredje land (land utanför EU/EES). Vidare pekar resultatet på att de tekniska utmaningarna med att nyttja molntjänster vid personuppgiftslagring för en verksamhet främst är kopplade till verksamhetens möjlighet att bevara uppgifternas integritet, kontrollera tillgång och behörighet samt säkerhetsställa att molntjänstleverantören och eventuella underleverantörer har adekvata säkerhetsskydd.

Innehåll

1	Introduktion.....	1
1.1	Bakgrund	1
1.2	Problem.....	2
1.3	Forskningsfråga	3
1.4	Syfte.....	4
1.5	Avgränsningar	4
1.6	Struktur	4
2	Litteraturgenomgång	5
2.1	Personuppgifter.....	5
2.1.1	Definition av personuppgift	5
2.1.2	Personuppgiftslagen	5
2.2	Molnet.....	6
2.2.1	Definition av ett datormoln	6
2.2.2	Molntjänsttyper	6
2.2.3	Varför använda sig av molntjänster?.....	7
2.2.4	Hur lagras data i ett moln?	9
2.2.5	Tekniska risker med molnlagring.....	10
2.3	Personuppgifter i molnet	10
2.3.1	Molnlagring av personuppgifter.....	10
2.3.2	Safe Harbour	12
2.3.3	Privacy Shield	12
2.3.4	Juridiska risker med molnlagring av personuppgifter.....	12
3	Teoretiskt ramverk	14
3.1	Litteratururval	14
3.2	Identifierade utmaningar.....	16
4	Metod	17
4.1	Metodval	17
4.1.1	Kvalitativa intervjuer.....	17
4.1.2	Kvantitativ sekundärdata.....	17
4.2	Urval	18
4.3	Intervjugenomförande	18
4.3.1	Intervjuguidens uppförande.....	19
4.4	Intervjuanalys	20
4.5	Undersökningskvalitet	20
4.5.1	Validitet.....	20

4.5.2	Reliabilitet	21
4.6	Etik.....	22
5	Resultat	23
5.1	Presentation av kvalitativ empiristudie.....	23
5.2	Integritet.....	23
5.2.1	Kravställningar ur ett integritetsperspektiv	23
5.2.2	Att lagra data i tredje land	24
5.2.3	Transparens hos molntjänstleverantör.....	24
5.3	Datasäkerhet	25
5.3.1	Kontroll och uppföljning av hur data lagras.....	25
5.3.2	Urvalsprocess som garanterar att rätt data lagras	25
5.4	Regelverk.....	25
5.4.1	En juridisk komplexitet	25
5.4.2	Avtal och analysprocess	26
5.4.3	Sammanfattning av statistik	27
5.4.4	Möjlighet till förhandsgranskning.....	27
5.4.5	Skillnader privat kontra offentlig verksamhet.....	27
5.5	Drift och kommunikation	28
5.5.1	Kommunikation med molntjänstleverantör.....	28
5.5.2	Säkerhetskopieringshantering och rätten att bli glömd	28
5.6	Sammanfattning av resultat	28
6	Diskussion.....	30
6.1	Dataintegritet	30
6.2	Datasäkerhet	30
6.3	Regelverk.....	31
6.4	Drift och kommunikation	31
7	Slutsats	33
7.1	Rekommendation för vidare forskning.....	34
8	Appendix.....	35
8.1	Intervjuguide.....	35
8.2	Sekundärdata	36
8.3	Intervjutranskribering	39
8.3.1	Malmö Stad	39
8.3.2	Helsingborgs Stad	45
8.3.3	Datainspektionen	48
8.3.4	LDC	53

8.3.5	SUNET	55
Referenser.....		57

Figurer

Figur 1, Molnets lager (Sosinsky, 2012)

7

Tabeller

Tabell 1, Identifierade utmaningar	16
Tabell 2, Intervjupersoner	23

1 Introduktion

Följande stycke introducerar bakgrunden till studien samt behandlar forskningsfrågan och dess avgränsningar.

1.1 Bakgrund

I takt med att världens digitala infrastruktur blivit allt mer omfattande, stabil och tillåtit större överföringshastigheter har lagring och hantering av data i allt större omfattning flyttats från lokala datacenter till det så kallade datormolnet. Ett datormoln är ett teknologiskt ramverk som via Internet möjliggör att tjänster som infrastruktur, plattform och mjukvara ut-kontrakteras till extern part i form av en molnleverantör. Det finns idag ett flertal populära molntjänster som används av både privatpersoner och företag. Datormoln är antingen privata eller publika, där privata moln innebär att kunden köper in molnets källkod och själv ansvarar för att driva molnet på egen hårdvara medan publika moln innefattas av att kunden nyttjar hela molnet och dess olika funktioner som en tjänst (Sosinsky, 2012). Traditionellt sett hanterar och förvaltar verksamheter datalagring och mjukvara lokalt i egen infrastruktur via egna system (Sosinsky, 2012) och att, i kontrast till kraftfulla persondatorer eller konventionella lokala datacenter, kunna nyttja molntjänster innebär en rad olika möjligheter för en organisation; möjligheter som för med sig fördelar såväl som nackdelar. Exempelvis kan molnet innebära fördelar ur ett resursperspektiv vad gäller drift, underhåll och minskat krav på personalkompetens men också vad gäller ökad skalabilitet och funktionalitet (Marston, Li, Bandyopadhyay, Zhang & Ghalsasi, 2010). Svenska myndigheter svarade i en enkätundersökning genomförd av Pensionsmyndigheten att deras två främsta motiv för att implementera molntjänster är minskade kostnader och ökad flexibilitet (Appendix 8.2, tabell 4). Vidare kan en introduktion av molntjänster inom en verksamhet också medföra svårigheter ur ett organisatoriskt perspektiv. Flera länders lagstiftare världen över ställer höga krav på hur personuppgifter får lov att lagras, exempelvis finns det ett intresse att behålla personuppgifter inom vissa specifika länder vilket bland annat kan vara beroende på det egna landets politiska ställning till andra länder (Avram, 2014). Vidare innebär en verksamhets transformation till molnet en process kantad inte uteslutande av juridiska utmaningar utan även frågetecken gällande säkerhet och pålitlighet ur ett tekniskt perspektiv (Avram, 2014).

Användandet av olika molntjänster inom verksamheter ökar stadigt och enligt statistik från Eurostat använder sig idag nästan 20 procent av alla företag inom EU med över tio anställda av någon typ av molntjänst. Avgränsas statistiken till företag inom Norden visar det sig att

drygt 40 procent av verksamheter använder sig av någon form av molntjänst (Eurostat, 2014). Konsultbolaget Gartner, vilket sysslar med bland annat branschspaning, uppskattar att 50 procent av organisationer världen över kommer att nyttja någon typ av blandad molnlösning år 2017 (Stamford, 2013). Svenska myndigheter är flitiga användare av molntjänsttypen SaaS (Software as a Service) då cirka 78 procent använder sig av en sådan lösning idag (Appendix 8.2, tabell 3) vilket understryker den betydelse molntjänster har. Vidare behandlar drygt hälften av svenska myndigheter personuppgifter i molntjänster (Appendix 8.2, tabell 5). Samtidigt som användandet av molntjänster expanderar genomförs det stora förändringar kring lagring och behandling av personuppgifter får utföras. 2018 kommer en ny europeisk dataskyddsreform att träda i kraft vilken bland annat stärker individens rätt till personlig integritet. Reformen kommer att rita om kartan för hur verksamheter inom EU får lov att använda molntjänster för lagring av personuppgifter, genom att bland annat ställa högre krav på molntjänstleverantörer, exempelvis när det gäller radering av data och den så kallade principen "rätten till att bli glömd" (European Commission, 2015).

1.2 Problem

Att för en organisation migrera sin lokala IT-verksamhet till molnet är ingen självklar process, framförallt inte om lagring av personuppgifter förekommer. EU-domstolen förklarade den sjätte oktober 2015 regeldirektivet "Safe Harbor" ogiltigt, ett avtal som tidigare tillät överföring av personuppgiftsdata till så kallat tredje land utanför EU/EES (Court of Justice of the European Union, 2015). Safe Harbour-avtalet gjorde det möjligt för europeiska organisationer att sluta avtal med amerikanska molntjänstleverantörer, vilket via avtalet kunde garantera det adekvata skydd som det europeiska datalagringsdirektivet krävde (Europaparlamentet, 1995). Eftersom de flesta stora molntjänstleverantörer har sin verksamhet i USA var Safe Harbour ett populärt avtal att nyttja, i syfte att förenkla processen vid val av molntjänster där personuppgiftslagring kunde förekomma. Vid EU-domstolens ogiltigförklarande av avtalet revs alltså bestämmelsen upp, vilket orsakade frågetecken kring hur organisationer i framtiden ska gå tillväga för att kunna anlita molntjänstleverantörer från tredje land på ett sådant sätt att lagring av personuppgifter ryms inom europeisk och nationell lagstiftning. Eftersom en av molnets mest fundamentala funktioner innebär att data lagras hos extern part, uppstår det, som ett resultat av landsgränsöverskridande dataförbindelser, frågor av teknisk och juridisk aspekt förenat med den här processen.

Ale kommun i Västra Götaland fick 2014 besked av Datainspektionen om att deras avtal med Microsoft gällande användandet av Microsoft Office 365, ett populärt molntjänstalternativ till Microsoft Office, inte var förenligt med rådande lagstiftning (Datainspektionen, 2014). Ale kommun hade i frågan självmant begärt en granskning av avtalet vilket sedan Datainspektionen underkände eftersom Ale kommun inte kunde kontrollera och verifiera personuppgiftsdans fysiska lagringsplats, det vill säga den geografiska plats för den enhet som lagrar datan, på biträdet, det vill säga Microsoft, samt eventuella underleverantörer anlitade av biträdet. Ale kommun rättande senare till de punkter som Datainspektionen påvisat i granskningen, men händelsen fick stort uppslag i media eftersom det tydligt visade på en av svårigheterna vid

tecknande av molntjänstavtal. Datainspektionens utlåtande betyder i praktiken att företag och myndigheter som hanterar personuppgifter måste genomföra ett omfattande förhandsarbete vid val av molntjänst för att kunna säkerhetsställa att leverantören uppfyller de säkerhetskrav som lagstiftningen ställer. Problematiken kring vilka åtgärder som krävs av en organisation inför en övergång till molntjänster där persondata kan lagras ter sig vara relativt komplex och det finns därför också en möjlig risk att verksamheter drar sig för att undersöka möjligheten att använda molntjänster. Som ett resultat av komplexiteten kring nyttjandet av molntjänster, där lagring av personuppgifter kan förekomma, riskerar alltså verksamhetens ansträngningar att mynna ut i en process som dels är mycket kostsam och dels kanske i slutändan bryter mot lagstiftningen.

Enligt en enkätundersökning genomförd av Pensionsmyndigheten framgår det att svenska myndigheter generellt har en relativt begränsad erfarenhet av molntjänster överlag, men i synnerhet vad gäller just PaaS- och IaaS-tjänster. 60 procent av myndigheterna sade sig ha ingen erfarenhet av dessa två tjänsttyper och ytterligare 20 procent sade sig ha liten erfarenhet. Den tjänsttyp vilken myndigheter säger sig ha mest erfarenhet av är SaaS-tjänster där drygt 40 procent av myndigheterna sade sig ha medelgod erfarenhet (Appendix 8.2, tabell 2).

Sveriges myndigheter upplever flera utmaningar när det gäller möjligheten att transformera utvalda delar av sin IT-verksamhet från egna lösningar till molnbaserade tjänster (Pensionsmyndigheten, 2016a). Enligt samma rapport från Pensionsmyndigheten finns det en rad olika frågetecken vad gäller lagring av personuppgifter, både ur ett integritetsperspektiv, datasäkerhetsperspektiv samt ur ett juridiskt perspektiv. Som största upplevda hinder för att använda molntjänster uppges i rapporten säkerhetsrelaterade frågor samt oklarheter kring juridiska förutsättningar för nyttjande av molntjänster (Pensionsmyndigheten, 2016a). Enligt ett utlåtande från Datainspektionen vid tillsyn av IT-företaget Brevos, numera Kivra, användande av molntjänster, uppgavs det att företaget inte hade kunskap om vilka bolag som behandlar personuppgifter för dess räkning och således bröt mot personuppgiftslagen. Eftersom personuppgiftslagen gäller för verksamheter såväl inom den offentliga som den privata sektorn är det därför en problematik som samtliga svenska verksamheter möter vid lagring av personuppgifter i molntjänster (Datainspektionen, 2011).

1.3 Forskningsfråga

Forskningsfrågan har formulerats i syfte att identifiera och beskriva de utmaningar som finns för en verksamhet vid användande av molntjänst i samband med lagring av personuppgifter. Den forskningsfråga som ställts lyder därför som följer:

Vilka är de tekniska och juridiska utmaningarna för svenska verksamheter vid lagring av personuppgifter i molntjänster?

1.4 Syfte

Syftet med studien är att deskriptivt identifiera de utmaningar som genom bred empiri anses vara utmanade för en verksamhet som vill nyttja eller implementera en molntjänster som innefattar någon form av datalagring av personuppgifter.

1.5 Avgränsningar

Studien kommer inte belysa någon utvald typ av molntjänst eller molntjänstleverantör, utan istället undersöka de tekniska och juridiska krav vilka en kund måste ställa på en leverantör av en molntjänsttyp där lagring av persondata kan förekomma. Det tekniska området avgränsas till molntjänster på publika moln som innefattar någon typ av datalagring samt behandling av lagrad data, det vill säga dataoperationer som innebär skriva, läsa, spara och radera. Studien utgår från ett svenskt perspektiv och därmed svensk lagstiftning och praxis. Som ett resultat av Sveriges medlemskap i EU och den globala teknikindustrins geografiska koncentration kommer studien även beröra Sveriges förbindelse med EU/EES samt USA.

1.6 Struktur

Studiens struktur innefattar en forskningsprocess vilken inleds med en introduktion av området, dess problem samt forskningsfråga och avgränsningar. Vidare innehåller studien en djupgående litteraturgenomgång vilken i detalj beskriver ämnesområden och teknik relevant för forskningsfrågan, vilket tillsammans formar studiens teoretiska ramverk. I metodavsnittet beskrivs de tekniker som använts i syfte att genomföra insamling av empirisk data samt en kritisk granskning av den här processen i förhållande till intervju effekter och datans trovärdighet. Studien presenterar sedan ett sammanfattande resultatavsnitt i vilken insamlad empiri redovisas, vidare konkluderas studien med efterföljande diskussion och rekommendation kring vidare forskningsområden.

2 Litteraturgenomgång

Litteraturgenomgången består av två huvudsakliga komponenter: Definition och beskrivning av begreppet personuppgifter, relevanta regelverk och avtalsformer samt molnteknikens definition, syfte och användning. Avsnittet inleds med en definition av personuppgifter i syfte att förankra förståelsen för den typ av information som studien betraktar. Vidare avhandlas molnets definition och tekniska grund i syfte att förankra den tekniska miljö som studien berörs av samt redovisar varför det finns ett intresse av att nyttja molntjänster. Fortsättningsvis definieras de tekniker och tillvägagångssätt som är relevanta för elektronisk datalagring av personuppgifter i moln och därefter studeras de lagar och regelverk som reglerar hur personuppgifter får lagras. Syftet med litteraturgenomgången är att författa en komplett kunskapsbas, vilken belyser samtliga aspekter av studiens problemområde, den nuvarande forskningens perspektiv på molntjänster och molnlagring samt dess utmaningar.

2.1 Personuppgifter

2.1.1 Definition av personuppgift

Enligt personuppgiftslagen, hädanefter PuL, definieras personuppgifter enligt “All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet” (3 §, SFS 1998:204). I vardagligt tal avser det oftast namn, adressuppgifter, personnummer eller annan information som enligt definitionen kan kopplas direkt till en fysisk person. Ett enskilt personnamn är därför oftast inte härledbart till en enskild fysisk person men däremot i kombination med en adress faller informationen under definitionen personuppgifter. I viss kontext benämns även begreppet känsliga personuppgifter vilket är extra känsliga uppgifter som normalt inte får registreras. Det kan beröra uppgifter så som hälsa, politisk åsikt och medlemskap i fackförening som enbart under vissa förutsättningar lagligt får registreras (13 §, SFS 1998:204).

2.1.2 Personuppgiftslagen

Syftet med PuL är att främja personlig integritet och skydda personer mot kränkande behandling genom dennes personuppgifter (1 §, SFS 1998:204). Därför ställs det höga krav från lagstiftningen på organisationer som avser att behandla sådan typ av information. Lagen ställer ett flertal krav på hur dessa ska behandlas, bland annat att det enligt grundregeln krävs samtycke från personen i fråga, att det ska finnas ett tydligt ändamål med behandlingen och att behandlingen inte missbrukas (9 §, SFS 1998:204). Vidare krävs det att tillstånd av gällande tillsynsmyndighet, vilket är Datainspektionen per 2016, ifall en organisation avser att genomföra någon form för automatisk behandling av personuppgifter. Däremot om organisationen utser

ett personuppgiftsombud, vilket är en fysisk person som ansvar för att kraven i PuL uppföljs, är sådant tillstånd inte nödvändigt. Istället behöver bara personuppgiftsombudet göra en anmälan till tillsynsmyndigheten (36-37 §, SFS 1998:204). Vidare kommer en ny dataskyddsreform att införas inom EU år 2018, vilket kommer bland annat leda till att PuL behöver moderniseras. Reformen är ett svar på den rådande integritetsdebatten om krav på stärkta rättigheter hos enskilda medborgare (Datainspektionen, 2016).

2.2 Molnet

2.2.1 Definition av ett datormoln

Ett datormoln är ett system som möjliggör extern exekvering av mjukvara via Internet. Molnet har sannolikt fått sitt namn från dess typiska systemarkitektur som bygger på en extern beräkningsenhet, vanligtvis i form av ett distribuerat serverkluster, vilken ansvarar för exekveringen av en viss eller ett visst antal applikationer, lagring av data samt infrastruktur (Sosinsky, 2012). Moln konstrueras enligt ett så kallat serviceorienterat arkitekturmönster (Service-Oriented Architecture) och innebär att en uppsättning virtuella komponenter tillsammans erbjuder exekveringsutrymme i form av en tjänst för externa klienter att nå via ett kommunikationsprotokoll över ett nätverk (Endrei et al. 2004). För att bruka den mjukvara, det vill säga de molntjänster som drivs på serverklustret, vilket är själva molnet, kan klienter i form av persondatorer eller mobila enheter via kommunikationsprotokollet och en anslutning till Internet skriva, exekvera och ta emot data. Datormoln och molntjänster innefattas således av att all typ av beräkning och informationsbehandling sker externt från de klienter som efterfrågar tjänsten, det vill säga "i molnet" (Sosinsky, 2012).

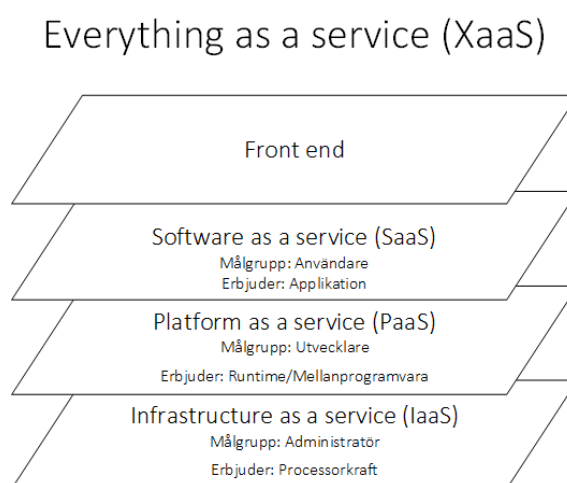
Då molnet innefattar en central beräkningsenhet innebär det att de klienter som kommunicerar med molnet nyttjar och delar samma molntjänster. Molnet syftar till att kunna erbjuda alla de tekniker som krävs för att driva en applikation i form av en tjänst via Internet och med det kommer krav på att molnet har en runtime att köra applikationen i, utrymme för att skriva data samt kanaler för kommunikation. Det kallas att molnet erbjuder EaaS, "Everything-as-a-Service", det vill säga "allting som en tjänst" vilket utgör kärnan i molnets tekniska syfte (Sosinsky, 2012).

2.2.2 Molntjänsttyper

För att ett moln ska kunna erbjuda EaaS, "allting som en tjänst", krävs tre fundamentala modullager vilka också utgör molnets huvudsakliga beståndsdelar: IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service) och SaaS (Software-as-a-Service) (Sosinsky, 2012). De tre molnlagren är strukturerade med bottenlagret som den mest maskinnära komponenten och topplagret som det lager med vilken användaren interagerar. Den första och mest fundamentala modulen är IaaS, infrastruktur som en tjänst, vilken innefattar molnets beräkningskomponenter och innehåller de tjänster som möjliggör molnets digitala infrastruktur. Exempel på

dessa är virtuella maskiner, olika typer av servrar så som SQL- och webbservrar, datapartitionering, skalning och säkerhetskopiering (Sosinsky, 2012). Nästa modul, ett steg upp i lagret, är PaaS, plattform som en tjänst, och innefattar den utvecklingsmiljö som applikationsutvecklare arbetar mot. Modulen innefattar främst applikationernas runtime, det vill säga är det lagret i vilket mjukvaran körs. Typiska användningsområden för applikationsutvecklare är drift av egenutvecklade webb- eller mobilapplikationer. PaaS:er erbjuder oftast en stor produktportfölj av olika molntjänster vilka ämnar understödja utvecklare applikationer med olika tjänster så som exempelvis kopplingar till databaser, testverktyg och skalbarhetsverktyg, samtliga verktyg som kommunicerar med applikationen såväl som molnets infrastruktur- och mjukvarumodul. SaaS, mjukvara som en tjänst, är molnets översta lager och innefattar de tjänster som omfattas av färdiga applikationer och mjukvara, exempelvis dedikerade program som tidigare endast gick att exekvera lokalt på en klientdator men som tack vare molnteknik nu kan nås som en molntjänst (Sosinsky, 2012).

Ovanpå SaaS-modulen lever ett gränssnitt som sammankopplar användaren med molnet. Interaktionen sker vanligtvis via en webbläsare, en applikation för mobila enheter, en toppskiktsklient i form av en programvara som installeras lokalt men som utför externa operationer eller direkt via en terminal (Sosinsky, 2012).



Figur 1: Molnets lager (Sosinsky, 2012)

2.2.3 Varför använda sig av molntjänster?

Den numera globala och högkvalitativa tillgänglighet till molntjänster världen över har för verksamheter inneburit stora förändringar. Statistik från bland andra Gartner Research utförd 2010 visar att molntjänster 2014 prognostiserades till en marknad värd 150 miljarder dollar och att små till medelstora företag förväntades spendera över 100 miljarder dollar på molntjänster vid 2014 (Marston et al. 2010). Statistik utförd av EU i november år 2014 visar att det

inom företag i norden finns en mycket stor beroendegrad av molntjänster och molnteknik där Finland har strax över 50 procent, Island drygt 40 procent och därefter Sverige, Norge och Danmark med respektive strax under 40 procent (Eurostat, 2014). Siffrorna ger sken av att företag i allt större utsträckning intresserar sig för molntjänster och molntekniker vilket är rimligt då adaptation av molntjänster i samband med transformation av egen IT-verksamhet är förenat med ekonomiska så väl som tekniska fördelar (Marston et al. 2010).

De ekonomiska fördelarna berör främst resursbesparingar relaterat till IT-investeringar. Organisationer vars affärsverksamhet kräver omfattande datacenter kan göra stora besparingar genom att migrera sin digitala verksamhet till molntjänster. Detta innebär att verksamheten inte längre själv behöver stå för den hårdvara som driver datacentret, oftast en större hall med ett större antal servrar, och inte heller behöver förse den med elektricitet för att driva hårdvara och kylning samt inte heller behöver investera i komponentunderhåll och komponentuppgradering. I och med ett migrerat datacenter försvinner även krav på kompetens för administration av datacentret och därmed kan verksamheten även göra personalrelaterade resursbesparingar, en undersökning från Gartner Research har indikerat att ungefär två tredjedelar av ett genomsnittligt företags IT-budget förläggs till kostnader relaterade till underhåll. Samtidigt visar en undersökning utförd av VMWare av sex företags datacenter att den större andelen servrar endast förbrukar mellan tio till 30 procent av deras totala beräkningskraft (Marston et al. 2010). Vid antagande om att en typisk server har en livslängd på tre år kommer endast kostnader för infrastruktur och energiförsörjning på egen hand överskrida inköpspriset, det vill säga att återbetalningstiden för investeringen uteblir. Ur ett ekonomiskt skalbarhetsperspektiv kan användandet av molntjänster innebära en fem- till sjufaldig återbetalningstidsreduktion för den totala molninvesteringen och är därför en betydligt mer kostnadseffektiv investering (Armbrust et al. 2009).

Nyttjandet av molntjänster innebär även en rad tekniska fördelar för såväl stora som små verksamheter. I och med att molnet ur ett prestandaperspektiv skalar beräkningsresurser betyder det indirekt att verksamheter kan skala sina driftskostnader och därmed bedriva en mer kostnadseffektiv verksamhet (Marston et al. 2010). Vidare kan molntjänster för främst mindre verksamheter öppna upp tekniska möjligheter traditionellt sett endast tillgängligt för större organisationer. Via molntjänster kan mindre verksamheter få tillgång till dyr industrimjukvara vilken tidigare krävt stora investeringar i form av hårdvaruinköp, en investering som, när mjukvaran erbjuds som en tjänst, inte längre behövs. Detta öppnar inte bara upp nya tekniska områden och skapar bättre förutsättningar för verksamheten att öka sin konkurrenskraft men sänker även barriären för IT-innovation och öppnar upp för nya marknader (Marston et al. 2010).

2.2.4 Hur lagras data i ett moln?

Molnlagring är benämningen på den term som omfattas av att information elektroniskt lagras i ett datormoln. Lagring av data sker i moln under antingen strukturerade eller ostrukturerade förhållanden (Sosinsky, 2012). Ostrukturerad datalagring är lagring där leverantören, exempelvis ägaren av molnet, satt villkor och begränsningar i form av tillgängligt lagringsutrymme, hur data får lagras och vilka applikationer som får lov att lagra data. Användaren har alltså mycket liten kontroll över de premisser som informationen lagras på och interagerar med lagringsutrymmet via en applikation, exempelvis via en lokal mjukvara eller via en webbläsarklient. Strukturerad datalagring används av utvecklare i deras arbete med att utveckla webbapplikationer och till skillnad från ostrukturerad datalagring innebär strukturerad lagring att utvecklaren har direkt tillgång till ett visst diskutrymme och själv bestämmer premisserna för hur information ska lagras (Sosinsky, 2012).

Vid lagring av strukturerad data, vilken är den lagringstyp som exempelvis personuppgifter förekommer i, nyttjar i princip alla stora molntjänsteleverantörer objektlagringsarkitektur (Object Storage Architecture) (Mesnier, Ganger & Riedel, 2003). Objektlagring är en lagringsarkitektur vilken innebär att varje stycke data som ska lagras fungerar som ett objekt i form av en behållare vilken innehåller den data som ska lagras, exempelvis ett fotografi, metadata samt en globalt unik identifieringsnyckel (Mesnier, Ganger, & Riedel, 2003). Objektlagring, som är en sammansättning av de traditionella lagringsteknikerna NAS (Network Attached Storage) och SAN (Storage Area Network), innefattas alltså både av hög filabstraktion vilket innebär att data kan lagras oberoende av operativsystem (cross-platform) samt policybaserad säkerhet men också direktaccess och skalabilitet (Mesnier, Ganger & Riedel, 2003). Skapandet av objekten påminner om hur data skapas i ett filsystem, men eftersom objekt kan växa och krympa dynamiskt är det lagringsenheten själv, det vill säga servern, som är ansvarig för all styrning och kontroll av hur data lagras (Mesnier, Ganger & Riedel, 2003). Eftersom ett moln ofta innehåller flera servrar bildar dessa tillsammans ett globalt filsystem (Global File System), vars princip bygger på att inhämtandet av ett visst objekt inte kräver att den tjänst som letar efter objektet måste ange en direkt sökväg till den enhet som lagrar data utan att tjänsten kan skicka en förfrågan till det globala filsystemet som oberoende en direkt sökväg returnerar platsen för det objekt tjänsten letar efter (Mason & Rodriguez, 2009). Eftersom dessa globala filsystem övervakas och administreras av automatiska processer, vars syfte är att optimera och strömlinjeforma molnet baserat på en rad olika prestandavariabler, är det vanligt att stora mängder data frekvent flyttas om mellan olika lagringsnoder (Mesnier, Ganger & Riedel, 2003).

Eftersom ett datormoln endast är så stabilt och pålitligt som den hårdvara som molnet drivs på finns det alltid risk för att hårdvarukomponenter fallerar och gör data otillgänglig, av denna anledning distribuerar molntjänsten data till flera olika noder i syfte att säkerhetskopiera informationen (Peterson, Gondree & Beverly, 2011). Som ett resultat av molnets tekniska natur vad gäller arkitektoniska principer och hur data lagras kan det i dagsläget vara svårt för molntjänsteleverantörer att vid en given tidpunkt veta exakt var data lagras ur ett geografiskt per-

spektiv, det vill säga var den enhet som fysiskt lagrar informationen befinner sig. Om molntjänsten dessutom använder serverfarmar som tillhör en tredjepartsleverantör uppstår ytterligare ett lager av komplexitet i form av tekniska såväl som juridiska aspekter. När en kund sluter ett avtal med en molntjänsteleverantör omfattas detta avtal av en rad olika SLA-värden (Service Level Agreement) vilka bestämmer exempelvis kundens tillgänglighet till molnet i form av prestanda, up-time och nätverkshastighet. På grund av komplikationen med var data lagras i ett moln är de SLA-värden som reglerar det som kallas för "data sovereignty", det vill säga datans geografiska placering, ofta mycket vaga eller otillräckliga (Peterson, Gondree & Beverly, 2011). Trots detta är objektlagring det självklara arkitektoniska valet för molntjänster då det möjliggör lagring av enorma mängder ostrukturerad på ett sätt som gör att det är relativt billigt ur ett prestandaperspektiv, det vill säga aktiviteter som avsökning och hämtning av data i systemet, samtidigt som det erbjuder stora möjligheter vad gäller skalabilitet (Mesnier, Ganger & Riedel, 2003).

2.2.5 Tekniska risker med molnlagring

Det finns en rad olika risker förenade med molnlagring där den nuvarande forskningen som den här studien tagit del av i princip är eniga om att det främst hotet gäller datans integritet och säkerhet. Sandeep (2012), Loganayagi och Sujatha (2012) samt Svantesson och Clarke (2010) pekar samtliga på just säkerhet och integritet är den primära utmaningen för molntjänster där det dels handlar om att faktiskt skydda datan från otillåten insyn och risk för stöld eller manipulation samt ur ett organisatoriskt perspektiv kunna övertyga potentiella kunder och verksamheter om att det är säkert och pålitligt att lagra sin information hos en molnleverantör. Vidare menar Svantesson och Clarke (2010) att det är viktigt att inte underskatta skillnaden mellan att driva ett eget IT-center och att nyttja en molntjänst och att en risk som finns förenad med detta är att verksamheten inte har samma kontroll över den tekniska miljö som den bedriver sin verksamhet i vilket kan få allvarliga följder som ett resultat av ny mjukvara eller förändringar i molnet. En annan risk är också att en verksamhet kan komma att överskattar den teknik som molnet bygger på, vilken ju fortfarande är förhållandevis ung, och därmed underskatta molnleverantörens säkerhetsåtgärder vilket kan resultera i ett förringande av egna säkerhetsåtgärder (Svantesson & Clarke, 2010).

2.3 Personuppgifter i molnet

2.3.1 Molnlagring av personuppgifter

Eftersom elektronisk lagring idag är standard för de flesta typ av större register har till viss del PuL anpassats för att hantera elektronisk behandling och lagring som eventuellt förekommer vid i molnet. Även om uppgifter kan krypteras eller anonymiseras, räknas de alltid som personuppgifter om det finns, vid hanteringsstillfället, en nyckel för åtkomst eller anonymisering (Pensionsmyndigheten, 2016b). Därför är det alltid fråga om huruvida möjligheten finns att härleda uppgifterna till en fysisk person som avgör om det är tala om personuppgifter eller

ej. För att förtydliga ansvaret vid behandling av personuppgifter skiljer lagen på den aktör som är personuppgiftsansvarig och personuppgiftsbiträde. Personuppgiftsansvarig är den som beslutar om syftet med behandlingen samt är ansvarig för att utse ett personuppgiftsombud. Ett personuppgiftsbiträde är en tredje part som behandlar uppgifterna och är anlitad av den personuppgiftsansvarige (3, 30-31 §, SFS 1998:204). Lagen ställer även krav på skriftligt avtal mellan parterna där särskild vikt ska läggas på säkerheten vid behandling av personuppgifter.

Datainspektionen, vilken är den gällande tillsynsmyndighet av PuL, har utformat ett antal rekommendationer till verksamheter som planerar att använda molntjänster där personuppgiften kan komma att lagras. De understryker att det alltid är den personuppgiftsansvarige som är skyldig att säkerhetsställa att samtliga anlidade leverantörer, kallade personuppgiftsbiträden, följer lagen vid behandling av uppgifterna. För att en organisation ska kunna göra det på ett tillfredsställande sätt föreslår Datainspektionen att en laglighetskontroll av den förutfattade hanteringen av personuppgifterna genomförs för att säkerhetsställa att behandlingen är legal. Det syftar till att bland annat undersöka om uppgifterna kan komma att behandlas felaktigt, om uppgifterna kan komma att lagras i tredje land samt vilka nödvändiga säkerhetsåtgärder förespråkas för att uppgifterna ska skyddas (Datainspektionen, u.å.).

Vidare rekommenderar Datainspektionen att organisationen genomför en risk- och sårbarhetsanalys vars syfte är att undersöka huruvida molntjänstleverantören uppfyller de krav i PuL 31 § (SFS 1998:204). Enligt Datalagringsdirektivet (1995), ett EU-direktiv som är bakgrunden till införandet av PuL i Sverige, innebär det att molntjänstleverantören ska vidta tekniska säkerhetsåtgärder så som kryptering, säkerhetskopiering, loggning, behörighetskontroll samt skydd mot skadlig programvara för att skydda personuppgifter. Det ska även finnas möjlighet för den personuppgiftsansvarige att kontinuerligt kontrollera att dessa säkerhetskrav uppföljs av molntjänstleverantören och vid behandling av särskilt känslig data, det vill säga exempelvis personuppgifter, bör dessa krav ytterligare stärkas (Datainspektionen, u.å.). Dessutom ska säkerhetskrav och andra aspekter kopplat till behandling av personuppgifter via ett biträde regleras med ett så kallat personuppgiftsbiträdesavtal enligt PuL 30 § (SFS 1998:204). Detta ska vara ett separat avtal med särskilda föreskrifter om hur biträdet får behandla personuppgifter. Det är dessutom den personuppgiftsansvariges skyldighet att säkerhetsställa att personuppgifterna, vid anlitage av molntjänstleverantör, inte överförs till ett så kallat tredje land (33 §, SFS 1998:204). Ett tredje land är ett land utanför EU eller det Europeiska ekonomiska samarbetsområdet, även kallat EES, vilket som regel inte anses uppfylla det adekvata skydd av data som EU-lagstiftningen kräver (3 §, SFS 1998:204).

2.3.2 *Safe Harbour*

Eftersom att ett flertal molnleverantörer är från USA har överföring hit tidigare varit tillåtet via ett särskilt Safe Harbour-avtal mellan leverantören och den personuppgiftsansvarige. Detta möjliggjorde att data innehållande personuppgifter kunde legalt överföras till tredje land om ett sådant avtal undertecknats. Dock underkände EU-domstolen den sjätte oktober 2015 Safe Harbour-avtalet eftersom att det inte kunde reducera eller eliminera tredje lands möjlighet att via nationell övervakning ta del av eller exponera personuppgifter (Court of Justice of the European Union, 2015). Detta betyder att alla tidigare undertecknade Safe Harbour-avtal inte längre är juridiskt giltigt och att verksamheter som fortsätter överföra personuppgiftsdata till tredje land med stöd av avtalet kan begå ett lagbrott.

2.3.3 *Privacy Shield*

För att verksamheter som redan tecknat avtal med amerikanska molntjänstleverantörer ska kunna fortsätta nyttja dessa utan risk för legala implikationer har EU-kommissionen tagit fram ett nytt ramverk, så kallat Privacy Shield, för överföring av personuppgifter till tredje land. De stora skillnaderna i det nyare Privacy Shield kontra det föråldrade Safe Harbour är främst stärkta rättigheter när det gäller integritet för privatpersoner och hårdare krav mot molntjänstleverantörerna. Genom avtalet ska personuppgifter behandlas i USA med krav om att behandlingen motsvarar EU-standard. Avtalet inkluderar även styrmekanismer så som sanktioner och exkludering ifall en leverantör inte respekterar bestämmelserna (European Commission, 2016). Eftersom avtalet annonserades i februari 2016 är bestämmelserna, vid uppsatsens författande, relativt nya och oprövade. Detta betyder att det i dagsläget saknas praxis och rättsfall för hur ramverket kommer att tillämpas.

2.3.4 *Juridiska risker med molnlagring av personuppgifter*

Det kan framstå som onödigt komplicerat och förlegat att ställa så pass hårda krav, både legalt och tekniskt, på molntjänstleverantörer vid lagring av personuppgifter men det finns flera risker förenat med bristande kontroll. Bland annat kan information dela resurser och lagringskapacitet med andra leverantörer vilket kan möjliggöra exponering av informationen till tredje part vid ett eventuellt intrång eller mänskligt fel (King & Raja, 2012). Vidare pekar King & Raja även på naturliga risker förenade med komplex infrastruktur så som skadliga intrång (2012). Sony upplevde ett sådant intrång 2011 när personuppgifter för 77 miljoner användare av den populära spelkonsolen Playstation blev stulna av en anonym hackergrupp (Quinn & Arthur, 2011). Incidenten vittnar om konsekvenserna vid icke-adekvat skydd av persondata samt den magnitud av personinformation som stora aktörer innehar och därmed riskerar att exponera. Emellertid hävdar King & Raja, något motsägelsefullt, att molnlagring kan vara säkrare än traditionell datalagring eftersom att det ofta finns dedikerad personal till att hantera eventuella intrång och säkerhetsbrister samt att tekniken hård- och mjukvara kontinuerligt hålls ajour (2012). Att lagra personuppgifter externt och hos tredjeland är enligt Cheng och Lai (2012) egentligen ingen nyhet då möjligheten att nyttja databaser utanför nationella gränser funnit i många år, däremot kommer det sätt som molntjänster idag interagerar samt de

större volymer data som skickas fram och tillbaka ha en betydande inverkan på den juridiska infrastrukturen i frågor om integritet relaterat till personuppgifter, vilket incidenten hos Sony pekar på (Cheng & Lai, 2012).

PuL betonar enligt 33 § (SFS, 1998:204) att personuppgifter inte får överföras till ett tredje land eftersom dessa länder normalt sätt inte kan garantera det adekvata skydd av uppgifterna som Datalagringsdirektivet (1995) kräver. En betydande risk är att ett tredje landet inte respekterar integritetsskydden eller att det inte finns möjlighet att kontrollera huruvida föreskrifterna i direktivet följs av landet i fråga (De Hert, Papakonstantinou, & Kamaraet, 2016). Exempelvis avslöjades det i mitten på 2013 av visselblåsaren Edward Snowden hur den amerikanska Nationella Säkerhetsmyndigheten (NSA) konsekvent övervakat och samlat in data om inhemska och utländska medborgare (BBC, 2014). De molntjänstleverantörer som lagrar personuppgifter i USA riskerar därmed att blir övervakade vare sig det rör sig om personuppgifter från inhemska eller utländska organisationer. Detta strider mot vad EU avser vara adekvat skydd av data (Datalagringsdirektivet, 1995) och var en av de primära anledningarna till att Safe Harbour-bestämmelserna ogiltigförklarades år 2015 (Court of Justice of the European Union, 2015). Vid lagring av omfattande personregister eller ytterst känsliga uppgifter finns det naturliga säkerhets och politiska konsekvenser av att tredje land har möjlighet att ta del av den typen av uppgifter. Inom EU finns det gemensamma reglemente för hur personuppgifter ska hanteras och skyddas, vid överföring mot tredje land reduceras möjligheten att utöva politiska påtryckningar för att säkerhetsställa att adekvat skydd upprätthålls.

3 Teoretiskt ramverk

Det teoretiska ramverket utgörs av identifierade utmaningar som ett resultat av studiens inlästa litteratur och litteraturgenomgång. Avsnittet omfattar inledningsvis en skriftlig summering av de identifierade utmaningarna ur ett litteratururvalsperspektiv, vilket lyfter den nuvarande forskningens syn på utmaningar förenade med molntjänster. Fortsättningsvis definieras sedan dessa utmaningar i en modell som summerar det teoretiska ramverket.

3.1 Litteratururval

Följande litteratururval innehåller en summering av de utmaningar som identifierats i samband med en verksamhets transformation till ett datormoln ur ett tekniskt och ur ett juridiskt perspektiv. Utmaningarna har kategoriserats med ett ID-nummer vilket korresponderar mot respektive rad i nedanstående tabell (tabell 1).

Integritet (1): King & Raja (2012), Loganayagi & Sujatha (2012) samt Sosinsky (2012) beskriver att en av molnteknikens största utmaningar innefattar bevarandet av datans integritet. De anser att det finns en betydande utmaning förenad med arbetet att förhindra att enskilda personer eller stater genom teknisk manipulation i hemlighet kan ge sig själva tillträde till informationen. Förenat med detta påstår King & Raja (2012) att molntjänstleverantörer, och indirekt de organisationer som nyttjar molntjänster, upplever en kritisk utmaning i form av att kunna övertyga användarna om att data de delar med sig lagras på ett sådant sätt att integritetsskyddet är adekvat. Svantesson & Clarke (2010) förtydligar detta genom att påpeka att datormoln som ett tekniskt ramverk är förenat med flertalet komplexa integritetsutmaningar då molnteknik i dagens format är en relativt ny och obeprövad teknik.

Datasäkerhet (2): Sandeep (2012) menar att den mest substantiella utmaningen för datormoln handlar om datasäkerhet och att brister relaterade till datasäkerhet fungerar som ett hinder för organisationer som vill flytta sin IT-verksamhet ut i molnet. Cheng & Lai (2012) anser att fördelarna med datormoln i slutändan kan innebära nackdelar. Även om molnleverantörer visserligen kan ha råd att implementera större och mer effektiva säkerhetsåtgärder i ett datormoln än vad en privatperson kan implementera på en persondator, kan de tekniker som är förenade med datormolnet innebära stora säkerhetsrisker. Exempel på dessa är fjärråtkomst, virtualization, plattformsdelning, gränsöverskridande dataflöde och ett utbrett användande av tredjepartmjukvara vilket kan leda till brist på kontroll över vart data befinner sig och vart data flyttas. King & Raja (2012), Loganayagi & Sujatha (2012) såväl som Sosinsky (2012) instämmer samtliga i detta och menar att integritetsutmaningen (1) i princip är likställd med arbetet att förhindra ogiltig dataåtkomst (2), då detta är direkt förenat med att bevara dataintegritet. Sosinsky (2012) menar att när en användares information förflyttas och lagras på sy-

stem som användaren inte har någon kontroll över, ökar de tekniska riskerna ur ett informationssäkerhetsperspektiv i form av att datatransaktioner exponeras för manipulation och därmed avlyssning.

Regelverk (3): Peterson, Gondree & Beverly (2011) pekar på att en överhängande utmaning med att lagra data i molnet är de regelverk vilka reglerar var, ur ett geografiskt perspektiv, känslig information som exempelvis personuppgifter får lov att lagras. De menar att det är mycket viktigt att se till att data lagras på ett sådant sätt att lagringen följer de nationella regelverk som ägaren till informationen är skyldig att följa. Här får de medhåll av Cheng & Lai (2012) vilka påstår att även om datormoln som koncept, det vill säga idén kring distribuerad lagring på centrala platser utspritt över ett visst geografiskt område, exempelvis över flera länder, inte är en revolutionerande teknik, kommer det nya sätt som vi använder oss av datormoln på ha en betydande inverkan på den juridiska infrastrukturen. De anser att det är av betydande vikt att säkerhetsställa att data lagras där den juridiskt sett får lagras i syfte att följa regelverk och skydda datans integritet. King & Raja hävdar att det sätt som datormoln idag lagrar och processar data på innebär utmaningar för dataskyddslagsstiftning, vars primära farhåga innefattar nationell säkerhet. De påstår att även om slutanvändaren i form av den person som förser molntjänsten med sina personuppgifter kanske inte har något egenintresse i att veta hur eller var sina uppgifter lagras, är detta något som är väldigt viktigt för det (EU-) land invånaren bor i och något som måste tas med i avtalsskrivandet som ett resultat av rådande lagstiftning (2012). Svantesson & Clarke (2010) påpekar slutligen att datormoln står inför betydande utmaningar när sekretessbelagd data distribueras och lagras i enheter vars juridiska nationella position inte är densamma som användarens.

Drift och kommunikation (4): Sandeep (2012) anser att företag drar sig för att integrera sina affärer med molntjänster, då dessa tjänster, som ett resultat av molnets tekniska natur, sker hos molntjänstleverantör och kanske inte upplevs som helt trovärdiga, något som Sandeep identifierar som en utmaning. Svantesson & Clarke (2010) menar att problemen inte bara handlar om att molnleverantören ska uppfylla datadirektiv och föreskrivna lagar utan att själva datormolnen i sig, som tidigare nämnts, är ett relativt nytt fenomen och bygger på omodern teknik, vilket ur ett organisatoriskt IT-perspektiv upplevs som en utmaning. Vidare beskriver Sosinsky (2012) att den risk som förenas med att driva egna IT-center vid molntjänst flyttas från egen part till molntjänstleverantören och att detta måste tas med i organisationens riskanalys.

3.2 Identifierade utmaningar

Ovanstående litteratururval sammanfattar litteraturgenomgångens identifierade utmaningar. Dessa utmaningar har kategoriserats enligt tekniska, juridiska och organisatoriska utmaningar. Den tekniska kategorin innefattar utmaningar som berör hur data lagras och behandlas ur ett direkt informationstekniskt perspektiv. Nedanstående tabell utgör en sammanfattning av det teoretiska ramverket där den första kolumnen innefattar utmaningens ID-nummer i relation till litteratururvalet, den andra kolumnen beskriver utmaningens kategori och den tredje kolumnen beskriver själva utmaningen.

#	Kategori	Utmaning
1	Teknisk, juridisk	Integritet
2	Teknisk, juridisk	Datasäkerhet
3	Juridisk	Regelverk
4	Teknisk, organisatorisk	Drift och kommunikation

Tabell 1: Identifierade utmaningar

Ramverket skiljer distinkt på integritet och datasäkerhet då integritet syftar till att data lagras på ett sådant sätt att obehöriga personer eller stater ej får insyn i datan på den plats där den lagras. Datasäkerhet syftar till att data ej vid överföring eller lagring kan manipuleras eller förflyttas från sin fysiska lagringsplats.

4 Metod

I följande stycke presenteras den vetenskapliga metod och det tillvägagångssätt studien bygger på för att forskningsfrågan “vilka är utmaningarna vid lagring av personuppgifter i molnet?” ska kunna besvaras. I stycket presenteras hur metodval utförts, hur den kvalitativa studien genomförts samt hur analys och bearbetning av data gått till. Den litteratur som legat till underlag för hur metodarbetet gått till är Dag Ingvar Jacobsens bok “Vad, hur och varför? - Om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen” (2002).

4.1 Metodval

4.1.1 Kvalitativa intervjuer

Vid val av metodik för insamling av empirisk forskningsdata finns det normalt två olika tillvägagångssätt: Kvalitativ och kvantitativ studie (Jacobsen, 2002). Vid en kvalitativ studie inhämtas normalt data från en handfull subjekt vilket, i motsats till en kvantitativ studie, gör bland annat generalisering av data svår genomförbart. Fördelen är dock att kvalitet och djup blir en mer central del i forskningen och därmed kan komplexa problem beskrivas i större detalj (Jacobsen, 2002). I vår studie om personuppgifter i molnet har vi för avsikt att ta del av djupare svar vid vår datainsamling varför vi valt att genomföra en kvalitativ studie. Vi har därför identifierat ett fåtal subjekt vilka vi genomfört en djupintervju med i syfte att skapa en detaljerad bild av problemet i praktiken. Eftersom vi innan studiens begynnelse tagit del av en liknande omfattande kvantitativ studie genomförd av Pensionsmyndigheten finns det motiv för att i vår studie försöka dra djupare slutsatser. Därför blev det tydligt att forskningsfrågan på ett tillfredsställande sätt kunde besvaras genom att utföra en kvalitativ studie.

4.1.2 Kvantitativ sekundärdata

I syfte att styrka empirin kring vår tes har en sekundär datakälla (Appendix 8.2) använts som tillägg till den egenutförda kvalitativa empiriska studien. Den sekundära datakälla vilken vi tillhandahållit är en sammanställning av Pensionsmyndighetens egen enkätundersökning där 148 myndigheter svarat på frågor om respektive användning av olika molnlösningar. Syftet med enkäten var att skapa en detaljerad bild av de olika myndigheternas molnanvändning i dagsläget samt den förväntade användningen om två år. Enkäten genomfördes i oktober 2015 och bestod av 48 frågor relaterade till bland annat verksamhetens syfte, användning av molntjänster och hantering av personuppgifter. Resultatet av enkäten användes som empiriskt underlag i rapporten Molntjänster i staten (Pensionsmyndigheten, 2016a), utformad av Pensionsmyndigheten på uppdrag av regeringen. Av de som svarat på enkäten angav strax under 80 procent (Appendix 8.2, tabell 1) att de innehar en roll inom verksamheten som direkt är

kopplad till IT, vilket både är relevant för problemområdet samtidigt som det till viss del motsvarar urvalet av intervjupersoner i den kvalitativa undersökningen. Vidare innefattar enkäten ett antal frågor som vi har valt ut eftersom de är direkt kopplade till problemområdet i form av ämnen som exempelvis berör adoptionsgrad och upplevd nytta av molntjänster, i vilken utsträckning personuppgifter lagras i dessa molntjänster samt huruvida personuppgiftsbiträdesavtal har tecknats. Dessa faktorer visar på relevansen av undersökningen vilket gör att vi bedömer undersökningen som relevant att nyttja som sekundärkälla.

4.2 Urval

Vid urvalsprocessen har vi valt att bygga vidare på resultatet av Pensionsmyndighetens enkätundersökning (Appendix 8.2), varvid vi avsett att intervjua personer med någon form av erfarenhet av molntjänst med personuppgiftslagring. Med erfarenhet avses en person som med ett tekniskt, säkerhetsmässigt eller juridiskt perspektiv, eller en kombination av dessa, varit delaktig i en implementation, process eller beslutsfattande vad beträffar molntjänster. Urvalsprocessen har till viss del präglats av de steg som Jacobsen förordar: Inskaffa överblick av de absolut mest önskvärda intervjupersonerna, dela in dem i undergrupper och välj rätt kriterier för att genomföra urvalet (2002). Metodiken har fungerat som assistans till vår urvalsprocess av lämpliga intervjupersoner, detta i syfte att säkerställa att personerna har korrekt erfarenhet samt är relevanta för problemområdet. Som ett naturligt resultat av dessa kriterier valde vi att avskärma verksamhetsurvalet till personer inom kommunal verksamhet samt Datainspektionen vilket är den gällande tillsynsmyndigheten för PuL.

De identifierade verksamheterna har initialt kontaktats via e-post och sedan har vidare korrespondens skett via telefon. Vi har eftersökt personer inom verksamheterna vars yrkesroll innebär att de antingen fungerar som nyckelpersoner för sådant som rör lagring av personuppgifter i molntjänster eller har haft ett betydande ansvar i en process gällande upphandling eller projektstyrning vid inköp av molntjänster med syfte att lagra personuppgifter. Urvalsprocessen resulterade i en lista på 20 kommuner, en relevant person från SUNET samt en relevant person från Datainspektionen. Av dessa 20 verksamheter fick vi svar från fyra vilka kunde tänka sig att ställa upp på en intervju. SUNET och Datainspektionen ställde också upp.

4.3 Intervjugenomförande

Ambitionen vid intervjugenomförandet var att i första hand genomföra fysiska intervjuer, det vill säga att vi och intervjupersonen befann oss i samma rum under samtalet. Men på grund av geografisk lokalisering och tidsbrist från intervjupersonens sida genomfördes intervjuerna per telefon eller Skype. Vid intervjugenomförande finns det både för- och nackdelar med att hålla ett personligt möte kontra en telefonintervju. Vid fysisk intervju kan nyanser och detaljer i svaren enklare fångas upp och tolkas av intervjuaren men vid telefonintervju minskar den så kallade intervjuareffekten vilket syftar på effekt som intervjuaren kan ha på intervjupersonen vid ett fysiskt möte (Jacobsen, 2002). Det kan exempelvis vara svårare att prata öppet och

fritt. En telefonintervju kan därför upplevas mer anonym och på så sätt är intervjupersonen mer benägen att dela med sig av detaljer (Jacobsen, 2002). Våra intervjuer genomfördes enligt en tematisk modell där vi valde att dela upp intervjun i olika teman för att uppnå ett öppnare intervjuklimat. Det genomfördes genom att ett fåtal grundläggande frågor och teman framtagits, vilka sedan ledde till följdfrågor beroende på de svar som intervjupersonen gav. Denna metodik gav oss möjlighet att följa en relativt öppen formalia vilket mynnade ut i möjligheten att ställa mer precisa följdfrågor ifall intervjupersonen berörde aspekter av intresse för vår studie.

4.3.1 Intervjuguidens uppförande

Intervjuguidens utförande är ett resultat av det teoretiska ramverk (tabell 1) som definierats av rapportens forskningsområde samt Pensionsmyndighetens enkätundersökning. Guiden syftar till att belysa viktiga aspekter i form av teman vilka anses relevanta för forskningsfrågan, det vill säga att samla in information om eventuellt upplevda utmaningar som ett resultat av en process vilken innefattas av att intervjupersonen interagerat med en molnlösning i vilken lagring av personuppgifter förekommer. Det teoretiska ramverket fungerar som utgångspunkt för intervjuguidens huvudsakliga ämnesområden och utgör den kunskapsbas vilket frågorna bygger på. I det intervjuförberedande arbetet studerades även sekundärdata, Pensionsmyndighetens enkätundersökning, där liknande frågor bearbetades för att uppnå en kontinuitet i forskningsarbetet. Vår avsikt var att gräva djupare i relevanta frågor som behandlades i enkätundersökningen för att på så sätt extrahera mer kvalitativ data. Under arbetet med litteraturgenomgången identifierades ytterligare aspekter vilka vi ansåg vara intressanta att omformulera som intervjufrågor.

Intervjuerna inleddes med ett segment där intervjupersonen fick berätta om sin roll för den verksamhet personen företräder. Vidare frågeställningar ämnade sedan belysa verksamhetens tekniska lösning, det vill säga i vilket syfte och i vilken grad de berörda verksamheterna använder molntjänster samt i vilken utsträckning personuppgifter lagras. Eftersom våra informanternas bakgrund var antingen juridisk eller teknisk fick frågorna, till viss del, anpassas efter personens roll. Det gjorde att vi inte utarbetade en intervjumall med fastställda frågor utan i stället skapade teman utifrån det teoretiska ramverket och sekundärdata. Då litteraturgenomgången beskriver en komplexitet vad gäller lagring av personuppgifter i molnet, berör frågorna sedan hur detta fungerar rent praktiskt för den verksamheten och ämnar belysa utmaningar som intervjupersonen upplevt i samband med exempelvis en upphandlings- eller implementationsprocess. Samtliga intervjuer spelades in digitalt för att förenkla transkribering och samtidigt ge oss en möjlighet att återkomma till utvalda delar ifall det krävdes ytterligare analys av svaren.

4.4 Intervjuanalys

Efter avslutande av intervju och empiriskt insamlande av data är det enligt Jacobsen (2002) viktigt att tre stadier av intervjuanalys genomförs. Jacobsen förordar att det empiriska data ska i analysprocessen kontinuerligt beskrivas, systematiseras och kategoriseras för att läsaren enklare ska kunna sätta sig in i den empiriska studien. Genom att samtliga intervjuer transkriberades kunde data enkelt beskrivas för läsaren i ett rent textformat och på så sätt ge läsaren en möjlighet att följa det empiriska arbetet. Vid analys undersökte vi främst hur intervjupersonen ställde sig till de identifierade utmaningarna inom teknik och juridik samt hur de i övrigt upplevde molntjänsterna kopplat till personuppgifter. Vi strukturerade upp svaren genom att analysera de aspekter som intervjupersonen berörde när de pratade om tekniska och juridiska utmaningar eller problematik kring molntjänster där lagring av personuppgifter förekommer. Den största delen av transkriberingen sållades bort i struktureringsarbetet varvid det endast återstod de aspekter och yttringar vilka vi ansåg vara mest relevanta för att hjälpa oss att besvara forskningsfrågan. I uppsatsen valde vi däremot att presentera transkriberingarna i dess helhet för att ge andra forskare möjlighet att använda sig av datan. Vidare kategoriserades dessa yttringar och aspekter som tekniska, juridiska eller övriga utmaningar. För att ytterligare konkretisera och precisera vår empiri delades resultatet av kategoriseringen in i underkategorier, vilket presenteras ytterligare i resultatdelen.

4.5 Undersökningskvalitet

I syfte att validera undersökningens kvalitet måste denna genomgå en kritisk granskning (Jacobsen, 2002). För att kunna utvärdera studiens kvalitet har vi genomfört en validitets- och reliabilitetsanalys vilken presenteras nedan.

4.5.1 Validitet

En studies validitet definieras huvudsakligen av två olika typer av validitet: Intern och extern. Den interna validiteten innefattas av studiens inre giltighet, det vill säga i vilken grad studiens resultat är trovärdiga och hur pass väl de överensstämmer med verkligheten (Jacobsen, 2002) medan den externa validiteten definierar hur pass generaliserbara studiens resultat är (Jacobsen, 2002).

I syfte att styrka studiens interna validitet har vi valt att ge våra intervjupersoner möjlighet att ta del av den resulterade transkriberingen, detta i syfte att skapa utrymme för korrigerings av eventuella fel eller missuppfattningar som uppstått. Även om den primära undersökningen i den här studien innefattar en kvalitativ studie, ur vilken det är svårt att dra generaliserbara slutsatser, nyttjar studien även en betydande sekundärkälla. Detta, i samband med den primära kvalitativa undersökningen, ger underlag för möjlighet till generalisering och beaktande vilket kan vara viktigt i samband med framtida forskning.

4.5.2 *Reliabilitet*

En studies reliabilitet definierar dess trovärdighet i förhållande till den sanningshalt som går att extrahera ur undersökningens implicita resultat. En studies reliabilitet hotas av främst tre olika effekter, undersökareffekten, kontexteffekten och risk för bristande uppmärksamhet (Jacobsen, 2002). Dessa uppstår som ett resultat av den undersökningsprocess som drivits och för att motverka dessa risker i syfte att förankra studiens reliabilitet har vi vidtagit åtgärder vilka enligt Jacobsen (2002) bör ha en positiv inverkan.

Undersökareffekten uppstår när störning av en naturlig miljö eller situation inträffar som ett resultat av att själva undersökaren har en effekt på det fenomen som undersöks. Detta sker vanligtvis i samband med intervjuer och kallas då för intervjuareffekt vilket innebär att intervjusamtalet tar intryck av sin intervjumiljö i form av exempelvis intervjuarens kroppsspråk, utseende eller talspråk. Av denna anledning måste undersökningen föra med sig en kritisk självgranskning i form av en frågeställning om vilken effekt detta intrång har (Jacobsen, 2002). Det går aldrig helt att undvika undersökareffekten, men genom att kritiskt bedöma i hur hög grad resultatet av en undersökning påverkas av dess metod och intrång i främmande miljö går det att skaffa sig en uppfattning om resultaten ger en korrekt bild av verkligheten (Jacobsen, 2002). Då den kvalitativa undersökningen i den här rapporten innefattas av telefonbaserade intervjuer gör vi bedömningen att risken för att resultat påverkats av undersökareffekten är mycket låg, då telefonsamtal av sin natur, det vill säga det faktum att det utförs på distans, har en mycket låg inverkan på den miljö som intervjun tar plats i.

Kontexteffekten uppstår som ett resultat av de sammanhang i vilken information har samlats in, det vill säga i vilken kontext information har extraherats (Jacobsen, 2002); det finns flera olika typer av kontexteffekter, artificiell eller naturlig samt planerad eller överraskande. Artificiell eller naturlig kontexteffekt innebär att informationsinsamlingens kontext antingen sker i ett sammanhang som är helt ovant för intervjupersonen, exempelvis att det tar plats i en miljö som denne ej tidigare befunnit sig i, eller om intervjun tar plats i en miljö som tidigare är känd. Vidare kan kontexteffekter också uppstå beroende på huruvida intervjutillfället är överraskande eller planerat, det vill säga om intervjupersonen har känt till undersökningen i förväg eller ej (Jacobsen, 2002). För att motverka kontexteffekten har vi låtit intervjuerna ta plats i naturliga miljöer och i en planerad kontext, det vill säga att intervjupersonen har intervjuats på sin arbetsplats och att personen vetat om detta innan. Detta då vi tror att fördelen med att intervjua i en naturlig kontext är övervägande gentemot nackdelarna samt att samtliga intervju personer i förväg bett om att få bli informerade om tänkta intervjufrågor i syfte att samla på sig en adekvat kunskapsbas i frågan.

Vidare kan studiens reliabilitet hotas av slarvfel som ett resultat av ouppmärksamhet från intervjuaren (Jacobsen, 2002). I syfte att motverka fel vid insamling av data har samtliga intervjuer spelats in i fullgod kvalitet och sedan transkriberats där transkriptionen och tolkningen av intervjun i efterhand, som ett resultat av studiens validitet, följts upp tillsammans med intervjupersonen. Om oklarheter kring insamlad information uppstått i efterhand, det vill säga om vissa tolkningar kan ha behövts förtydligas efter det att intervjutillfället tagit plats, har dessa formulerats och skickats till intervjupersonen via e-post.

4.6 Etik

Vid all form av undersökande forskning bör etiska aspekter diskuteras och tas i beaktande. Enligt Jacobsen (2002) finns det tre essentiella föreskrifter en empirisk undersökning bör följa: Informerat samtycke, krav på privatliv och korrekt återgivning. Informerat samtycke betyder att intervjupersonen ska ha lämnat sitt fulla samtycke till att bli empiriskt studerad samt samtyckt till de förhållande då detta ska ske. Det är viktigt att forskaren håller en öppen, professionell och tydlig dialog vad gällande syftet med studien. Under vår studie har vi varit genomgående tydliga och öppna med syftet av undersökningen. Samtliga intervju personer har fått en öppen förfrågan att delta i undersökningen och har således beviljat samtycke genom att acceptera vår hänvändelse. De tillfrågade har även fått möjlighet att erhålla den slutgiltiga publikationen via e-post samt blivit anonymiserade om de önskat.

Vidare är det väsentligt för en undersökning att korrekt återge data i sitt sammanhang (Jacobsen, 2002). Med det menar Jacobsen att intervjupersonen bör få ges en möjlighet att validera och korrigera eventuella felaktigheter eller missuppfattningar. Det betyder också att data ska presenteras i sin riktiga form och inte manipuleras eller förvrängas för att passa studiens syfte (Jacobsen, 2002). Vid genomförande av vår undersökning har vi, efter medgivande av intervjupersonen, spelat in samtliga intervjuer för att kunna presentera transkriberingen i en korrekt och fullständig version.

Slutligen betonar Jacobsen (2002) intervju personens krav på privatliv, varvid han syftar på att det empiriska data vilken samlats in inte ska kunna härledas till privata aspekter eller företags-hemligheter. Framförallt bör forskaren vid utformning av undersökningsmetodik ställa kritiska frågor om hur pass känslig eller privat data som denne avser att samla in är. Ju känsligare data som samlats in, desto högre krav kring anonymisering behöver ställas (Jacobsen, 2002). Vår empiriska undersökning och forskningsfråga har stor förankring till en generalisering kring ett problem, vilket gjorde att våra intervjufrågor riktades mot den studerade organisationen och problemet i större utsträckning än intervjupersonen. Dock ställdes ett antal frågor riktade till personens egna upplevelser kring vissa problem för att vi skulle få ett djupare svar. Vid dessa frågor var det av stor vikt att behålla fokus på rollen som personen innehar och således ej beröra personens privatliv.

5 Resultat

Följande stycke presenterar den empiriska studiens resultat. Stycket struktureras i enighet med det teoretiska ramverkets problemområden varpå de olika identifierade resultaten delas upp i underrubriker i syfte att belysa resultatens olika teman i förhållande till det teoretiska ramverket.

5.1 Presentation av kvalitativ empiristudie

Person	Roll	Organisation	Datainsamling	Appendix
P1	IT-säkerhetsarkitekt	Malmö Stad	Intervju via Skype	Appendix 8.3.1
P2	Jurist	Helsingborgs Stad	Telefonintervju	Appendix 8.3.2
P3	Jurist	Datainspektionen	Telefonintervju	Appendix 8.3.3
P4	IT-chef	LDC	Telefonintervju	Appendix 8.3.4
P5	Systemförvaltare	SUNET	E-postkonversation	Appendix 8.3.5

Tabell 2: Intervjupersoner

5.2 Integritet

5.2.1 Kravställningar ur ett integritetsperspektiv

P1 menar att verksamheter generellt inte är vana vid att kravställa samt teckna avtal ur ett integritetsperspektiv utan gör det snarare utifrån ett affärsperspektiv. Detta uppfattas som en utmaning och P1 menar att verksamheter bör bli bättre på att teckna avtal ur andra perspektiv än det affärsmässiga (P1: 34). Ett exempel som P1 berör kretsar kring att vid flytt av IT-verksamhet till molntjänster behöver myndigheter, men framförallt företag, bli bättre på att vikta individens rätt till integritet högre än sin egen vinstmaximering och kostnadseffektivisering (P1: 34).

5.2.2 Att lagra data i tredje land

Problematiken kring tredje land har diskuterats och lyfts av samtliga intervjupersoner. Eftersom lagring av personuppgifter i tredje land med stöd av Safe Harbour-bestämmelsen efter oktober 2015 inte längre kan anses vara lagligt, bad vi intervjupersonerna kommentera detta. Malmö Stad lagrar, enligt P1s kännedom, inga personuppgifter i tredje land utan de har genom avtal säkerhetsställt att data stannar inom EU/EES eftersom de hade en viss skepsis gentemot bestämmelsen vid dess införande (P1: 18). På SUNET förlitade de sig på ett avtal som till viss del var baserat på Safe Harbour vid upphandling av tjänsten Box men de är idag igång med en process att gå över till alternativ så som Privacy Shield (P5: 7). Enligt P5 beror detta delvis på att nuvarande avtal behöver förnyas och då passar de på att även justera eventuella otydligheter (P5: 8). Helsingborg Stad har, genom Google, också avtal som är baserat på Safe Harbour, eftersom Safe Harbour vid tidpunkten då avtalet tecknades fortfarande var giltigt och bedömdes som lagligt att applicera (P2: 21-22). I detta fall avvaktar verksamheten i stället rättsutvecklingen eftersom det fortfarande anses vara ett så pass nytt beslut, vilket gör att det normalt sett tar tid innan det får praktiska implikationer (P2: 23-26).

Datainspektionen gav vid ogiltigförklarandet tre månaders respit till organisationer som tecknat ett Safe Harbour-avtal i syfte för dessa att kunna ställa om till ett lagligt alternativ. P3 menar på att de inte genomförde några inspektioner under respiten samtidigt som det under denna karantän tillkom det så kallade Privacy Shield, ett lagligt alternativ till Safe Harbour (P3: 18). Privacy Shield är, vid utförandet av den här studien, inte helt färdigställt, vilket betyder att det saknas praxis för hur bestämmelsen ska tolkas juridiskt och praktiskt. Vidare påpekar P3 att samma lagstiftning som exempelvis myndighetsövervakning fortfarande är kvar i USA, vilket var den egentliga grunden till att Safe Harbour från början ogiltigförklarades (P3: 18). Därför ställer P3 sig tveksamt till huruvida Privacy Shield verkligen kommer att skilja sig så mycket från det tidigare Safe Harbour i praktiken (P3: 18).

5.2.3 Transparens hos molntjänstleverantör

P1 betonar vikten av att molntjänstleverantörer är transparenta i deras informationslagringsmetodik i syfte att verksamheten i egenskap av kund ska kunna kontrollera att lagstiftning och gällande avtal respekteras (P1: 36). P1 berättar att flera stora leverantörer är noga med detta och, som exempel på noggrannheten, har information på sina respektive hemsidor om var eventuella underleverantörer befinner sig så att verksamheten kan kontrollera och följa upp att deras uppgifter faktiskt inte flyttas till tredje land (P1: 36). P1 beskriver vidare att det finns en utmaning i att som beställare av en molntjänstleverantör inte riskera ha allt för stor tilltro till leverantören av tjänsten. Detta eftersom den anlitande verksamheten i form av uppdragsgivare i slutändan alltid är ansvarig ägare av uppgifterna och därmed ytterst skyldig för hur dessa hanteras. Detta gäller oavsett molntjänstleverantörens transparens och möjlighet till kontroll samt avtalsuppföljning (P1: 28, 36).

5.3 Datasäkerhet

5.3.1 Kontroll och uppföljning av hur data lagras

Datainspektionen understryker att vid lagring av personuppgifter är det den personuppgiftsansvarige, det vill säga den person som enligt avtal anlitar en molntjänstleverantör i syfte att nyttja en tjänst där lagring av personuppgifter kan förekomma, som är den ytterst ansvarige för att säkerhetsställa att lagen följs av leverantören och samtliga underleverantörer (P3: 24). P1 menar att detta innebär en utmaning i kravställningsprocessen och talar om vikten av att förstå att den information som lagras på en molntjänst alltid främst ägs av anlitaren oavsett var eller hur informationen behandlas (P1: 28). Kravställandet präglas således av en process där det är extra viktigt att teckna ett avtal som innefattar att verksamheten i form av kund kan säkerställa att de ges möjlighet till adekvat insyn och därmed möjlighet till kontroll och uppföljning för hur molntjänstleverantören lagrar verksamhetens information (P1: 28).

5.3.2 Urvalsprocess som garanterar att rätt data lagras

Malmö Stad har i sin övergång till molnet varit tydliga med vilken typ av data som får finnas i molnet respektive egen infrastruktur. Exempelvis har de begränsat i vilken utsträckning känsliga personuppgifter ska finnas inom någon av de anlitade molntjänstleverantörerna (P1: 6). P1 poängterar att en distinkt avvägning bör göras mellan känsliga och icke-känsliga uppgifter samt att de anställda på Malmö Stad måste vara tydligt informerade om vilka uppgifter de får lov att behandla i en molntjänst (P1: 6). Helsingborgs Stad har inom sin molntjänst för skolan gett ut tydliga instruktioner till sina anställda för att de som nyttjar systemet ska vara väl medvetna om vilka typer av uppgifter som får behandlas inom molntjänsten (P2: 8).

5.4 Regelverk

5.4.1 En juridisk komplexitet

Samtliga intervjuer har mer eller mindre behandlat juridiska frågor rörande hur intervjupersonerna förhåller sig till PuL, EU och relevant lagstiftning. De personer vi intervjuat har alla haft en god kännedom om de mest grundläggande juridiska aspekterna när det gäller behandling av personuppgifter. P4 säger att om det finns en risk att personuppgifter lagras i ett system så ska den personuppgiftsansvarige se till att alla aspekter av PuL uppfylls (P4: 22). Detta styrks av P2 från Helsingborgs Stad, där de i varje nämnd har personuppgiftsombud som även träffas kontinuerligt för att diskutera personuppgiftsbehandlingen inom kommunen (P2: 30). P1 upplever att processen med att införa molntjänster där personuppgiftslagring till viss del är mer komplex, eftersom reglerna kring tredje land måste tas i beaktande, något som inte gäller i samma utsträckning som vid användande av egen lokal infrastruktur (P1: 16).

Flera av intervjupersonerna nämner EU som en viktig aspekt i frågan om hur enskilda myndigheter ska förhålla sig till lagen. Exempelvis tror P1 att den nya dataskyddsreformen, vilken kommer införas 2018, kommer ställa högre krav på molnleverantörer och personuppgiftsansvariga (P1: 20). P3 tror att den nya reformen, som bland annat ställer högre integritetskrav på leverantörerna, kommer att avlasta den personuppgiftsansvarige som idag har hela ansvaret för att lagen följs av leverantör och eventuella underleverantörer (P3: 26). Till viss del har de förståelse för att det finns en viss obalans i ansvarsfrågan där den personuppgiftsansvarige tvingas ta ett mycket stort ansvar (P3: 26). Vidare tror P3 att frågan egentligen kanske inte uppfattas komplex för en person med juridisk bakgrund och erfarenhet men att frågan däremot kan tyckas mindre viktigt för en person utan samma juridiska erfarenhet (P3: 28). P3 menar också att lagstiftningen är medvetet formulerad på en abstrakt nivå för att den ska vara tidsbestående, vilket kan göra att det uppfattas som problematiskt för en person utan liknande juridisk erfarenhet och vana (P3: 28).

Vid diskussion om huruvida intervjupersonerna tror att den juridiska processen med tillhörande utmaningar kommer förändras i framtiden tror P1 att det kommer krävas att lagstiftningen hittar en balans mellan teknik och integritet (P1: 44). P1 och P3 tror båda att fler rättspraxis förhoppningsvis kommer göra processen att gå mot molntjänster med personuppgifter mer strömlinjeformad (P1: 46, P3: 22). P2 vill inte spekulera i framtiden utan betonar att de inom Helsingborgs Stad i stället aktivt följer den rättsliga utvecklingen (P2: 23-24).

5.4.2 *Avtal och analysprocess*

Inom Helsingborgs Stad läggs stor vikt vid att se till att risk- och sårbarhetsanalysen hålls kontinuerligt uppdaterad mot eventuella nya risker som kan uppstå (P2: 12). P2 utformade nyligen en risk- och sårbarhetsanalys vilket var första gången intervjupersonen genomförde en sådan analys på en molntjänst. För att underlätta arbetet använde P2 därför mallar från SKL (Sveriges Kommuner och Landsting) och hämtade information från praxis som Datainspektionen skapat samt utnyttjade eget nätverk (P2: 14). På LDC tittade verksamheten på en liknande analys som ett annat lärosäte genomfört och eftersom tjänsten samt avtalet var det samma gjorde de endast mindre justeringar vilket gjorde processen relativt enkel (P4: 14). LDC hade också i samma process åberopat ett avtal som SUNET tecknat med tjänsten Box. Det medförde att LDC inte behövde genomföra själva avtalsprocessen eller förhandla om personuppgiftsbiträdesavtal. Istället behövde de enbart genomföra en risk- och sårbarhetsanalys vilket de även löste genom att applicera en liknande analys, genomförd av Linköpings Universitet (P4: 5-8). Malmö Stad hävdar att risk- och sårbarhetsanalys enligt lag ska genomföras även om personuppgifter ska lagras inom egen inhemsk infrastruktur och menar därför att det oftast är samma säkerhetsaspekter som ska granskas oavsett om de anlitar molntjänstleverantör eller ej (P1: 16).

5.4.3 *Sammanfattning av statistik*

Samtliga intervjupersoner har vid ett eller flera tillfällen berört legala aspekter och utmaningar gällande tolkningar av de juridiska lagar som reglerar på vilket sätt och under vilka förutsättningar som data får lagras. Pensionsmyndighetens enkät indikerar att det bland svenska myndigheter finns ett glapp mellan de lagar som datainspektionen tillser och vad myndigheter faktiskt gör för att bemöta dessa. Exempelvis visar enkätundersökningen från Pensionsmyndigheten att endast cirka 35 procent av myndigheter alltid genomför en risk- och sårbarhetsanalys vid inköp av SaaS-tjänster (Appendix 8.2, tabell 6). Vidare är det cirka 40 procent av de tillfrågade som har tecknat personuppgiftbiträdesavtal med SaaS-leverantören (Appendix 8.2, tabell 7).

5.4.4 *Möjlighet till förhandsgranskning*

P1 menar att som ett resultat av den juridiska komplexiteten förenat med att börja använda en molntjänst finns det en utmaning i form av att någon verksamhet måste gå först i syfte att testa lagstiftningen. Ett exempel på detta är fallet med Ale Kommun som införskaffade molntjänsten Office 365 vilket underkändes av Datainspektionen. P1 menar att upphandlingen och genomdrivandet av en så pass stor process är förenat med kostnader och pekar på utmaningen ligger i att inte kunna få ett godkännande på förhand av datainspektionen (P1: 26). Som det ser ut idag genomför Datainspektionen först sina granskningar efter det att en tjänst har avtalats fram, vilket också innebär att det är först då som verksamheten kan få ett besked om huruvida deras avtal är förenligt med lagstiftningen (P3: 16). Enligt P1 kan det därför vara svårt att motivera en verksamhet och då framför allt inom offentlig sektor (P1: 26) att gå först i en sådan process, med avsikt att få fram ett beslut vilket sedan ytterligare verksamheter kan nyttja i form av att tillämpa Datainspektionens utlåtande på egen praxis (P3: 16).

5.4.5 *Skillnader privat kontra offentlig verksamhet*

P1 diskuterar också skillnaden mellan offentlig och privat verksamhet när det gäller behandling och omfång av personuppgifter. Offentliga verksamheter har enligt P1 ett större ansvar att skydda personuppgifter och sätta medborgarens integritet i centrum, dels eftersom de arbetar på uppdrag av medborgarna. P1 bedömer därmed att lagstiftningen är något tuffare mot offentliga verksamheter vilket också gör att de tar något mer seriöst på integritetsfrågor (P1: 40, 42). Datainspektionen har också nästan uteslutande granskat verksamheter inom offentlig sektor, men de tror samtidigt att användandet av molntjänster inom privat sektor är utbrett. I grund och botten är det samma regler ur en juridisk synvinkel för privat sektor. P3 menar att det i slutändan är en prioriteringsfråga för inspektionen, men att de har för avsikt att även granska den privata sektorn i större utsträckning (P3: 14).

5.5 Drift och kommunikation

5.5.1 Kommunikation med molntjänstleverantör

P1, som erhöll en mer säkerhetsteknisk yrkesroll, lyfte en problematisk aspekt rörande möjligheten att med egenförvaltd eller producerad mjukvara vistas i tredjeparts exekveringsmiljö (PaaS) (P1: 44). P1 menar att det vid egen hantering av exekveringsmiljö är betydligt enklare att arbeta med versionshantering för mjukvarukomponenter som är av betydande roll för den egna mjukvaran och att nya versioner i tredjepartsmiljön kanske inte annonseras eller upptäcks i samma utsträckning som vid egenförvaltd infrastruktur (P1: 44). Ett exempel på detta kan vara att en verksamhetskritisk funktion inom en infrastrukturtjänst modifieras över en natt, exempelvis att en tvåstegsautentiseringsfunktion för en viss tjänst skulle raderas eller modifieras, vilket för en egenutvecklard mjukvarutjänst som förlitar sig på den här funktionen skulle ha allvarliga konsekvenser (P1: 44). P1 menar därför att en utmaning i samband med detta är att upprätthålla adekvat kommunikation mellan verksamheten som använder molntjänsten och molntjänstleverantören i syfte att vara uppmärksam och förberedd på mjukvaruförändringar i molnmiljön (P1: 44).

5.5.2 Säkerhetskopieringshantering och rätten att bli glömd

Som ett resultat av det nya dataskyddsdirektivet, vilket träder i kraft 2018, kommer det att ställas nya krav på rätten till individers integritet (P3: 28). P1 menar att detta kommer innebära tekniska utmaningar i form av att versionshantering av säkerhetskopierad information vilken kan bestå av personuppgifter (P1: 28). Det nya dataskyddsdirektivet kommer innebära att individer har rätt till att bli glömda, det vill säga att få deras uppgifter raderade från samtliga lagringsplatser. P1 menar på att det i samband med detta finns en utmaning i att ha en ordentlig och strukturerad insikt i hur molnet och leverantören lagrar och säkerhetskopierar data (P1: 28). Vidare menar P1 att det därmed ställs höga krav på upphandlare, vilka är ansvariga för att dessa aspekter regleras i tillräcklig utsträckning, något som P1 menar definierar den här utmaningen (P1: 30).

5.6 Sammanfattning av resultat

Samtliga personer som intervjuats i den kvalitativa studien har varit delaktiga i eller haft viss insyn i en implementering av en molntjänstlösning där lagring av personuppgifter förekommit. Samtliga intervjuade personer har också på ett eller annat sätt arbetat gränsöverskridande mellan de informationstekniska och juridiska perspektiven, men med ett naturligt fokus på sitt huvudområde som ett resultat av sin respektive yrkesroll. De intervjuade har generellt goda erfarenheter och kunskaper gällande processen att ta steget ut i molnet, exempelvis har samtliga verksamheter hävdad, med undantag för Datainspektionen, att de har både personuppgiftsombud, personuppgiftsbiträdesavtal samt genomfört eller avropat en risk- och sårbarhetsanalys; något som krävs av lagstiftningen. Vidare uttryckte ingen av de intervjuade någon

större osäkerhet kring hur hantering av personuppgifter ska behandlas generellt enligt lagstiftningen. Den gemensamma bilden bland intervjupersonerna är att personuppgiftslagring regleras i tillräcklig omfattning genom PuL men att det uppstår frågetecken kring hur vissa aspekter av lagskriften ska appliceras i förhållande till en molntjänst. Framst är det problematiken kring tredje land som flera intervjupersoner pekat på, där det råder viss förvirring efter ogiltigförklarandet av Safe Harbour-avtalen vilket i sin tur har påverkat de verksamheter som har sin nuvarande lösning för lagring av personuppgifter i tredje land med stöd av Safe Harbour.

6 Diskussion

6.1 Dataintegritet

Ett genomgående tema i litteraturen innefattas av utmaningar förenade med att bevara datans integritet, något som beskrivs av King & Raja (2012), Loganayagi & Sujatha (2012) såväl som Sosinsky (2010). Studiens resultat, vilket såväl P1, P2 som P3 pekade på, visar på att en av de mer omfattande delarna av en verksamhets arbete med att börja använda en molntjänst omfattas av förhandsarbete i form av att utföra en risk- och säkerhetsanalys samt teckna ett personuppgiftsbiträdesavtal. Det huvudsakliga syftet med dessa två komponenter är att skydda datans integritet på ett sådant sätt att obehöriga personer inte kan få tillgång till uppgifter via exempelvis ett intrång. Peterson, Gondree & Beverley (2012) påstår att det finns en betydande komplexitet förenat med att teckna avtal där sekretessbelagd data lagras i andra länder än ursprungslandet; en bild som överensstämmer med verkligheten. Lagstiftningen, och därmed indirekt Datainspektionen, ställer enligt samtliga intervjupersoner stora krav på att molntjänsten måste kunna bevara datans integritet och att verksamheten kan följa upp och kontrollera detta. I anslutning till detta menar P1 att verksamheter upplever en utmaning i form av att teckna avtal ur ett integritetsperspektiv snarare än ur ett affärsperspektiv vilket även detta tycks överensstämmer med verkligheten.

Det finns tendenser att vissa verksamheter har en viss nonchalans vad gäller bevarandet av personuppgifters integritet, inte minst som P1 nämner att det kanske handlar om ett attitydproblem där verksamheter hellre lägger större vikt vid effektivisering än integritet vid tecknande av avtal. Detta styrks av Pensionsmyndighetens enkät vilken visar på att cirka 35 procent av myndigheter alltid genomför en risk- och sårbarhetsanalys vid inköp av SaaS-tjänster (Appendix 8.2, tabell 6). Vidare är det cirka 40 procent av de tillfrågade som har tecknat personuppgiftsbiträdesavtal med SaaS-leverantören (Appendix 8.2, tabell 7). När verksamheter drar sig för att göra risk- och sårbarhetsanalys samt teckna personuppgiftsbiträdesavtal blir utmaningen att bevara datans integritet allt större. Dock fann vi i vår empiri att samtliga intervjuade parter tar dessa processer på största allvar och därför går det inte att med säkerhet säga hur pass utbredd problemet är.

6.2 Datasäkerhet

Det finns till viss del två polariserade aspekter inom datasäkerhet i molntjänster som diskuteras inom litteraturen. Cheng & Lai (2012) menar på att molntjänstleverantörer ofta har större kunskap och finansiella medel till att implementera större säkerhetsåtgärder än vad ett företag med egen infrastruktur kan införskaffa. Men enligt P1 skapar det också en tillit och övertro till molntjänstleverantören som enligt resultatet kan vara förenad med större risk eftersom information inom molntjänst alltid ansvaras för av den personuppgiftsansvarige. Även om dessa

aspekter avtalas och granskas av Datainspektionen vid behov, är det fortfarande av stort intresse för den ansvarige att säkerhetsställa att den molntjänstleverantör som anlitas vidtar adekvata säkerhetsåtgärder för att förhindra de säkerhetsintrång som exempelvis obehörig dataåtkomst, vilket även påvisas av litteraturen (King & Raya, 2012; Loganayagi & Sujatha, 2012). Resultatet visar att verksamheter arbetar med att förhindra dessa säkerhetsrisker genom att ställa tydliga krav mot leverantörerna samt se till att användarna av systemen är välinformerade om hur de ska användas på ett säkert sätt.

6.3 Regelverk

Cheng & Lai påstår att den fundamentala arkitekturen av ett datormoln, det vill säga en infrastruktur med distribuerad lagring, har en direkt inverkan på vissa legala aspekter så som olika lands dataskyddsdirektiv (2012). Även King & Raja styrker denna uppfattning att tekniken skapar utmaningar för lagstiftare vilket leder till att det skapas ett glapp mellan ny teknik och gammal juridik (2012). Vår empiri visar att de som befinner sig i gränslandet mellan teknik och juridik har en viss förståelse för att juridisk praxis tar tid att ta fram, vilket gör att det finns en viss osäkerhet när ny teknik ska prövas legalt. Molntjänster för med sig ytterligare komplexitet eftersom det är en geografiskt gränsöverskridande teknik som lagstiftningen ännu inte har hittat en tillfredställande lösning på när det gäller behandling av personuppgifter. Eftersom att regelverket samtidigt ställer stora krav på anlitarerna av en molntjänst försvåras ytterligare processen att ta steget ut i molnet och där visar vårt resultat att offentlig sektor ofta avropar existerande avtal eller delar praxis inbördes. Dels för att det är en bekväm lösning, men också för att de bekräftat att de upplever svårigheter vid att driva en process för att ta steget ut i molnet eftersom det kan vara komplicerat och kostsamt. Därför intar kommuner till viss del en mer försiktig inställning och väntar kanske tills en viss tjänst fått godkännande istället för att själva driva på processen.

6.4 Drift och kommunikation

Svantesson & Clarke beskriver molntjänster som ett relativt nytt fenomen som bygger på omogen teknik och att detta ur ett organisatoriskt perspektiv kan ses som en utmaning (2010). Sandeep anser att molnets tekniska natur kan innebära att företag, som ett resultat av en tveksamhet gentemot trovärdigheten hos molntjänstleverantören, drar sig för att investera i molntjänster och markerar detta som en utmaning (2012). Detta överensstämmer väl med verkligheten och kan härledas till utmaningar inom drift och kommunikation. P1 nämner en problematik att med egenförvaltd eller producerad mjukvara vistas i tredjeparts exekveringsmiljö, vilket tyder på att verksamheten dras med utmaningar dels inom drift och administration av egen mjukvara i molnet och i och med det även kommunikation gentemot sin molntjänstleverantör. P1 säger att det är betydligt enklare att förvalta egenutvecklade applikationer på egen infrastruktur i kontrast till att nyttja molntjänster, vilket inte bara skulle kunna bero på verk-

samheters ovana att arbeta med molntjänster, något som tydlig indikeras av Pensionsmyndighetens enkätundersökning, utan även att molnteknik och PaaS:er är, i förhållande till verksamhetens konventionella infrastruktur, svåra att helt anpassa till verksamhetens ändamål. Exempelvis kommer det nya datadirektivet som träder i kraft 2018 innebära att verksamheter måste kunna leva upp till nya lagstadgade integritetskrav och därmed individers rätt till att bli glömda, det vill säga individers rätt till att få information om sin person raderad. Detta ställer ytterligare krav på kommunikationen mellan en verksamhet och molntjänstleverantör i form av att verksamheten måste kunna få insikt i hur molntjänsten säkerhetskopierar data samtidigt som verksamheten själv också måste driva sina molntjänster på ett sådant sätt att alla de avtal och krav som ställs uppfylls ur ett tekniskt perspektiv.

7 Slutsats

Studien ämnade att besvara följande forskningsfråga:

Vilka är de tekniska och juridiska utmaningarna för svenska verksamheter vid lagring av personuppgifter i molntjänster?

Under forskningens gång har vi strävat efter att precisera och artikulera de utmaningar som beskrivs av empirin och jämföra mot existerande forskning. Vår undersökning visar på att de finns flera tekniska och juridiska utmaningar för en verksamhet som avser att nyttja en molntjänst för personuppgiftslagring. Framförallt kan det konstateras att den tekniska arkitekturen bakom molnsystem bidrar till en svårtolkad lagstiftning. När den nuvarande lagen stiftades var molntjänsttekniken inte särskilt utvecklad och det var relativt enkelt att förhålla sig till PuL och relaterade lagar. Men i en global värld med gränsöverskridande avtal och tjänster behöver lagstiftningen anpassas snabbare för att hänga med i den tekniska utvecklingen. Vår undersökning visar att lagstiftningen inte gör detta, vilket skapar utmaningar för verksamheter. Den största juridiska utmaningen är därmed främst att kunna navigera inom en föråldrad lagstiftning samt lösa problematiken kring lagring i tredje land, vilket betonas i resultatet av vår undersökning som en stor utmaning.

Vidare ser vi att de tekniska utmaningarna med att nyttja molntjänster vid personuppgiftslagring för en verksamhet främst är kopplade till verksamhetens möjlighet att skydda uppgifter, kontrollera behörighet samt säkerhetsställa att molntjänstleverantören och eventuella underleverantörer vidtar adekvata säkerhetsåtgärder. Molntjänsttekniken i sig för även med sig utmaningar när det gäller möjlighet att begränsa avlyssning eftersom data kan transporteras, processas och lagras i olika länder, vilket ökar risken för att obehöriga kan ta del av informationen. Det kan också vara svårt för en beställare eller användare av en molntjänst att säkerhetsställa att data raderats enligt avtal eftersom det finns problematik med att veta om det finns eventuella säkerhetskopieringar då infrastrukturen i sig inte administreras av egen personal.

7.1 Rekommendation för vidare forskning

Vår forskning har belyst tekniska och juridiska utmaningar kopplat till molnlagring av personuppgifter. Studien fann även resultat i form av indikationer på utmaningar inom problemområden utanför de tekniska- och juridiska aspekten. Ett exempel på detta innefattas av att en verksamhet upplevde att det stöd som erbjuds en organisation innan verksamheten börjar nyttja en molntjänst är undermåligt, det vill säga att verksamheten inte kan bli granskad av Datainspektionen på förhand utan endast efter genomförd molntransformation (vilket nämns av P1 i transkriptkolumn 22). Därav finns det motiv till varför ytterligare forskning kan undersöka huruvida det finns utmaningar inom andra problemspekter såsom organisatoriska och ekonomiska. Det kan även vara av intresse för forskningen att skapa förståelse för vilken innebörd utmaningar har på verksamheter samt varför utmaningarna överhuvudtaget existerar.

8 Appendix

8.1 Intervjuguide

Tema	Syfte
Inledning	Syftet med den första och inledande delen av intervjun innefattades av frågor av enklare karaktär. Här var syftet att få en grundläggande förståelse för intervjupersonens bakgrund och roll i förhållande till problemområdet.
Nuvarande molnanvändande	För att resten av intervjun ska få ett meningsfullt ändamål inleder vi den empiriska insamlingen med att samla in information kring verksamhetens nuvarande molnanvändande, vad för typ av personuppgifter som lagras, hur det lagras, vilka produkter eller vilken plattform som används samt i vilken utsträckning verksamheten använder sig av dem.
Upphandlingsprocessen	Oavsett den utsträckning i vilken verksamheten använder sig av molntjänster har de enligt vår urvalsprocess ett ändamål om att göra det, därför är det intressant att samla in data om en planerad, pågående eller avslutande upphandlingsprocess för inskaffandet av molntjänster.
Upplevda utmaningar	Baserat på föregående avsnitt vill vi sedan samla in de upplevda utmaningar som verksamheten tror sig få, ha, eller ha haft i samband med implementationen av en molntjänst.
Kommande aktiviteter	Givet det empiriska data som samlats in under intervjun är det relevant att ställa några kortare frågor om hur verksamheten ämnar fortsätta sitt arbete med molntjänster.
Avslutning	Till sist avslutas intervjun med frågor som berör eventuell expansion kring ämnen som plockats upp tidigare under intervjun, följdfrågor som ett resultat av oklara eller ej förstådda svar samt eventuell diskussion kring vidare kontakt eller kontakt med andra intressenter som kan vara till relevans för intervjun i sig och problemets område.

8.2 Sekundärdata

Utdrag ur Pensionsmyndighetens enkätundersökning genomförd oktober 2015.

Din organisatoriska hemvist		
Answer Options	Response Percent	Response Count
IT-funktion	79,5%	120
Utvecklingsfunktion	1,3%	2
Verksamhetsfunktion	10,6%	16
Annan funktion	8,6%	13

Tabell 1: Din organisatoriska hemvist

Myndighetens erfarenheter av molntjänster						
Answer Options	Ingen	Liten	Medel	Stor	Vet ej	Response Count
Programvara som tjänst (SaaS)	28	36	60	16	1	141
Plattform som tjänst (PaaS)	80	36	14	5	2	137
Infrastruktur som tjänst (IaaS)	81	32	12	10	1	136

Tabell 2: Myndighetens erfarenheter av molntjänster

Använder myndigheten idag programvara som tjänst, SaaS?		
Answer Options	Response Percent	Response Count
Ja	78,3%	112
Nej	21,0%	30
Vet ej	0,7%	1

Tabell 3: Använder myndigheten idag programvara som tjänst, SaaS?

Motiv för att lägga dessa SaaS-tjänster i molnet?		
Answer Options	Response Percent	Response Count
Minskade kostnader	48,5%	47
Ökad flexibilitet	49,5%	48
Ökad skalbarhet	24,7%	24
Ökad tillgänglighet	41,2%	40
Ökad säkerhet	17,5%	17
Nya innovativa tjänster	25,8%	25
Snabbare implementering	39,2%	38
Minskat behov av egen IT-kompetens	51,5%	50
Annat:	18,6%	18

Tabell 4: Motiv för att lägga dessa SaaS-tjänster i molnet?

Vilken typ av information finns i dessa SaaS-tjänster?		
Answer Options	Response Percent	Response Count
Verksamhetsinformation utan personuppgifter	65,6%	61
Verksamhetsinformation med personuppgifter	54,8%	51
Verksamhetsinformation med känsliga personuppgifter	8,6%	8
Personaladministration	53,8%	50
Ekonomi	40,9%	38
Annan:	20,4%	19

Tabell 5: Vilken typ av information finns i dessa SaaS-tjänster?

Har ni genomfört risk- och sårbarhetsanalyser för dessa SaaS-tjänster?		
Answer Options	Response Percent	Response Count
Alltid	34,4%	32
Ibland	46,2%	43
Aldrig	19,4%	18

Tabell 6: Har ni genomfört risk- och sårbarhetsanalyser för dessa SaaS-tjänster?

Har ni tecknat personuppgiftsbiträdesavtal för SaaS?		
Answer Options	Response Percent	Response Count
Ja	39,8%	37
Nej	17,2%	16
Delvis	19,4%	18

Tabell 7: Har ni tecknat personuppgiftsbiträdesavtal för SaaS?

8.3 Intervjutranskribering

8.3.1 Malmö Stad

Verksamhet: Malmö Stad

Intervjuperson: P1

Yrkesroll: Arkitekt inom IT och säkerhet

Tid och plats: 10:00 till 10:45 måndagen den 25 april 2016, telefonintervju via Skype

Rad	Text
1	Vi tänkte inleda intervjun med att fråga om din yrkesroll inom Malmö Stad och vad den innefattar?
2	Vi har lite olika IT organisation inom Malmö men den centrala IT-organisation är den som vi kallar för IT-Malmö som sträcker sig över två olika förvaltningar egentligen. Det är utförarsidan med IT-service då som finns för serviceförvaltningen och sen så finns IT-enheterna alltså stadskontorets som tillhör kommunikationsavdelningen. Jag jobbar på enheten som heter IT-styrning och vi fungerar primärt som beställare och ska arbeta fram strategier styrdokument och peka riktningen för IT-arbete helt enkelt. Mitt jobb då som IT-säkerhetsarkitekt är att översätta de krav som kommer från lagstiftare, policydokument och verksamhetskrav och så vidare och försöka omvandla det till tekniska säkerhetslösningar och göra själva IT-säkerheten som är en del av informationssäkerhetsarbetet. Så det är det jag gör.
3	Hur pass utbredd är molntjänstanvändandet inom Malmö stad?
4	Ja, det beror lite på hur man definiera molntjänst. Alltså om man inkluderar hosting där data passerar någon annanstans så är det nog ganska utbredd om man tänker på typ Google, Amazon eller Microsoft Azure eller vad det nu är. Man får börja med att slå fast definition av vad man menar med molntjänst, om man även inkluderar hosting.
5	Det har vi gjort från vår sida, så det [hosting] är absolut en del av vår definition.
6	I så fall så är det nog ganska utbredd då många verksamheter använder system där antingen all eller delmängder av data bor hos en extern leverantör, alltså på någon annans dator helt enkelt. Så det finns lite överallt men däremot är det inte så särskilt vanligt när det kommer till känsliga personuppgifter, där är det väldigt begränsat. Men [icke-känsliga] personuppgifter finns givetvis lagrat, visserligen beroende på hur man definierar personuppgifter, men användarnamn, namn och den typen av uppgifter finns.
7	Okej, gäller detta då alla delar av Malmö stad, inklusive skola och kommunmyndighet?
8	Ja skolan är lite speciellt eftersom de har två ben inom sin organisation där den administrativa sidan huserar datan primärt hos oss där man använder en vanlig klient och ansluter till vår infrastruktur. Medans den pedagogiska delen använder man <i>Google Apps for Education</i> och där har då samtliga gymnasieelever ett konto och de allra flesta lärare har också sina konton och e-postadresser där. Så den pedagogiska delen lever i Google Apps for Education och den administrativa delen lever i intern infrastruktur.
9	Är Google Apps for Education något som ni har upphandlat fram?
10	Ja, här är ju problemet med en så stor organisation som Malmö. Vi har ju många olika politiska styrorgan Vi har ju kommunfullmäktige och så kommunstyrelse och sen var vi ett antal nämnder. Dels stadsdelsnämnderna men också tekniska nämnder, fritidsnämnd och kulturnämnd osv. Många av de här lever sitt eget liv vad det gäller upphandling och delvis styrning så exakt hur man gjorde upphandlingen Google Apps for Education kan jag inte svara på. Utan den frågan får man nog ställa till skolan eller skolförvaltningarna i det fallet. Jag var inte inblandad själva upphandlingen.
11	Finns det någon liknande upphandlingsprocess för molntjänster som du har varit med om?

12	Ja, vi upphandlar inte molntjänster så som molntjänster utan vi upphandlar funktionen och sen huruvida leverantören vill leverera tjänsten här <i>on-premis</i> eller i molnet är väl underordnat. Vi krävställer hur det behöver se ut om de ska ligga i molnet men vi har svårt att i offentlig upphandling specificera att det måste levereras just som en molntjänst.
13	Hur ser du på personuppgifter i förhållande till risk- och sårbarhetsanalys samt personuppgiftbiträdesavtal?
14	Det här har då domstolar prövat att antal gånger, just de här med personuppgiftbiträdesavtal som Malmö då till exempel har tecknat tillsammans med Google. Det har varit uppe på prövning ett antal tillfällen och nu har man kommit fram till, i den senaste revisionen, att det är "good enough". De duger och vi har inte fler synpunkter heller. Men det där är ju svårighet just med molntjänster så där får man vara väldigt tydliga med kravställningen och uppföljningen givetvis.
15	Upplever ni generellt att införande av molntjänster generellt kräver mer jobb än andra processer?
16	Jag vet inte om de är mer jobb, det handlar väl mer att arbetet sker på olika ställen. Om vi ska föra in ett nytt system där vi ska hantera personuppgifter så gör ju vi en risk- och sårbarhetsanalys på att hantera den här informationen. Där är det väl kanske inte så jättestor skillnad på om det sker i molnet eller om det sker i vår egen infrastruktur. Vi vill ha samma säkerhetsmekanismer runt det då och kraven är dem samma. Förutom då det här med att man inte får flytta personuppgifter till tredje land vilket är sådana saker som man får krävställa i upphandlingen. Men om vi gör bedömningen att leverantören uppfyller det som lagstiftaren kräver så ser jag inte att det är stor skillnad att hantera i molnet eller hantera det i egna nätverk.
17	Okej, intressant. Om vi kollar lite mer på tredje land, har ni något avtal idag som just berör det? Förlitar ni er exempelvis på den så kallade Safe Harbour-principen?
18	Nej, de har vi aldrig gjort eftersom att Safe Harbour är en självreglerande historia så har vi gjort bedömningen att Safe Harbour ensamt inte duger utan vi ställer högre krav på leverantörerna. Så vitt jag känner till så förvarar vi ingen data utanför Europa idag utan den data som finns stannar inom europeiska datacenter och så är det också med Microsofts molntjänster som vi kör tekniska piloter på och så vitt jag förstår är det samma sak med Google.
19	Innan vi började med vår studie så läste vi om ett fall i Ale kommun, som du kanske känner till, där de hade upphandlat Office 365 och därefter begärt en granskning av Datainspektionen. I granskningen fick de ett negativt resultat dels på grund att Datainspektionen inte tyckte att de tillräckligt kunde kontrollera de underleverantörer som Microsoft anlätade samt i vilka länder de fanns. Det var lite det som lyfte vårt intresse kring denna fråga och att försöka förstå hur verksamheter tänker kring den här problematiken. I våra ögon känns det som om det ställs väldigt höga krav på verksamheten, hur upplever du det?
20	Ja, det gör det och det kommer väl att ställas ännu större krav när den nya dataskyddsförordningen träder in. Nu är ju den formellt klubbad och nu har man två år på sig att ställa om. Men behandling av personuppgifter kommer att fungera på ett helt annat sätt i hela EU om två år än hur det gör idag. PUL blir ju också lite påverkat i och med det och då får man hitta en ersättare till det. Men just Ales kommun där så hade de gått igenom alltihop och den invändig man hade, om jag minns det här rätt, var väl precis som du säger att man hade inte tillräckligt insyn om vilka länder underleverantörer hade sin verksamhet i och det är något som jag har för mig att de har rättat till sedan dess. Jag tror att det här utlåtande kom i april/maj för två år sedan, under 2014. Så vitt jag förstår det så har man rättat till det här idag så det här är något som regleras i avtal.
21	Ja, det stämmer bra.
22	Men den frågan får ni ställa till Ale kommun. Men det här är ju lite problemet att de hade varit skönt om man hade både som myndighet och som företag någon man kunde vända sig till. Vi har tänkt göra så här, kan ni snälla komma med ett utlåtande om det är okej? Tyvärr så går det inte riktigt idag utan man får göra, tänka och klura och sen så får man utföra. Därefter får man fråga Datainspektionen. Nu har vi gjort så här, kan ni snälla granska det och då får man först ett utlåtanden i efterhand och det där

	är synd. Det borde gå att få ett förhandsbeslut, i alla fall på de här stora tjänsterna som rör Google, Amazon och Microsoft, där avtalen egentligen inte borde behöva ändras så mycket. Men de är svårt idag.
23	Vi får också uppfattningen att man [verksamheten] måste både vara relativt tekniskt kunnig och samtidigt ha juridiken på sin sida för att ta sig ut i den här världen.
24	Absolut och om man tittar på informationssäkerhetsområdet överhuvudtaget så pratade man inte så mycket informationssäkerhet för tio år sedan, då var de mer fokus på IT-säkerhet. Sen svängde det och nu pratar man informationssäkerhet och då glömmer man lite bort att detta ska omsättas i tekniska lösningar. Det räcker alltså inte bara att ställa krav utan man måste också följa upp att det görs. Så det är helt rätt man behöver kunna både teknik, juridik och verksamhet om man ska ta steget ut i molnet.
25	Det här problemet som vi talade nyss om, att verksamheten kan gå till datainspektionen först efter det att man börjat bruka molntjänster och alltså endast kan få ett redan implementerat system granskat, ses det som ett problem eftersom att man gör en stor investering och lägger ner mycket tid på att gissa sig fram bara för att få en smäll på fingrarna av datainspektionen? Upplevs som det som en utmaning i den här processen?
26	Ja, framförallt så är det ju så att någon måste gå först. Då har Ale kommun valt att göra det här för Office 365, så resten av kommunsverige kan ju bara tacka och bocka för att Ale kommun har valt att driva det. Någonstans där så kan man fundera på om det hade varit bättre att de stora kommunerna gjorde det istället för att lilla Ale kommun ska bära de kostnaderna. Å andra sidan kan man ställa sig frågan: "Är det kommunens uppgift att testa lagstiftningen eller borde de vara SKL [Sveriges Kommuner och Landsting] som borde först och få en sådan här sak prövat?". Här är väl ett av problemet med de här tillsynsmyndigheterna, att någon måste vara först. Någon måste bli granskad och så ligger det på en kommun att ta kritiken och genomföra den här processen. Det är ibland svårt att motivera de som ska fatta beslut om att det är något som vi borde gå i bräschen för, det vill säga "borde vi vara längst fram?". Det är en utmaning.
27	Om din roll som just säkerhetsarkitekt, vad ser du för tekniska problem och vad är det för aspekter du tittar på då i sådana här processer?
28	När man gräver ner sig i det här så finns det massor med grejer man kan invända kring och det beror lite på om man har teknikhatten på eller juridikhatten på sig. Men det som blir väldigt tydligt för organisationen eftersom vi fortfarande äger informationen vi lägger ut oavsett om vi låter Microsoft eller Google ta hand om infrastrukturen så är ju vi fortfarande ägare och ansvarar för den information som finns. Det gör att man måste vara väldigt tydlig i sin kravställning. Bristen på insyn i infrastrukturen kan ju vara en anledning till att man ska vara lite försiktig när det gäller känsliga personuppgifter och molnleverantörer. Nu med den nya dataskyddsförordningen så får vi se hur den ska tolkas och tillämpas. Jag tror att det finns en anledning att dra till bromsen lite om man nu är på väg att flytta ut i molnet. Det här med rätten att bli glömd exempelvis, som det trycks ganska mycket på i den nya lagstiftningen, kan bli ett litet problem om man inte precis har insikt i hur uppgifter sparas i backuper eller liknande.
29	Det är alltså svårt att kontrollera detta [backup och rätten att bli glömd] då?
30	Ja, det är det och det ställer ju höga krav på avtalen som skrivs och kraven när man gör upphandlingen. Det är i upphandlingskraven som man egentligen har möjlighet att ha en påverkan.
31	Kan man säga att verksamheter idag drar sig lite för att göra en flytt till molnet tills det här nya direktivet har gått igenom?
32	Ja, jag tror nog att vi [verksamheter generellt] kommer och göra förflyttningen från on-premise-lösningar därför att det inte är ekonomiskt försvarbart att driva egna datacenter när man kan köpa infrastrukturen på burk. Men där handlar det kanske om att lägga rätt information i molnet och behålla rätt information internt. Detta är inte bara för att man ska uppfylla lagstiftarens krav utan framförallt för att för myndigheten, men också för privata företag, så är ju det här en förtroendefråga. Även om vi har bra

	<p>avtal med våra molnleverantörer som säger det ena och det andra och hur saker och ting ser ut medan datainspektionen säger "det här är godkänt" så är det ju fortfarande en förtroendefråga, om inte medborgarna har förtroende för Microsoft som molnleverantör eller Google, eller Amazon eller vilka det nu kan vara så är det ju lite svårt att motivera att man har till exempel känsliga personuppgifter hos den molnleverantören. Och nu efter Snowden, vi har nog inte sett alla effekter av den läckan än även om det just nu är ganska tyst så är det väl bara en halv miss ifrån att en ny avlyssningsskandal blåser upp. Apple och FBI:s krav på att Apple skulle bygga in bakdörrar i sina mobiltelefoner till exempel och få hjälp att knäcka de där sakerna, sådana krav kommer ju komma igen och ju mer det pratas om det desto lägre förtroende upplever jag i alla fall att medborgare i Sverige får till, i det här fallet, framförallt amerikanska teknikleverantörer. Skulle det nu visa sig att Apple beordras göra det här eller att Microsoft, Google eller Samsung går ut och säger att "nä men såhär har vi gjort i enlighet med amerikansk lagstiftning men det gäller inte er kunder i Europa" då klurar man nog litegrann på "men om de kan göra så med sina telefoner, vad händer då om de kan göra det i sina molnlösningar eller i sina operativsystem man har på datorerna?". Eller vad det nu kan vara, så det är en förtroendefråga.</p>
33	<p>Vidare har vi tittat lite på vad gäller processering av data, att data exempelvis kanske lagras i ett EU-land för att sedan skickas till en server i Nordamerika för behandling. Detta skapar ju en slags extra komplexitet i frågan om var data hanteras, hur ser du på det?</p>
34	<p>Ja, där känner jag att det nog snarare handlar om en avtalsfråga där det beror av att du i avtalet skriver var datan ska lagras eller var datan ska lagras och behandlas. Det är ju avtalsfråga som inte borde vara så svår att komma till rätta med om man börjar skriva bra avtal och det är väl lite där problemet har varit, alltså att man är inte van att skriva avtal utifrån integritetsperspektiv utan man är van att skriva avtal utifrån ett affärsperspektiv. Och det är väl kanske sunt, men man säger ju att ju mer vi flyttar ut grejer, ju mer vi låter andra behandla information som vi äger, desto bättre måste man nog bli på att placera individen vars uppgifter man hanterar i centrum och väga och det är väl lite det den nya dataskyddsförordningen är till för. Det vill säga att tvinga både myndigheten, men framförallt företag skulle jag säga, att vikta individens rätt till integritet högre i förhållande till sin egen vinstmaximering, kostnadseffektivitet eller vad man nu har för anledning att göra den här outsourcingen eller den här flytten till molntjänsten. Så man behöver bli bättre på att skriva avtal och skriva avtal utifrån andra aspekter.</p>
35	<p>Hur kontrollerar ni att den personuppgiftsdata ni lagrar i molntjänster faktiskt fysiskt befinner sig inom de länder som är tillåtet enligt lagstadga och ert avtal?</p>
36	<p>Så vitt jag vet så ligger de hostingleverantörer och molntjänster vi använder för behandling av personuppgifter eller annat sekretesskyddat material i Sverige eller i Europa och det här är avtalsmässigt snarare än att vi exempelvis har ett system som granskar var datan finns. Att vi laddar upp information till Microsoft och sen kontrollerar att de inte skyfflar vidare någonstans bygger ju på avtal och rätt till revision. Detta är dock inte någonting som IT-organisationen ansvarar för utan det gör varje nämnd som sluter den här typen av avtal, vi har ju en statsrevision som ansvarar för den typen uppföljningar och det här är ju en aspekt som finns med i avtalen. Man ska ha rätt att göra den typen av granskning och där använder vi ett antal revisionspartners som kan vara behjälpliga vid den typen av uppföljning. Här ska man också komma ihåg att man kanske inte ska ha en allt för stor tilltro till de här teknikorganisationerna, faktum är ju så att skulle det visa sig att ett företag bröt mot ett avtal och flyttade på data eller på något sätt slarvade med datans placering där det enligt avtal endast fick förvaras i Sverige men istället flyttades till exempelvis Nordamerika, Kina eller Ryssland så tror jag att det skulle vara ett dråpslag för den organisationen. Tittar man på Google, Microsoft och Amazon som ju är de stora leverantörerna idag så är de väldigt noga och väldigt öppna med den här typen av behandling av information helt enkelt. Och jag tror att det kommer att bli ännu lättare för både företag och myndigheter att använda molntjänster framledes när den nya dataskyddsförordningen finns på plats eftersom det ställer väldigt höga krav som är kopplat till skadestånd och liknande. Idag, om du bryter mot personuppgiftslagen, händer det i ärlighetens namn inte sådär jättemycket annat än att man får kritik av datainspektionen, men om man börjar koppla viten till dessa lagbrott så uppstår det ju ett intresse hos både leverantörerna men också de som nyttjar molntjänsterna att det finns en transparens och att alla vet vad som gäller och hur datan behandlas. Både Microsoft och Google, som är de vi använder idag, är väldigt öppna med det här.</p>

37	Du arbetar ju med IT-säkerhet och molntjänster inom den offentliga sektorn, har du erfarenhet kring dessa frågor inom den privata sektorn och finns det i så fall några skillnader mellan dessa två?
38	Inte med den här typen av frågor men däremot så har jag ett ganska stort nätverk av kollegor som arbetar med ungefär samma sak inom privat sektor. Idag är det en väldig skillnad på att arbeta med IT och informationssäkerhet i offentlig sektor jämfört med den privata. Det gäller ju då just när det kommer till behandling av personuppgifter och hur det används, idag är det stor skillnad men jag tror att det kommer vara mycket mindre skillnad om fyra år.
39	På vilka sätt skiljer sig arbetet med IT och informationssäkerhet sig åt mellan offentlig och privat sektor?
40	Det finns exempel på lite det som jag tidigare var inne på, att man på den privata sidan kanske är mer villig att offra integriteten på effektiviseringens altare. Det är väl kanske mindre viktigt för en privat organisation idag att sätta medborgarens integritet i centrum medan det är någonting vi inom den offentliga sektor hela tiden utgår ifrån. Vi är ju en förtroendebransch på ett helt annat sätt och lagstiftandet är nog lite tuffare mot offentlig sektor än vad man är mot privat sektor.
41	Kan man säga att ni hanterar känsliga uppgifter i större utsträckning, exempelvis volym på register?
42	Ja, så är det väl och även om vi inom den offentliga sektorn har privata aktörer som i viss mån hanterar känsla personuppgifter åt oss. exempelvis privata vårdgivare, så utför de uppdraget på uppdrag av kommunen eller landstinget och i någon mån är ju vi då ansvariga för den informationen i alla fall. Det finns ju visserligen många privata företag som hanterar känsliga personuppgifter men de gör det inte på uppdrag av myndighet utan där är det oftast så att medborgaren har registrerat sig själv oavsett om de här uppgifterna är känsliga eller inte. Skyddade anställningar är ett exempel på känsliga personuppgifter som du har få av i företag, så där är det en uppgiftstypsskillnad och där är det nog framförallt även en skillnad i attityden till medborgare i överlag. I privat sektor är medborgaren nästan alltid kund och i offentlig sektor så är de ibland kund, ibland brukare men väldigt ofta uppdragsgivare så där tror jag att det finns en attitydskillnad.
43	Sammanfattningsvis kan man alltså säga att det finns en del utmaningar vad gäller ämnen kring lagring av personuppgifter i molntjänster ur ett integritetsperspektiv?
44	Ja, absolut och jag tror att lagstiftaren till sist kommer att hitta en nivå mellan teknik och integritet gällande var man ska ligga någonstans. Så att lagstiftningens minimikrav blir minst laguppfyllnad och att sedan allting därefter innefattas av förtroendebitar. Just där tror jag att när lagstiftaren blir mer mogen till att stifta lagar som speglar teknikutvecklingen så kommer det att bli lättare för privata såväl som offentliga myndigheter att göra flytta till molnet men vi befinner oss fortfarande i lite oprövat område. En av utmaningarna med molnet innefattas av att man får vänja sig vid att saker ibland kanske bara händer. Man har en tjänst som man tycker funkar på ett visst sätt och rätt vad det är så gör molnleverantören en förändring av tjänsten vilket resulterar i att helt plötsligt så ligger kanske inte de tekniska förutsättningarna på rätt ställe i förhållande till den information man lagrar. Här krävs det ju då att man har en kontinuerlig dialog med molnleverantörerna så att inte deras effektivisering, förändring av nyintroduktion av tjänst påverkar informationsintegriteten. Det här tar sig uttryck i tekniken, om vi har systemen liggande hos oss och det släpps en ny patch hinner vi testa den och analysera dess inverkan men i molnet så bara händer det. Rätt vad det är så har det kommit en ny version där då exempelvis stödet för flerfaktorsautentisering strukits. Det är alltså någonting som också ställer stora krav på de organisationer som gör flytten till molnet, en miljö där saker händer och där verksamheten har mindre kontroll över sin miljö.
45	I och med det nya datadirektivet, hur tror du att processen för verksamheter att börja nyttja molntjänster kommer påverkas, tror du att det kommer bli enklare eller mer komplext?
46	Jag tror inte att lagstiftningen i sig kommer att göra det enklare, däremot så kommer det att komma ett antal domstolsutslag och ett antal tillsynsärenden som i förlängningen kommer göra det enklare. Datainspektionen lär ju få ett förändrat uppdrag så jag tror att det kommer att bli enklare och jag tror också

	<p>att det kommer att ske en förflyttning hos organisationerna så att man använder molntjänster där det är vettigt att använda molntjänster. Där det inte är vettigt att använda molntjänster, det vill säga där information är för känslig eller där det blir för komplicerat att lösa ur ett avtalsmässigt perspektiv så tror jag att man kommer att välja att ha kvar den typen av information lokalt. Den här tokigheten som finns där molnförespråkare säger "nej men allt ska ligga i molnet" och folk som inte är riktigt redo att gå till molnet säger "nej nej vi kan inte lägga någonting där som vi inte kan posta på internet", jag tror att den typen av extrepositioner kommer att försvinna och att man tar en mer pragmatiskt syn på det och ju fler som blir pragmatiska desto lättare blir det att föra dialoger och lära sig av varandra.</p>
--	--

8.3.2 Helsingborgs Stad

Verksamhet: Helsingborgs Stad

Intervjuperson: P2

Yrkesroll: Jurist

Tid och plats: 15:45 till 16:10 tisdagen den 26 april 2016, telefonintervju

Rad	Text
1	Kan du börja berätta lite vad du gör som jurist för Helsingborgs stad?
2	Jag bistår i juridiska frågor och förvaltningar. Framst inom juridiska frågor som har koppling till skolan, alltså skoljuridiska frågor. Så därav min inbladning i just den här frågan när det gäller Google Apps for Education. För då kom det upp att man hade önskemål från verksamheternas sida att användas sig av Google Apps for Education just som ett pedagogiskt verktyg i det dagliga skolarbetet. Då uppkom den här situationen av att man skulle göra någon form för riskbedömning eller riskanalys om det var möjligt att genomföra det ur ett juridiskt perspektiv. Framförallt då för att det skulle innebära att personuppgifter skulle finnas i den här tjänsten vilket var bakgrunden till min koppling till tjänsten Google Apps for Education. Men som jurist i allmänhet så bistår man förvaltningar och bolag i juridiska frågor samt agerar ombud i rättsliga processer om det skulle uppstå ett sådant behov.
3	Kan du berätta lite mer om Google Apps for Education inom Helsingborgs stad?
4	Nu har man haft Google Apps for Education här i Helsingborg ett tag och syfte är nummer ett att utbyta pedagogisk information. Det är begränsat på det sättet vad som egentligen ska finnas i den molntjänsten. Det finns skriftliga instruktioner där det tydligt står vad som ska finnas där. Sen använder man andra system för att exempelvis dokumentera kunskapsutveckling. Så man får titta lite på dels vad det är för uppgifter som ska vara i tjänsten och om det är så att det är något som är känsligt och därefter säkerhetsställa att det är ett personuppgiftsbiträdesavtal. Det är de min granskning har gått ut på och när jag gjorde den bedömningen så gjorde jag det dels utifrån de vägledningsinstruktioner från Datainspektionen och tillsyner som de hade genomfört gällande Google Apps for Education i andra kommuner. Sen är det så att det är standardavtal så det är det man måste titta på när man sedan väl väljer en molntjänst. Men det juridiska perspektivet kopplar man på när man ser ett behov att utvärdera om det är ok utifrån ett juridiskt perspektiv samt kontrollera att all dokumentation vi behöver är på plats.
5	För att förtydliga, just Google Apps for Education, finns det personuppgifter i tjänsten eller är det mer avsett som ett pedagogiskt verktyg?
6	Ja, för att du skapar användarnamn. Elever och pedagoger har användarnamn vilket är en personuppgift, så som namn och efternamn. Sen beror de såklart på vad man gör i tjänsten pedagogiskt, alltså vilka uppgifter som kan finnas med där. Men visst finns det personuppgifter eftersom du måste skapa användarnamn med namn och efternamn.
7	Är det avsett för mer än den enkla typen av personuppgifter, exempelvis känsliga uppgifter?
8	Nej, det är inte tänkt att det ska finnas känsliga uppgifter i det och det måste man försöka säkerhetsställa genom att ha instruktioner om vad den här tjänsten är till för.
9	Kopplat tillbaka till risk- och sårbarhetsanalys, vad det något som ni gjorde?
10	Ja, den har Skol- och fritidsförvaltningen ansvarat för. Så de har genomfört en sådan analys där de då har tagit med de övervägande som jag har gjort utifrån det juridiska perspektivet.
11	Vad det några speciella aspekter av analysen som du upplevde som lite extra krångliga?
12	Nä, det som är viktigt som jag ser det är att man faktiskt ser över analysen och reviderar vid behov. Det är en sak att man måste hålla riskanalysen levande, sen ska det samtidigt framgå vad man ska använda

	det till, alltså omfattningen och så klart ändamålet. Det framgår av den risk- och säkerhetsanalys som har gjort i detta fall där tanken är att personuppgifter som inte omfattas av sekretess eller inte är känsliga, ska finnas där. Det är inte tänkt att känsliga uppgifter ska finnas med. Sen är en viktig del informationen utåt vilket innebär att man ska få information om att i och med att du använder den här tjänsten så kommer uppgifter som exempelvis namn och efternamn finnas i molntjänsten.
13	För att summera, det fanns inte riktigt något i den här processen som du upplevde som främmande eller speciellt utmanande?
14	Jo, jag hade inte fått den här förfrågan tidigare så det var en utmaning utifrån att det gällde en molntjänst och att det fanns ett behov. Så det är klart de var så att eftersom jag inte hade varit involverade i en risk- och säkerhetsanalys tidigare av den här digniteten. Så utmaningen var då att kunna stötta förvaltningen i den frågan utifrån ett juridiskt perspektiv. Men då finns det väldigt bra material och underlag från SKL (Sveriges Kommuner och Landsting) som var till stor hjälp. SKL har underlag eller en mall som man kan använda då när det gäller att göra en risk- och sårbarhetsanalys vid molntjänster i skolan. Så den kom till väldigt stor hjälp och även de beslut som fanns på området från Datainspektionen. Men också ett utbyte med en jurist i Malmö.
15	Som då hade gjort en liknande analys?
16	Ja precis.
17	Så man kan säga att ni förlitade er lite på som fanns på SKL men också genom tips och råd från andra som har gjort liknande analys?
18	Jag skulle inte säga att vi förlitar oss på dem utan alla gör sitt eget arbete. Men genom att det finns ett underlag eller liknande arbete så finns det goda exempel som man faktiskt kan jobba med i den egna kommunen. Så skulle inte säga att man förlitar sig på det utan man måste göra någon form för omvärldskoll själv när man hanterar en sådan här fråga. Vad finns det? Hur ser det ut? Vad är eventuell risker?
19	Just det, det är absolut intressant och värdefullt.
20	Det framgår också i den här risk- och sårbarhetsanalysen att den här mallen från SKL har tjänat som grundstomme och att den faktiskt har används, men sen måste man ju göra sin anpassning och det svarar egentligen Skol- och fritidsförvaltningen bäst för.
21	Du kanske nämnde det tidigare. Gick Google Apps for Education under Safe Harbour-bestämelsen?
22	Ja, för där var en koppling i avtalet att man tillämpade det som vid den tidpunkten bedömningen genomfördes var okej.
23	Hur kommer ni jobba framöver med detta eftersom Safe Harbour ogiltigförklarades i oktober 2015 av EU-domstolen?
24	Nu följer jag rättsutvecklingen och får se vad innebär för konsekvenser.
25	Så det tar lite tid innan det förändrats och slår igenom?
26	Ja precis.
27	Hur ser ni på den nya dataskyddsreformer som ska införas 2018? Är det någonting som ni ser i den som kommer förändra den här frågan just när det gäller personuppgifter och molntjänster?
28	Vi tittar på det och förbereder för den förändringen och i första skede handlar det om att titta på vad vi har för olika personuppgiftsbehandlingar för att säkerställa att ändamålet är tydligt och var det är för uppgifter. Vi får göra den här grundkollen igen och då får man titta på om det är någonting som man behöver ändra eller justera. Så att det här är ju fortfarande så pass nytt och att det ligger 2 år fram i tiden så har vi precis börjat ur ett juridiskt perspektivet titta på det. Så vi får se vart det landar.

29	Hur jobbar ni inom kommunen med personuppgifter generellt?
30	Hos oss har vi utsett ett personuppgiftsombud på varje nämnd och sen har vi en som också sitter centralt på stadsledningsförvaltningen, under den förvaltningen som jag också tillhör. Som då är sammankallade i ett nätverk så de träffas regelbundet där man då diskuterar den här typen av frågor där man från nätverkets sida har försökt underlätta för verksamheten genom att exempelvis göra gemensam anmälan för personuppgiftsbehandling om det är så att man ska behandla personuppgifter så det ser likadant ut. Att varje ombud ansvarar då att föra förteckningar över de behandlingar som finns. Så att de då förs diskussioner kontinuerligt. Så det är det jag kan beskriva utifrån mitt perspektiv.

8.3.3 Datainspektionen

Verksamhet: Datainspektionen

Intervjuperson: P3

Yrkesroll: Jurist

Tid och plats: 09:05 till 09:45 torsdagen den 28 april 2016, telefonintervju

Rad	Text
1	Berätta lite om din roll på datainspektionen.
2	Jag började på Datainspektionen 2009. Datainspektionen har tre operativa enheter, enheten för näringsliv och arbetsliv, enheten för myndigheter, vård och utbildning samt enheten för rättsväsendeförsvaret och kameraövervakning. Jag har under hela min yrkestid varit på enheten för näringsliv och arbetsliv och har först kommit i kontakt med molntjänster 2011. Då vi tidigare inte hade tittat på molntjänster gjorde vi ett enhetsövergripande projekt då där vi granskade molntjänster som användes av aktörer inom varje enhet för vilken jag var projektledare och var med och granskade. Då var jag även med och granskade myndigheters och skolors användning varför jag har en del inblick i den frågan. Sedan så har Datainspektionens granskning av molntjänster i överlag främst rört skolor och kommuners användning av molntjänster efter det och då har jag inte varit inblandad i det eftersom det inte faller på min enhet, sen har jag förstås sett vad de har gjort men inte varit med i själva granskningen.
3	Vad är Datainspektionens roll gentemot företag och myndigheter?
4	Som jag nämnde så har ju Datainspektionen tre operativa enheter och så har vi en administrativ enhet, nu är vi nog cirka 50 anställda, vi har pendlat mellan 45 och 50 men just nu är vi 50 och dels så är vi ju då tillsynsmyndighet över personuppgiftslagen men det finns ju också en mängd registerförfattningar som rör personuppgiftsbehandling som vi är också tillsynsmyndighet över. Sedan har vi också tillsyn och är tillståndsmyndighet över inkassolagen och kreditupplysningslagen, det faller främst på min enhet så det är sådant som jag också sysslar med. Sedan har vi också tillsyn över kameraövervakning på platser dit allmänheten inte har tillträde, det vill säga på till exempel arbetsplatser, flerfamiljsfastigheter och liknande. Det är en ganska gammal myndighet ändå, från 1973, vi har en generaldirektör som då är den som bestämmer och tar principiella beslut. Vi är flest jurister här men har också tre IT-specialister då det ofta handlar om säkerhetsåtgärder och IT-säkerhet och liknande i våra tillsyner. Dels så tillsynar vi, vilket vi kan göra både genom platsinspektion där vi går ut och tittar på hur det går till men det vanligaste är att vi har skrivbordsinspektioner där vi skriver frågor till den personuppgiftsansvarige som den då får svara på skriftligen. Sedan arbetar vi också förebyggande genom att hålla utbildningar, både egna och uppdragsföreläsningar och försöker att gå ut med information på vår webbsida och i olika broschyrer och skrifter och så vidare.
5	Har ni någon uppfattning om hur många inspektioner ni gör per år ungefär? Granskar ni mest skolor och kommuner när det gäller PUL?
6	Jag tror att det varierar lite över tid, vad gäller tillsyn av PUL, skolor och kommuner så är det mest i samband med molntjänster. Jag gjorde en liten koll här på vad vi har gjort som jag kan dra igenom så kanske ni kan se om ni har nytta av det. Vi hade den granskningen som jag ledde år 2011, då granskade vi tre olika aktörer. Det var Salems kommun, Brevo och Enköpings kommun och vi ville då titta på aktörer som använde en plattform [PaaS] och då använde Brevo Microsoft Azure och Salems kommun använde Google Apps och Enköpings kommun använde sig av Dropbox. Vi konstaterade en mängd brister hos samtliga aktörer och därför följde vi exempelvis upp Salems kommun i maj 2013 vilket också mynnade ut i den information om molntjänster som ni kanske har sett på vår hemsida. Det är i princip en sammanfattning av de brister vi hade sett i och med PUL och deras molntjänstanvändande.
7	Har du något exempel på vilka dessa brister var?
8	Bland annat så var det ändamålsbegränsning, personuppgifter får ju bara behandlas i särskilt uttryckligt specificerade ändamål. Vid outsourcing eller användande av en molntjänst så måste man se till att även den man använder sig av inte använder de har personuppgifterna för andra ändamål och då finns

	<p>det ju ett krav på personuppgiftsbiträdesavtal och att man skriver instruktioner till biträdet angående vad de får lov att göra med uppgifterna. I de här avtalen så fanns de inte en sådan begränsning att "ni får bara göra de här sakerna för det ändamålet vi har bestämt", utan där var det också för att utveckla tjänsterna och liknande, där sa vi då att detta inte var förenligt med PUL. Sen var det så också att dels så måste man ju då i det här avtalet ge instruktioner till hur biträdet ska behandla uppgifterna och man måste då också kunna kontrollera att biträdet följer de instruktioner man har gett och då fann vi att när det gällde lagring och gallring då var inte de här instruktionerna tillräckligt tydliga så det var någonting vi slog ner på.</p>
9	<p>Fanns det något som var kopplat till problematiken med lagring av uppgifter i tredje land?</p>
10	<p>Vid den tiden gällde fortfarande Safe Harbour och i alla fall Google hade anslutit sig till de principerna och jag tror att även Microsoft hade gjort det, det är också möjligt att de istället hade standardavtalsklausuler. Detta var dock inte någonting vi slog ner på, däremot slog vi ner på att den man anlitar, att där måste man ha ett sådant avtal där man kan säkerställa att de får instruktioner och att de följer dem, men om den i sin tur anlitar underleverantörer, då måste man ha samma kontroll på dem. I det läget så hade de inte kontroll över vilka underleverantörerna var och då kunde man ju inte heller ha kontroll om uppgifterna fördes över till tredje land, så det fanns det en sådan problematik. Och där fanns det ju en hel del problematik, det var inte bara överföring till tredje land utan det var även själva kontrollen av det. När vi följde upp Salem, vilket överklagades till domstol hos förvaltningsrätten som gick på vår linje, innebar det att det skapades lite domstolspraxis. Senare under 2013 inledde vi en tillsyn av Sol-lentuna vilka hade ungefär samma hantering som Salem där de inte heller hade något avtal, kunskap eller kännedom om hanteringen. Sedan så gick vi 2014 på Ale kommun och de hade ju då Office 365 och då var det ju den punkten som vi hittade, det vill säga att de inte hade kontroll på underleverantörerna. Vi checkade ju också då alla de sakerna som vi hade tagit upp i och med molntjänsterna så det var ju liksom mot de punkterna som vi tidigare hade hittat brister hos de andra, det var de som vi checkade av även mot Ale. Senare så i juli 2014 så följde vi upp vårt beslut mot Ale och då hade de informerat oss om hur de skulle åtgärda det här problemet, de hade en lista på var vilken biträdesman anlitas, för vad de skulle anlitas för och var de befann sig. Den listan avsåg de sedan att publicera på en webbsida så att den personuppgiftsansvarige skulle kunna gå in och titta på det här och att det är så de har svarat upp mot det här kravet. Det är ingenting som säger att det måste ske på en webbsida men är det en sådan här stor aktör med många personuppgiftsansvariga så kan jag tänka mig att det är det vanligaste. I juni 2014 så granskade vi Malmö som använde Google och då hade de ett nytt avtal men det var samma brister som vi hade sett tidigare hos Salem. Vi har även granskat Simrishamn i juli 2014 vilka också använde Google och det har vi också följt upp och då hade de ett nytt avtal igen och på det nya avtalet så hade vi inga synpunkter utan den granskningen gick de genom med. Det är så långt, de tillsynsärenden som vi har haft vad gäller molntjänster som riktar sig mot kommuner och skolor. Sen har vi haft lite andra, jag vet att vi har tittat på ett företag som heter Trustly som är en betaltjänstlösning och de använde också molntjänster. Molntjänster var inte det som var fokus för den inspektionen men i och med att de använder sådant så blev det också ett föremål för granskning, de använde inte någon av de stora molntjänstaktörerna utan de använde en mindre molntjänst.</p>
11	<p>Hur ser det ut i offentlig sektor kontra privat i själva granskningsarbetet?</p>
12	<p>Jag skulle säga att den heta potatisen just nu är den offentliga sektorn. Min erfarenhet är att det är däri-från vi får mest frågor just nu. Pensionsmyndigheten hade ett regeringsuppdrag som de nyligen redovisade vilket rörde just molntjänster i staten. Vi gör ju inga branschundersökningar eller liknande men de har ju gjort det vilket visade på just detta.</p>
13	<p>Ett företag som exempelvis ett försäkringsbolag, vilket ju kan ha en del personuppgifter, skiljer sig ett sådant företags förutsättningar för molntjänster gentemot en myndighet?</p>
14	<p>Det är en av de sakerna som vi försöker förmedla till samtliga verksamheter, att ur en juridisk synvinkel så skiljer ju exempelvis reglerna för outsourcing inte sig åt. Det är samma regelverk som auktoriserar PUL och för myndigheter är det ju ytterligare lagar och hittills i alla våra tillsynsbeslut rörande molntjänster så finns det ju den här skrivningen att det har aldrig rört känsliga personuppgifter som vi har granskat. Om man tittar i våra beslut gäller dessa under förutsättningen att det inte handlar om</p>

	<p>känsliga personuppgifter då inget av våra tillsynsärenden har innefattat det. Vid känsliga personuppgifter är det fler säkerhetsåtgärder som måste till och kanske större kontroll av sina biträden. Just när du nämner försäkringsföretag, vilka ju då oftast har väldigt mycket känsliga uppgifter, måste de ju då tänka lite mer på detta och där har vi än så länge inte kommit med någon vägledning vilket jag kan tro att de här organisationerna tycker är lite problematiskt. Vi säger ju att det är samma regler som gäller oavsett om ni har en molntjänst, outsourceat eller om ni har informationen i egna system med det är samma säkerhetsåtgärder som krävs. Är det dessutom känsliga uppgifter det gäller måste det ju utforskas vad för krav som gäller då, om det hade varit loggar och logguppföljning, åtkomstkontroll och så vidare blir det ju så att när det outsourceas så kanske man inte kan gå in och kontrollera hos biträdet hur det här genomförts. Då måste man ju ha sett till och också kunnat se om de har någon typ av kontrollverksamhet som gjort de här åtgärderna som måste till när det är känsliga uppgifter och att de kan lösas. Eftersom vi inte har några tillsynsbeslut så tror jag att det kan upplevas som lite jobbigt för de verksamheter detta är relevant för. Där har ju inte vi heller någon vägledning att ta fasta på, att vi inte kan titta tillbaka på andra verksamheter och säga "det här och det här har vi sett brister på, det här borde ni kolla på".</p>
15	<p>Hur kommer det sig då att ni främst kontrollerar kommuner eller myndigheter och att ni inte i samma utsträckning gör tillsyn mot privat sektor?</p>
16	<p>Från början så var det nog att det var svårt att veta vilka inom privat sektor som använder sig av molntjänster, kommuner och landsting har man större insikt över vad man gör i och med att vi har en offentlighetsprincip. Jag tror att det idag är mer utsträckt att det även är privata aktörer som använder sig av molntjänster. Så det är också en prioriteringsfråga där vi nu har valt att titta på kommuner och skolor där vi hoppas att vi ska komma med så mycket praxis så att man även ska kunna få vägledning i privat sektor. Vi är också inte så många här på datainspektionen så man vill ju inte jobba på två fronter och gör man det vill man absolut inte komma fram till olika saker. Det är ju också så att har vi en granskning av molntjänster just nu, är det den som blir vägledande och sen så tar nästa grej vid efter det. Men jag tycker absolut att det ligger i tiden att även titta på. Jag är inte säker på att det behöver vara privata objekt, men jag är övertygad om att känsliga personuppgifter finns någonstans där ute i molnet och då borde de vara bra att titta på det för att få praxis. Är det någonting som släpper till? Är det precis samma råd när vi granskar? Jag tror att de blir fler saker som man måste tänka på eftersom det är fler säkerhetsåtgärder som ska till när man behandlar känsliga uppgifter.</p>
17	<p>Vi snuddade lite på Safe Harbour där innan. Hur har Sverige och kanske omvärden reagerat på Safe Harbours-ogiltigförklarande? Vad är det som har hänt sedan oktober 2015?</p>
18	<p>Den här 29-gruppen som består av alla dataskyddschefer med undergrupper, de gav på sätt och viss tre månaders respit i oktober vilket betyder att organisation har tre månader på sig att ställa om. Under de tre månaderna så gjordes inga, vad jag känner till, inspektioner där vi tittade på och granskade företag som använder Safe Harbour. Sen kom det här Privacy Shield där EU-kommissionen gick ut med att de kommit överens med amerikanska företrädare om någonting som ska ersätta Safe Harbour-principerna. Men de är inte riktigt klart än, för som jag förstår är det en överenskommelse som inte på något sätt är rättsligt bindande. För de var det som var problematiskt i den här EG-rättsdomen av ogiltigförklaring så finns ju den lagstiftningen i USA fortfarande kvar. Så frågan är, och det är ju också det här Privacy Shield när 29-gruppen nu igen har det på sitt bord att utreda och komma med ett yttrande, hur det förhåller sig de här? Det har också dragit ut lite på tiden och det skulle komma tidigare i vår och det har de inte gjort ännu.</p> <p>De håller också på att se över användning av standardavtalsklausuler och Binding Corporate Rules för det har dataskyddsmyndigheten gått ut och sagt att man än så länge kan använda sig av och det är inte ogiltigförklarande i den domen. Det finns ju en sådan fråga, att för man över uppgifter till USA med stöd av dem så är det samma lagstiftning där som finns oavsett vilket stöd man för över uppgifter. Så det är också en fråga som är på bordet. Jag skulle nog säga att de är väldigt problematiska för de företag som lutar sig mot framförallt Safe Harbour-överföringar eftersom det är inte längre en giltig grund och där måste man hitta ett annat sätt eller sluta föra över uppgifterna.</p>
19	<p>Vi har pratat med några kommuner och fått en viss uppfattning att deras avtal fortfarande ligger mot Safe Harbour och att de väntar och ser vad som ska hända närmast. Vi har uppfattat det som att det är lite svårt att navigera i detta. Vad tror du om det?</p>

20	Ja, det är ju svårt att hitta en lösning om man för över uppgifter till USA även efter den domen och det är därför kommissionen gick ut med Privacy Shield vilket är väldigt intressant hur de ska kunna gå att lösas. Men det är ju på en EU-nivå och inte någonting som vi som dataskyddsmyndighet gör någonting på egen hand utan där får alla dataskyddschefer ha en gemensam ståndpunkt i frågan.
21	Vi har talat lite om det här med att ni bland annat jobbar för att förenkla processen för verksamheter som vill gå in och använda molnet där personuppgifter avser att lagras? Du nämnde tidigare att ni jobbar med att informera och fastställa praxis. Är det något ytterligare ni gör för att assistera verksamheter att gå igenom en sådan här process?
22	Ja, det är nog främst information och för att vi ska gå ut med ny information så sätter vi aldrig ner foten och säger; så här tycker vi att rättsläget borde se ut. Utan vi inspekterar alltid och kommer med ett tillsynsbeslut som är överklagbart, det är så ny praxis bildas. På det sätter måste vi gå ut och inspektera en aktör som kanske inte tycker det förenklar tillvaron att vi kommer dit men samtidigt är de det ända sättet för oss att komma med vägledning. Men säger vi någonting så måste de alltid vara överklagbart. Däremot den här 29-gruppen jag nämnde, de har ju möjlighet att komma med vägledning och de har också tagit fram ett papper som handlar om molntjänster där de ger vägledning som man ska titta på. Så där finns ytterligare lite saker utöver våra tillsynsbeslut och vår egen vägledning.
23	Vi pratade med en annan kommun och då diskuterades vi liknande frågor med en anställd inom IT. Hans uppfattning var att de krävdes att någon gick först ut i dessa frågor, exempelvis Ale kommun som var först ut med Office 365 så fick de se hur det rättsliga spelade ut. Hur ser ni på det?
24	Så som systemet ser ut så är det tänkt att den personuppgiftsansvarige ska göra en laglighetskontroll. Vad är det för något som krävs för den här personuppgiftsbehandlingen och titta på är det här det krävs? Nu ska jag gå och anlita en molnleverantör, jag tänker att det är det här som krävs och om jag anlitar den hör molnleveratören, upplever de att företaget lever upp de villkoren jag ställt redan i första ledet. Det som är så svårt är ju att det är standardiserade villkor och enskilda personuppgiftsansvariga har svårt att ge egna instruktioner, om de kommer fram till att de bör inkludera fler säkerhetsaspekter eller liknande? Då har de svårt att påverka tjänsten och det är något som är problematiskt med molntjänster där den starka aktören är biträdet. Så som lagstiftningen är uppbyggd är det den personuppgiftsansvarige som ska ha kontroll och se till att lagen är uppfylld och det var också en sådan sak som vi tittade på i den här granskningen av första projektet. Vad är det som är symptomatiskt för molntjänster? Ja det är ju för mycket tillit från den personuppgiftsansvarige att biträdet är så duktiga på det, så de kan lösa det men lagstiftningen kräver inte att de ska ha tillit utan att de ska ha kontroll och förstå vad de är det ska lösa. Man måste vara en bra kravställare och ställa krav och sen matcha de här kraven jag vill ha, levereras de åt den här tjänsten?
25	Är den viss mognadsprocess där hela verksamhetsverige ska anpassa ny teknik till lagstiftningen?
26	Ja, och jag tänker på att du hade som sista fråga där om hur jag tror att nya dataskyddsförordningen kommer påverka. Jag funderade på det i morse när jag läste din fråga. I övrigt så har jag inte satt in mig i den biten om säkerhet och biträde för vi håller på med processen att titta på förordning här på datainspektionen. Vi har delat upp de olika bitar och det är inte den biten som jag ska bli expert på men som det är idag så är det den personuppgiftsansvarige som är ansvarig och ska se till att lagen följs och alla skyldigheter ligger egentligen på den personuppgiftsansvarige med förordningen så inför man även skyldigheter och ansvar hos biträdet. Som det är idag så ligger det otroligt mycket på det här avtalet som den ansvarige ska teckna med biträdet, att den ser till att biträdet inte gör någonting mer med uppgifterna och behandlar dem på rätt sätt. Det finns ingen annan sanktionsmöjlighet, det finns ingen lag som säger till biträdet, du gör fel nu. Utan det är den personuppgiftsansvariges ansvar att se till att det inte blir fel. I den kommande förordningen så läggs det skyldigheter även på biträdet så då kommer det finnas lagstiftning som kräver att biträdet tar tillvara på enskildas rättigheter och att de har en säkerhetsnivå. Det tror jag kanske kan höja nivån även på molntjänsten vilket gör att de kanske blir lättare för de som anlitar dem.

27	Är det några speciella aspekter som du tänker på när verksamheter kontaktar er som de pekar på är svårt i den här processen?
28	<p>Nu har det ju gått fram till många att det är viktigt att styra biträdet genom avtal och instruktioner men jag tror för många som inte är jurister så känns det nog problematiskt. Varför är det så viktigt? Sen tror jag att bakgrunden till den lagstiftning som finns idag grundar sig inte bara på PUL utan där är EU-skyddet för de mänskliga rättigheterna och de grundläggande rättigheterna i EU:s stadgar. De ger ett skydd för privatlivet och där räknar man upp till exempelvis att personuppgifter endast får behandlas för specificerade ändamål och sen så finns ju dataskyddsdirektiven där detta uttrycks. Sen så har det implementerats genom PUL och det här gör ju att det är en ganska generell lag. Det står inte lagen när du använder en molntjänst ska du göra så här, utan det står när du behandlar personuppgifter. Man måste höja det lite till en teoretisk nivå. Det tror jag kan kännas problematiskt, de hade varit lättare om de varit specificerat men det är ju också för att den ska vara tidsbestående. Det här är generella principer men skydd för de mänskliga rättigheter och privatlivet vilket ska gälla oavsett vilken teknisk utveckling som kommer. Så att jag tror att företag tycker att det är lite abstrakt men bakgrunden till det är ju att det ska alltid ska kunna appliceras och där man säger att det kommit med i förordningen. Den är ju betydligt längre än vad både direktivet och personuppgiftslagen är och man kan säga att den praxis som utvecklas runt om i medlemsstaterna kodifieras till viss del genom förordningen så den kommer vara mer ordrik och mer beskrivande. Sen kanske den heller inte alltid kommer göra det lättare att ta till information för den är ju en politisk kompromiss mellan alla länder som måste tolkas vilket gör att det kommer nya problem med det.</p>

8.3.4 LDC

Verksamhet: LDC**Intervjuperson:** P4**Yrkesroll:** IT-chef**Tid och plats:** 11:00 till 11:20 tisdagen den 12 april 2016, telefonintervju

<i>Rad</i>	<i>Text</i>
1	Vi sitter med vår kandidatuppsats och tittar på utmaningar när man vill använda en molntjänst och där man vill lagra personuppgifter. Vi har fått information om att universitetet gått över till molntjänsten Box och därför har vi kontaktat dig.
2	Nyligen är ju relativt, det är ganska länge sedan, vi har kört Box nu i, kommer inte ihåg exakt när vi startade men ett bra tag. Men vi kan väl gå efter frågorna du skickade, så jag kan gå efter dem när jag pratar.
3	Kan du beskriva kort din roll för LU?
4	Alltså jag är ju IT-chef med titel och ansvar för den centrala IT:n på Lunds Universitet. Sen finns det mycket annat IT ute men man väljer ju om man vill använda oss eller om man vill ha något eget. Ni sitter ju på EHL (Ekonomihögskolan vid Lunds Universitet) och just EHL har ju valt oss som en helhetsleverantör och när vi tittar på anställda så hanterar samtliga på universitet. Men det är ju rätt centraliserad organisation så det ska man ha med sig. Men vissa saker kan jag ändå jobba som gäller för hela universitetet. Det är lite kort om min roll.
5	Vi har fått information att LU gått över till tjänsten Box, kan du beskriva varför och hur processen gått till?
6	Box, som jag sa det var en tjänst som togs fram av universiteten gemensamt, det var väl Chalmers som drev processen och den dåvarande CIO:n där och han gjorde det tillsammans med SUNET (Swedish University Computer Network) så det här det slutade med att behovsanalysen gjordes, där man behövde någon form av lagtjänst där man kunde dela mellan lärosätet.
7	Hur valde ni molntjänstleverantör?
8	SUNET gjorde helt enkelt en upphandling och då vann box, det var de som bäst kunde förmedla det som gällde kravspecifikation vid det tillfället och ja, sen tecknade SUNET det avtalet och sen kan universitet avropa mot det så vi har inte gjort någon egen upphandling mot någonting sådant härifrån utan vi bara hoppade på det som SUNET hade gjort.
9	Fanns det speciella hinder eller utmaningar vid valet?
10	När det gäller inre utmaningar så är det samma sak. Där fanns en upphandlare som var okej enligt de regler och lagar som finns och då var de ganska enkelt för oss, så vi slapp göra det jobbet själva.
11	Jaha, så det fanns redan ett färdigt upplägg som var godkänt och klart för er.
12	Ja precis, som vi bara kunde gå in på.
13	Genomfördes en risk- och sårbarhetsanalys vid val av molntjänst? Hur genomfördes i så fall denna?
14	När det gäller risk- och sårbarhetsanalys fick varje lärosäte göra det själv för att då säkra upp sig själva, det är ju ingenting som man förlitar sig bara på SUNET. Och för vår del så tittade vi på den sårbarhetsanalys som Linköpings Universitet hade gjort i det här fallet. Och vi gick igenom den och matchad den med våra krav och hittade inget annat än att vi kunde se att den också fungerade. Och det tredje är när

	det gäller PUBA (personuppgiftsbiträdesavtal) så är det ju i det här fallet SUNET som har tecknat personuppgiftsbiträdesavtal.
15	Okej
16	Så just den [forskningsfrågan] som ni har kommit på här är för oss ganska enkelt.
17	Ja jag förstår, så ni har egentligen inte gjort så mycket. Ni har inte varit så delaktiga i processen själva då kan man säga?
18	Nä det har vi inte. Det är så att det här är ett behov som vi kan avropa på ett enkelt sätt. Vi är trygga med att det följer lagar och regler och föreskrifter och allt vad som gäller så att vi hoppade på det och erbjöd det ut till de anställda på universitetet helt enkelt.
19	Okej. Så då har du inte heller koll på om det var några speciella utmaningar just vid upphandling här eftersom det handlade om personuppgifter.
20	Nä det var ju helt vanligt då SUNET drev upphandlingen.
21	Men hur fungerade det här generellt sätt om ni för LU här vill ha något nytt system eller upphandla, går det mycket centraliserat eller gör ni egna upphandlingar också?
22	Ja, alltså jag tycker att vi ska koncentrera upphandlingar och göra gemensamma upphandlingar på LU men visst där sker ju en del som sker ute men bättre och bättre så går det mot gemensamma upphandlingar för hela LU. I det fallet så handlar det om det finns någon tendens eller chans att det blir någon form av molntjänst eller del av molntjänst så får vi göra en risk- och sårbarhetsanalys och man får se till att man har PUL-aspekterna täckta.
23	Ja, precis.
24	För varje val. Det är så man får göra.

8.3.5 SUNET

Verksamhet: SUNET**Intervjuperson:** P5**Yrkesroll:** Systemförvaltare**Tid och plats:** 12e, 15e, och 20e april 2016, konversation över e-post

Rad	Da-tum	Av-sän-dare	Text
1	12 april 2016	Författarna	<i>Inledande förfrågan om intervju med intressant person på SUNET.</i>
2	15 april 2016	SUNET	<p><i>Kontaktpersonen önskar att svara på e-post varvid denne diskuterar öppet kring vår forskningsfråga; "Vilka är utmaningarna för svenska verksamheter vid lagring av personuppgifter i molnet"?</i></p> <p>Om vi avgränsar oss till upphandlingsdelen är frågan någorlunda avgränsad men det är inte en liten fråga på något sätt, försöker sammanfatta vad som gäller och hur det fungerar så kan vi se om vi behöver hitta en tid eller inte. I upphandlingen (som gjordes innan Safe Harbour ogiltigförklarades) krävdes eg. bara att företaget antingen lagrade data inom EU eller i ett "godkänt" tredje land (Safe Harbour) samt att företaget skrev på ett personuppgiftsavtal (bilaga till avtalet).</p>
3			Avtalsmässigt finns sen personuppgiftsbiträdesavtal mellan LU (<i>Lunds Universitet</i>) och SUNET och mellan SUNET och Box (<i>en molntjänstleverantör</i>), nu är det lättare att svara på hur det ser ut idag då vi är mitt i processen att gå över från Safe-Harbour till BCR(<i>Binding Corporate Rules</i>) så jag förklarar det upplägget och inte hur det såg ut tidigare. LU ger SUNET en fullmakt att å deras vägnar teckna personuppgiftsbiträdesavtal med de leverantörer som LU har SUNET-tjänster av (t.ex. Box). SUNET tecknar sedan ett PUBA (<i>personuppgiftsbiträdesavtal</i>) med Box som gäller för alla lärosäten som har Box-tjänsten (förenklat). I avtalet mellan LU och SUNET finns instruktioner för hur SUNET och SUNETs leverantörer får hantera LUs personuppgifter.
4			<p>LU har alltså två avtal med SUNET, ett för tjänsten Box och ett för personuppgifter där Box är en av tjänsterna. PUBA mellan LU/SUNET/Box hanterar de uppgifter LU av personuppgiftsansvariga för (namn, e-post, koppling) och gäller inte de personuppgifter en anställd lagrar i tjänsten (där är den anställda personuppgiftsansvarig och inte lärosätet).</p> <p>PUBA/IDPA/BCR är avtal och gäller (såklart) inte över enskilda länders lagar, amerikanska eller svenska staten har alltid rätt att begära ut information men det är en separat fråga i sammanhanget.</p>
5	20 april 2016	Författarna	<i>Vi tackar för svar och ställer en rad följdfrågor på de intressanta aspekterna personen belyst i tidigare konversation.</i>
6	20 april 2016	SUNET	<p><i>Kontaktpersonen besvarar våra följdfrågor med nedanstående svar.</i></p> <p>När och hur började SUNET övergå till användande och förvaltande molntjänster?</p> <p>SUNET har som många andra NRENS gått från att leverera nät till att leverera nät, integrationer/identitetsfederationer och tjänster, det är svårt att sätta ett datum på när SUNET började använda molntjänster då det är många olika tjänster och molntjänster är ett vagt begrepp. Box har varit en SUNET-tjänst sedan hösten 2012.</p>

7		<p>Hur har Safe Harbour-domen påverkat avtalsprocessen, så som den med Box? Tvådelat, avtalen vi har/hade med Box var inte enbart baserade på Safe Harbour men ogiltigförklarandet av Safe Harbour har lett till att vi behöver teckna nya avtal (vilket ändå skulle göras) som baseras på model clauses eller BCR istället. Vi hade alltså oavsett behövt teckna nya avtal och arbetet med PUBA mellan lärosäte-SUNET-leverantör var ett arbete som redan pågick, dock behövde bägge processerna ändras/anpassas.</p>
8		<p>Har avtalsprocessen det blivit enklare eller mer komplex för lagring av personuppgifter efter Safe Harbour-domen? I det stora hela är det samma som tidigare, ett "avtal" ersätts av ett annat, det innebär en massa avtalsarbete men väldigt förenklat så byter vi Safe Harbour mot BCRs och processen ser likadan ut.</p>
9		<p>Tycker du att det finns speciella hinder eller utmaningar i en sådan här avtalsprocess, kopplat till personuppgifter? Eftersom "alla" tjänster hanterar personuppgifter (t.ex. namn, e-post-adress) är det svårt att svara för enbart kopplingen till personuppgifter. Självklart tar det mer tid avtalsmässigt att ha en extern leverantör som måste ha PUBA men det är ett lagkrav så det finns inte något val, samma gäller t.ex. LOU (<i>lagen om offentlig upphandling</i>) vilket tar tid men som krävs för att köpa in tjänster.</p>
10		<p>Hur upplever du dagens regelverk och säkerhetskrav kring lagring av personuppgifter? Det beror på vilka regelverk och säkerhetskrav ni pratar om, PUL kräver att det finns PUBA (inklusive instruktioner till UB) och det är väl inarbetat hos de flesta men sen finns det såklart interna såväl som lagmässiga krav på hantering av skyddsvärd och känslig information som är en helt separat fråga. Vad det gäller "vanliga" personuppgifter tror jag inte något lärosäte eller någon leverantör inte har rutiner och mallar klara för personuppgiftshantering (standardavtal, PUBA, instruktioner).</p>

Referenser

- Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee, G., Patterson D.A., Rabkin, A., Stoica, I. & Zaharia, M. (2009). Above the Clouds: A Berkeley View of cloud computing, *University of California at Berkeley*. Technical Report EECS-2009-28, University of California
- Avram, M-G. (2014). Advantages and challenges of adopting cloud computing from an enterprise perspective. *Procedia Technology*. vol. 12, ss.529-534
- BBC. (2014). Edward Snowden: Leaks that exposed US spy programme *BBC News*, 17 januari 2014. Tillgänglig online: <http://www.bbc.com/news/world-us-canada-23123964> [Hämtad 13 april, 2016]
- Cheng, F-C. & Lai, W-H. (2012). The Impact of Cloud Computing Technology on Legal Infrastructure within Internet - Focusing on the Protection of Information Privacy. *Procedia Engineering*. vol 29, ss 241-251
- Court of Justice of the European Union (2015). Press Release No 117/15, 6 oktober 2015, Tillgänglig online: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf> [Hämtad 11 april 2016]
- Datainspektionen. (2016). EU:s dataskyddsreform, Tillgänglig online <http://www.datainspektionen.se/lagar-och-regler/eus-dataskyddsreform/> [Hämtad 2 maj 2016]
- Datainspektionen. (2014). Tillsyn enligt personuppgiftslagen (1998:204) - Behandling av personuppgifter i molntjänsten Office 365. 25 april 2015. Diarenr 1475-2013 Tillgänglig online: <http://www.datainspektionen.se/Documents/beslut/2014-04-28-ale-kommun.pdf> [Hämtad 20 mars 2016]
- Datainspektionen. (2011). Tillsyn enligt personuppgiftslagen (1998:204) - Brevo AB. 28 september 2011. Diarenr 574-2011. Tillgänglig online <http://www.datainspektionen.se/Documents/beslut/2011-09-30-brevo.pdf> [Hämtad 27 april 2016]
- Datainspektionen. (u.å.). Molntjänster, Tillgänglig online <http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/molntjanster/> [Hämtad 12 april 2016]
- Datainspektionen. (u.å.). Safe Harbor, Tillgänglig online <http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/internationell-verksamhet/safe-harbor-domen-far-stora-konsekvenser/> [Hämtad 12 april 2016]
- De Hert, P., Papakonstantinou, V., & Kamara, I. (2016). The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection. *Computer Law & Security Review*. vol. 32, no. 1, ss.16-30
- Endrei, M., Ang, J., Arsanjani, A., Chua, S., Comte, P., Krogh, P., Luo, M., & Newling, T. (2004). Patterns: Service-Oriented Architecture and Web Services, *IBM Redbook*, Tillgänglig online: <http://www.redbooks.ibm.com/redbooks/pdfs/sg246303.pdf> [Hämtad 8 april 2016]

- Europaparlamentet. (1995). Europaparlamentet och rådets direktiv 1995/46/EG, 24 oktober 1995 Tillgänglig online: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:sv:HTML> [Hämtad 8 april 2016]
- European Commission. (2016). EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield. Pressmeddelande, 2 februari 2016, Bryssel
- European Commission. (2015). Överenskommelse om kommissionens reform av EU:s uppgiftsskydd stärker den digitala inre marknaden. Pressmeddelande, 15 december 2015, Bryssel
- Eurostat. (2014). Cloud computing - statistics on the use by enterprises, november 2014 http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_statistics_on_the_use_by_enterprises [Hämtad 11 april 2016]
- Jacobsen, D. (2002). Vad, hur och varför? - Om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen. Lund: Studentlitteratur AB
- King, N. J. & Raja V.T (2012). Protecting the privacy and security of sensitive customer data in the cloud. *Computer law & Security review*. vol 28. ss. 308-319
- Loganayagi, B. & Sujathaa, S (2012). Enhanced Cloud Security by Combining Virtualization and Policy Monitoring Techniques. *Procedia Engineering*. vol 30 ss. 654 – 661
- Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. & Ghalsasi, A. (2010). Cloud Computing - The Business Perspective. *Decision Support Systems*. vol. 51, no. 1, ss.176-189
- Mason, R. & Rodriguez, A. (2009). Method and system for versioned file system using structured data representations. US Patent 8566362 B2
- Mesnier, M., Ganger, G.R. & Riedel, E. (2003). Object-based Storage Architecture. *IEEE Communications Magazine*. Augusti 2003
- Pensionsmyndigheten. (2016a). Molntjänster i staten, En ny generation av outsourcing. Tillgänglig online <https://secure.pensionsmyndigheten.se/24304.html> [Hämtad 13 mars 2016]
- Pensionsmyndigheten. (2016b). Bilaga: Juridisk analys molntjänster i staten. Tillgänglig online <https://secure.pensionsmyndigheten.se/24304.html> [Hämtad 13 mars 2016]
- Peterson, Z., Gondree, M. & Beverly, R. (2011). A position paper on data sovereignty: the importance of geolocating data in the cloud. *HotCloud'11 Proceedings of the 3rd USENIX conference*. ss. 9-9
- Sandeep, S. K. (2012). A combined approach to ensure data security in cloud computing. *Journal of Network and Computer Applications*. vol 35, ss. 1831–1838
- SFS 1998:204. Personuppgiftslag.

Sosinsky, B. (2012). *Cloud Computing Bible*, Indianapolis: Wiley Publishing Inc

Stamford, C. (2013). Gartner Says Nearly Half of Large Enterprises Will Have Hybrid Cloud Deployments by the End of 2017, Tillgänglig online <http://www.gartner.com/newsroom/id/2599315> [Hämtad 2 april 2016]

Svantesson, D. & Clarke, R. (2010). Privacy and consumer risks in cloud computing. *Computer Law & Security Review*. vol 26 ss. 391-397

Quinn, B., & Arthur, C. (2011). PlayStation Network hackers access data of 77 million users *The Guardian*, 26 februari 2011. Tillgänglig online: <https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data> [Hämtad 12 april, 2016]