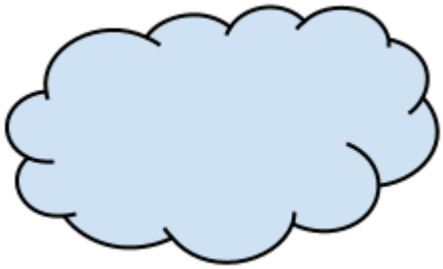
GÖTEBORGS UNIVERSITET

.



MoIntjänster och förtroende

En kvalitativ studie av hur förtroendet kan ökas för moIntjänster

Cloud services and trust

A qualitative study on how to increase trust in cloud services

Patrik Murman
Christopher Rynner

Kandidatuppsats i informatik

Rapport nr: 2014:060
ISSN: 1651-4769

Göteborgs universitet
Institutionen för tillämpad informationsteknologi
Göteborg, Sverige, Maj 2014

Abstrakt

Molnet har tagit IT-världen med storm och skapat nya möjligheter för användare att på ett smidigt sätt komma åt olika tjänster. Molnet erbjuder en uppsjö av olika tjänster som både passar stora och små organisationer. Utvecklingen går fortfarande framåt och fler organisationer börjar eller håller på att migrera till någon form av molntjänst. Detta medför också att en rad frågor och problem uppstår, nya som gamla. IT-branschen har belyst problemet att organisationer har lågt förtroende till molntjänster, eftersom det handlar om att låta en extern part sköta något som organisationen innan har skött själv. Denna uppsats huvudområde är hur organisationer skall få ökat förtroende för molntjänsteleverantörer. Vi ställde frågan:

”Hur skapas ökat förtroende mellan kund och molntjänstleverantör?”

Vi genomförde en kvalitativ intervjustudie med personer från tre olika större företag som har anknytning till molntjänster och en litteraturstudie till ämnen som vi ansåg relevanta (molnet, juridik, informationssäkerhet och förtroende). Vi vill med vår studie visa på att förtroende har en viktig roll i molntjänster eftersom det berör oftast två olika parter, kund och leverantör. En låg grad av förtroende kan bidra till att organisationer inte migrerar till molnet. Resultatet av denna undersökning är att det inte bara finns en låg grad av förtroende till molntjänstleverantörerna utan också till själva tjänsterna vilket bland annat beror på uppdaterade lagar och uppmärksammade säkerhetsbrister. Vi fann att molntjänstleverantörerna kan förbättra sitt anseende genom att vara öppnare och arbeta närmare kunden samtidigt som kunden måste ta sitt ansvar.

Nyckelord: *Molntjänster*, *förtroende*, *juridik*, *säkerhet*

Abstract

Cloud Computing has taken the IT world by storm and has created new opportunities for users to seamlessly access different services. The cloud offers a variety of different services that suit both large and small organizations. Cloud computing is still in development and many organizations are beginning to consider or have implemented a form of cloud service. This also leads to a series of questions and problems, both new and old. The IT industry has highlighted a problem in organizations confidence in cloud services, because a third party will be handling a part of the organization that the company has previously handled themselves. This papers main focus is how to increase organizations trust in cloud service providers. We asked the question:

"How can trust be increased between customer and cloud service provider?"

We conducted a qualitative study with people from three large companies related to cloud services and literature into topics that we considered relevant (cloud, law, information security and trust). The purpose of this study is to show that trust plays an important role in cloud services. It affects mostly two different parties, customer and supplier. A low level of trust can contribute to organizations opting not to use a cloud service. The findings of this paper is that there is a low level of trust not only towards the providers, but also towards the cloud services themselves, due to outdated laws and largely noted security issues. We found that the cloud service providers can do their part by working more transparently and closer with the customer, along with the customer themselves taking responsibility.

The report is written in Swedish.

Keywords: *Cloud services, trust, law, security*

TACK

Vi vill tacka alla informanter för all hjälp på vägen och all den viktiga information som ni har delat med oss.

Tack Jan, Malin, Peter, Gunnar, Jonas, Marta, Magnus, Samir, Marina och David.

Vi vill också tacka vår handledare, Lennart Peterson som har hjälpt oss med uppsatsen.

Stort tack!

Innehållsförteckning

1. Inledning

Cloud Computing eller molntjänster har blivit den nya flugan och det alla verkar sträva efter. Det har blivit så stort att branchföretaget IDG har en egen tidning om det (Cloud Magazine 2014). Privat använder de allra flesta molnlösningar numera i och med att både iPhone och Android sparar data i respektive molnläsning. Det finns många olika sorters molntjänster och typer av moln. Kortfattat innebär det att datan som hanteras inte sparas lokalt på den dator som används, utan lagras genom internet, molnet, på en server någon helt annanstans och som är tillgänglig när som helst, var som helst. Trots denna hype och all uppståndelse i tidningar och media hade vi relativt svårt att finna företag som utnyttjade molntjänster till fullo. Vi ställde oss då frågan varför inte företagen vill utnyttja detta som enligt branchmedia och experter verkar så bra och verkar vara framtiden. Vi fann en hel del tidigare kandidatuppsatser i ämnet (Hassan 2011; Älmeblad 2011; Höcke, Pihlström & Helenius 2012) och fick bland annat utifrån dessa inspirationen till att ställa frågan varför inte företagen litar på den nya tekniken i molntjänster. Vi känner att efter ha läst en del av detta att det generellt finns en okunskap angående molnet, kombinerat med det erkända motståndet till förändring som hindrar företag från att hoppa på molntåget. Det har kommit ut rapporter inom branchmedia och populärmedia som påvisar att många är skeptiska och tveksamma till molnet (MyNewsDesk 2014; Mattmar & Holmin 2013; Åhlin 2013). Vi vill i vårt arbete ta reda på hur företagen kan bli mer positivt inställda till molnet och hur de ska få en ökad tillit till molntjänster.

1.1 Bakgrund

De senaste åren har molntjänster vuxit och blivit en allt mer populär teknologi som används av både stora och små organisationer. Det är fortfarande en teknologi som inte är fullt utvecklad utan att det fortfarande sker utveckling inom området. För att få en uppfattning hur populärt molntjänster är räcker det att surfa in på några svenska IT-hemsidor (Computer Sweden, Techworld, CIO Sweden, Ny teknik med flera), där finns det många artiklar och diskussioner om molntjänster. Görs en sökning på google med sökordet “molntjänster” så dyker det upp 284 000 sökresultat som belyser olika områden inom molnet (Google 2014). Det kan vara allt från organisationer som vill leverera tjänster till kunder eller hur en molntjänst fungerar. Det som också belyses är problem och frågor som rör molntjänster. Det kan vara frågor som rör det juridiska perspektivet eller hur informationssäkerheten fungerar kring en viss tjänst.

Molnet gör det möjligt att använda resurser via internet istället för att de används lokalt. Tjänster innefattar applikationer, nätverk, plattformar, lagring, servrar, databaser med mera, det vill säga det som tidigare fanns i organisationens serverhall finns nu istället tillgängligt via internet. Vilket medför en större resurseffektivitet eftersom organisationen väljer vilka tjänster som skall användas, som exempel att en organisation använder en databas på en server så används bara den tjänsten. Det som används det är vad som betalas för (Edvardsson & Frydlinger 2013).

1.2 Syfte

Syftet med denna studien är delvis att belysa hur viktig förtroendefrågan är vid upphandling och införskaffande av främst molntjänster, men även andra internetbaserade tjänster. Ett annat syfte är att skapa ökad kunskap och medvetenhet generellt angående moln och molntjänster. Syftet är också att ta reda på vad som kan göras för att öka förtroendet och göra det lättare för både kunder och molntjänstleveratörer att skapa ett affärsförhållande som både kan dra nytta av. Intressenter till uppsatsen är organisationer som är nyfikna på molntjänster eller håller på att migrera över till molnmiljön samt organisationer som vill förbättra sin kontakt med molntjänstleverantören.

1.3 Frågeställning

Utifrån ovanstående bakgrund och introduktion kom vi fram till följande frågeställning:

Hur skapas ökat förtroende mellan kund och molntjänstleverantör?

1.5 Avgränsningar

Undersökningen i studien är begränsad till tre större företag. Ekonomins inverkan på förtroende har inte tagits med i denna uppsats. Undersökningen som genomfördes var endast av kvalitativ sort och inga kvantitativa metoder har använts vid undersökning av förtroendenivån hos molntjänstleverantörer.

2. Metod

I detta avsnitt presenterar vi hur vi gått tillväga för att genomföra vårt arbete och komma fram till resultatet. Det kommer inkludera vilket förhållningssätt vi haft under arbetet, vilka slags metoder vi använt oss av för att komma fram till resultatet och även en kort analys av metodvalen. Som utgångspunkt i val av metoden har vi använt oss av Patel och Davidsson (2013). Vi har också i slutet av avsnittet en modell där vi förklarar hur teorierna hänger ihop och varför vi anser de är viktiga.

2.1 Vetenskapligt förhållningssätt

Enligt Patel och Davidsson (2013) finns det främst två olika inriktningar av forskning: kvantitativ forskning och kvalitativ forskning. Kvantitativ forskning innebär forskning i form av statistiska, mätbara hypoteser och resultat. I kvalitativ forskning, som vi valt att arbeta med, ligger fokus på så kallade ”mjuka data”, i detta fall i form av intervjuer och analyser av inhämtat textmaterial (ibid).

Enligt Patel och Davidsson (2013) är syftet med en fenomenografisk analys att studera hur fenomen i omvärlden uppfattas av människor och att hur de agerar utifrån dessa uppfattningar. Om vi går tillbaka till frågeställningen: ” *Hur skapas ökat förtroende mellan kund och molntjänstleverantör?”* så betyder detta alltså att vi studerar hur ett fenomen, molnet, uppfattas av människor eller kunder för att sedan studera hur de agerar utifrån detta. Precis som Patel och Davidsson (2013) hävdar, har vi i vårt fenomenografiska arbete jobbat med öppna, kvalitativa intervjuer där den eller de intervjuade fått beskriva sin uppfattning av det fenomen vi studerar. Efter intervjuerna har vi studerat dessa, för att finna likheter eller skillnader i dessa, med andra ord en induktiv process. Vi utgår alltså inte från en färdig teori som ska testas, utan målet är att skapa en trovärdig och lokal teori utifrån empirin i vårt unika fall (ibid).

För att genomföra studien har vi använt två olika forskningstekniker som tillvägagångssätt. Att använda en enda kände vi skulle vara för endimensionellt och vi tror att det ger mer när det går att kombinera olika tekniker. På så sätt genereras ett trovärdigare resultat. De tekniker vi använt oss av är en *litteraturstudie* och *intervjuer* med relevanta personer.

2.2 Litteraturstudie

För att få kunskap i ämnet och för att kunna ställa vårt resultat från intervjuerna mot något krävdes först en litteraturstudie. Det är från denna vi har hämtat kunskap om både molnet och allt som hör till och om förtroende. Litteraturstudien är något som gjorts genomgående under

hela arbetet, då vi först efter att ha fastställt vårt problemområde började söka i litteratur för akademiskt relevanta problem. När vi funnit detta och skapat problemformuleringen fortsatte litteratursökningarna, då både djupare och mer utvidgad kunskap i ämnet krävdes. Litteraturen har främst sökts och hämtats ifrån Göteborgs universitetsbibliotek och sökningarna har gjorts online. Därifrån har vi kunnat hämta en stor mängd tidskrifter, rapporter och artiklar om vårt valda ämne. Nästa steg var att välja ut vilken litteratur som passade bäst in för vårt valda ämne och utifrån det fick vi fram den litteratur som krävdes för uppsatsen. Vi har främst tagit stöd i andra kanditatuppsatser, för att sedan använda de källor vi fann där. Vi har också använt ett par tryckta böcker och någon enstaka tidskrift för att få fram den kunskap som krävdes för kandidatuppsatsen.

2.3 Intervju

Vi har i vårt arbete genomfört tre intervjuer, varav en av dessa är en gruppintervju med en fokusgrupp på fyra personer. Då det var svårt att få tag i företag eller organisationer som ville ställa upp på detta, och med den tidsram vi hade, valde vi att varken studera ett specifikt fall eller göra ett stickprov utan de intervjuade faller under så kallade tillgänglig grupp (Patel & Davidsson 2013). Det innebär också att resultaten av intervjuerna inte kan gälla generellt för företag eller personer insatta i ämnet, utan endast som underlag för att stödja teorier (ibid). Innan intervjuerna genomfördes var vi självklart noga med att följa de etikregler som formulerats av vetenskapsrådet (VR 2009). Det vill säga att de intervjuade är informerade om det vi syftar forska om, de har alla samtyckt till att medverka, intervjumaterialet kommer endast nyttjas i forskningsändamål och till sist de intervjuade ska ges möjlighet till konfidentialitet. I den sista punkten hade de intervjuade olika grad av krav på konfidentialiet. Detta innebar emellertid inga problem för uppgiften, då vi inte ansåg att de intervjuade eller deras företag specifikt behöver omnämnas i rapporten. Intervjufrågorna (Bilaga 1) var baserade på låg grad av standardisering och strukturering (Patel & Davidsson 2013). Detta för att ge den intervjuade mycket svarsutrymme och för att anpassa intervjun i den riktning samtalet tog, alla frågor ställs med andra ord inte i samma ordning till de intervjuade. Vi hade delat in intervjufrågorna i fyra olika teman vi ansåg intressanta för arbetet, från lite mer neutrala ”standard” frågor som till exempel vad den intervjuade arbetar med, till frågor som var mer ingående på vårt studerade problemområde. De intervjuer vi genomfört har med andra ord varit så kallade semistrukturerade intervjuer (ibid). De intervjuade försågs med intervjufrågorna ett par dagar i förväg, via mail. Intervjuerna varade mellan 40 min till en timma och samtliga spelades in av oss efter godkännande av de intervjuade.

Vi genomförde en intervju med informant A som arbetar som IT-strateg på en myndighet här i Göteborg. Informantens arbetsuppgifter innefattar bland annat leverans av driftstjänster för affärssystem och informationssystem, leverans och paketering av komponenttjänster såsom lagring och servar och andra strategiska IT-frågor. De använder sig av en blandning av egenutvecklade system, standardlösningar och outsourcade tjänster.

Informant B arbetar som account manager i en organisation där uppgifterna är att vara kontoansvarig för mellanstora och stora organisationer. Har kontakt med kunder som är på väg in i en molnmiljö eller redan är etablerad i den.

Den tredje intervjun är med en fokusgrupp på fyra personer från ett stort internationellt företag. I denna fokusgrupp finner vi bland andra företagets operations manager tillika security manager, en ansvarig ur deras operationsteam som sitter mycket med server, storage och hallar. Även ansvarige för IT-driften är också med i denna intervju. Vi sökte information om molnet och potentiella sätt att öka förtroende för molntjänster och det råkade sig te sig att detta företag är intresserat av att studera molntjänster och allt omkring för att eventuellt ge sig på att flytta ut delar av företagets infrastruktur i någon form av molnlösning.

2.4 Analys

Efter genomförda intervjuer valde vi i samråd med vår handledare, att inte transkribera dessa. Transkribering är en väldigt tidskrävande process och det skulle inte ge oss mer ur forskningssynpunkt än att sammanfatta intervjuerna på det sätt vi istället valde att göra. Efter intervjuerna har vi valt att sätta oss ner, lyssna igenom intervjuerna och skriva ner allt av intresse som uppkommit under intervjun i ett relativt ostrukturerat dokument. Utifrån detta dokument har vi sedan sammanställt och skapat det som blivit vårt resultat ur en akademiskt intressant synvinkel. I resultatet finns några citat från intervjuerna nedskrivna, men vi valde främst att ha egen kommenterad text, med endast ett få antal citat då det lätt blir så att citat kan sättas ur sina sammanhang (Patel & Davidsson 2013). I den slutgiltiga analysen och diskussionen/slutsatsen diskuteras resultaten av intervjuerna och tillsammans med det vi studerat i litteraturstudierna presenterar vi våra slutsatser av arbetet.

3. Teori

Teorin behandlar de områden som vi har undersökt. För att kunna leverera bra intervjuer och sätta oss in i ämnet har vi studerat molnet, informationssäkerhet, legala aspekter och förtroende. Vi vill med detta avsnitt skapa en förståelse till forskningsfrågan och med hjälp av teorin kunna belysa problemfrågan.

3.1 Förtroende

För att vi ska kunna fastställa och argumentera för hur det skapas ett ökat förtroende för molntjänster anser vi först att vi måste definiera vad förtroende innebär. Vi måste också visa på redan erkända sätt att skapa ökat förtroende och sedan visa hur dessa kan appliceras på molntjänster.

Enligt Lexin (2014) menas med förtroende: *”övertygelse om att man kan lita på någon eller något ”* . En annan definition *är ”det att tro och lite på att någon är förmögen att handla (intellektuellt och moraliskt) korrekt, och också handlar korrekt”* (Wiktionary 2014). Genom dessa två definitioner kan vi alltså ta ut att det handlar om att lita på något eller någon, eller sätta sin tro till dessa i hopp om att de handlar korrekt utifrån specificerad situation. En tredje definition av förtroende, eller den engelska översättningen som vi valt oss använda oss av, trust, inom affärsrelationer är den förväntan som finns på affärspartnern att denne kommer agera i överensstämmelse med dess åtagande, förhandla ärligt och inte utnyttja situationen om det skulle uppstå någon sådan (Papazoglou & Ribbers 2006).

Papazoglou och Ribbers (2006) fortsätter med att beskriva förtroende som ett dynamiskt koncept som förändras över tiden och kan alltså öka eller minska beroende på erfarenheterna av sin affärspartner under denna tid. De fortsätter med att beskriva lite av den unika situation som affärsverksamhet via internet kan medföra, exempelvis att mycket av partnerskapet sker på distans, där den köpande partnern inte alltid kan se det som köps och eller allt det som köps och alltså måste sätta sitt förtroende till sin affärspartner att varan levereras i rätt tid och i rätt format.

En annan anledning till varför förtroende är så viktigt inom affärsrelationer är att om köparen inte känner lika starkt behov av att skydda sig och sina varor för partners opportunism, information bytas betydligt öppnare och kan därför utforska lösningar på ett bredare sätt. För att sådant förtroende ska uppstå behövs oftast en längre tids förbindelse som visar för bägge

parter att detta affärspartnerskap eller förbindelse är någonting viktigt för bägge. (Papazoglou & Ribbers 2006).

Papazoglou och Ribbers (2006) skriver också att marknadstransaktioner mellan affärspartners påverkas av en mängd risker och osäkerheter. Därför är förtroende och begreppet opportunistiskt beteende centralt inom affärsverksamhet. Med opportunistiskt beteende menas jakten på egenintresse med svek eller falskhet (ibid). Detta är givetvis motsatsen till förtroende, som i sin tur beskrivs som tron eller viljan att lita på styrkan, godheten och förmågan hos ens partner, i detta fall affärspartner som exempelvis säljare och/eller köpare. Om förtroende saknas kommer parterna endast att samarbeta under en begränsad tid, under ett system av formella regler och bestämmelser, som kommer att behöva förhandlas, samtyckas, utvecklas och ibland tvingas fram. En sådan rättslig och omständlig process kan verka som ett substitut för förtroende, med medför ökade kostnader. Avsaknaden av förtroende kan alltså innebära högre kostnader (ibid).

Papazoglou och Ribbers (2006) tar upp olika sorters förtroende; personbaserad – egenskaperna hos en person, företagsbaserad – är låst till företaget som en helhet, instutitionsbaserad – vilket betyder att det grundar sig i formalia som exempelvis lagar och normer inom en viss bransch. Den sista och fjärde sortens förtroende som nämns är förtroende till teknik – förväntan att teknologin fungerar som den ska och att om eller när det inte fungerar så blir detta åtgärdat eller kompenserat för. Det sista stycket att det blir åtgärdat eller kompenserat för, menar Papazoglou och Ribbers (2006), att det påvisar att det egentligen visar förtroendet till de människor eller organisation som använder tekniken och inte endast i tekniken i sig. I vårt fall med molntjänster ser vi företagsbaserat och institutionsbaserat förtroende som de två viktigaste delarna.

Det går aldrig ha totalt förtroende för ens affärspartner, så frågan är hur mycket risk organisationen är villig att ta. Det är balansgången mellan risk och förtroende som är vital. Organisationer väljer generellt ökad risk när fördelarna väntas vara större än riskerna. När det gäller organisationer är det oftast de ekonomiska fördelarna som lockar att ta större risker (Papazoglou & Ribbers 2006).

Smyth et al. (2010) argumenterar för att förtroende inte är något rationellt och kan därför inte beräknas. De menar mer att förtroende byggs i sociala sammansättningar genom lärande och subjektivitet.

I detta fall med molntjänster tillkommer ytterligare svårigheter när det gäller att bygga förtroende. Som Lim, Sia, Lee och Benbasat (2006) skriver så är det speciellt utmanande att utveckla förtroende i en onlinemiljö på grund av bristen på direkt kontakt av fysiska personer eller butiker involverade. Khaled, Khan och Malluhi (2010) skriver att all ny teknologi gradvis bygga upp sitt rykte för bra prestanda och säkerhet och på så sätt förtjäna förtroende över tid.

Lim et al. (2006) nämner bland annat två olika sätt för företag som marknadsför sig på onlinetjänster att få ökat förtroende hos potentiella kunder. Det ena sättet är att bygga förtroende genom anknytningar. Det vill säga att som, i detta fall, marknadsför sig molntjänstleverantören tillsammans med andra välkända företag. På så sätt ökar kundens förtroende (förutsatt att kunder känner förtroende för de andra företagen.) Det andra sättet som nämns är genom likhet. Att se att andra personer eller företag som liknar en själv i exempelvis bransch, storlek eller mål, litar på denna molntjänstleverantör gör att en själv känner ett ökat förtroende för dessa.

3.2 Molnet

I detta avsnitt beskrivs molnet och tjänster som ingår i molnet. Vi har tagit stor hjälp av Edvardsson och Frydlinger (2013) för deras förklaring om molnet har mycket information som är väsentlig. Istället för att använda oss av flera källor som ändå skriver samma sak, så blev det bättre att använda en källa.

3.2.1 Definition av molnet

Molnet har haft en uppsjö av olika definitioner men nu när molntekniken inte är lika ny så finns det utvecklade definitioner. Vi har tagit hjälp av National Institute of Standards and Technology's (NIST 2014) för att kunna förklara molnet med hjälp av NIST:s definition. NIST är en organisation som publicerar standarder och riktlinjer för informationsteknologi och drivs av USA:s handelsdepartement som har publicerat 15 stycken utkast av definition av molnet och den senaste versionen blev den slutgiltiga definitionen. Enligt NIST är molnet en relativ ny affärsmodell inom IT-branschen och den har möjliggjort att tjänster går att använda på ett mer resursvänligt och konfigurerbart sätt än tidigare (Mell & Grace 2011). Definitionen beskriver fem viktiga egenskaper hos molnet som förklaras med hjälp av NIST (Edvardsson & Frydlinger 2013).

Självbetjäning
Molntjänster kan aktiveras eller avaktiveras av molntjänstkunden själv genom ett internetgränssnitt som molntjänstleverantören tillhandahåller. Det går att få tillgång till den mängd datorresurser som önskas och när det önskas av användaren (Edvardsson & Frydlinger 2013). Vanligtvis benämns denna typ av tjänst som on-demand. Eftersom molntjänstekunden ska kunna ha tillgång till tjänsten när som helst under dygnet och är det viktigt att den är funktionell och tekniskt tillgänglig. Nyckeln till självbetjäning är att molntjänstekunden självständigt ska bestämma när en tjänst ska användas. Enligt Edvardsson och Frydlinger (2013) är en nackdel att kunden inte får samma kontakt med molntjänstleverantören, för i vanliga fall finns det en mänsklig kontakt mellan kund och säljare, detta kan leda till minskad avtalsmöjlighet. När en molntjänst köps så är det med några klick på en hemsida, Edvardsson och Frydlinger (2013) kallar det för click-wrap (kryssa i en ruta vid beställning över webbgränsnittet) och "*take it or leave it*" utan förhandling. Om kunde inte accepterar molntjänstleverantörens villkor blir det inget köp (ibid).

Bred tillgänglighet oberoende av geografisk etablering
Med molntjänster är tillgängligheten att tjänsterna ska gå att användas på olika plattformar och att den geografiska aspekten inte ska spela någon större roll (så länge användaren kan komma åt internet kan tjänsterna nås). Innan har anställda utfört sina arbeten med stationära datorer som varit knutna till den egna arbetsplatsen, kontoret, men nu har marknadens och kundens krav på tillgänglighet förändrats. Det har ingen betydelse om den anställde är på kontoret, i sin bostad eller hos sina kunder, molnettjänsterna innebär åtkomst till de nödvändiga programvarorna. Utvecklingen av bärbara datorer, smartphones och surfplattor gör det dessutom enkelt att komma åt internet för att kunna använda molntjänsterna (Edvardsson & Frydlinger 2013).

Resursdelande
Resursdelande innebär att molntjänstleverantörens infrastruktur framstår som ett enda system för molntjänstkunden. Det är inte relevant för kunden att veta om molntjänstleverantören använder sig av en gigantisk server eller många mindre. Kunden behöver inte ha kunskap ur ett tekniskt perspektiv var servrarna befinner sig, utan det som är betydelsefullt för kunden är endast att kunna komma åt molntjänsterna och att detta är driftssäkert.

Detta medför att molntjänstleverantören på ett virtuellt sätt kan tillhandahålla olika tjänster åt kunden och samtidigt allokerar och re-allokerar de fysiska och virtuella resurserna åt kunden på ett ”osynligt sätt” (Edvardsson & Frydlinger 2013).

Skalbarhet
Med skalbarhet betyder att molntjänsterna anpassas utifrån vilka behov kunden har. Jämför med användning av egna servrar och andra egna infrastrukturresurser krävs det en uppskattning av det aktuella behovet och behovet av att planera i förväg hur resurser ska användas och vad behovet kan vara. Vilket medför att det alltid finns en viss överkapacitet och därför ett visst resursslöseri. För att undvika att resurser slösas bort genom att de inte används efter kundens behov så kan de stängas av (Edvardsson & Frydlinger 2013).

Till exempel om kunden väljer att använda en tjänst för datalagring där kunden laddar upp 4GB information, för att sedan radera 1GB, då används 3GB. Kundens behov är 3GB och behöver då inte betala för 4GB (Edvardsson & Frydlinger 2013).

Den processen sker omedelbart och kunden behöver inte kontakta molntjänstleverantören och tjänsten skalas ned till vad kunden använder. Edvardsson och Frydlinger (2013) kallar detta uttrycket för "*IT på kran*", så fort kranen sätts på så kommer vattnet och när den stängs av slutar vattnet. Skalbarhetens hastighet ska se till att varje ändring som görs inte är märkbar för kunden. Omedelbar skalbarhet inte realistiskt för alla typer av molntjänster men utgångspunkten bör vara att komma så nära omedelbarhet som möjligt (Edvardsson & Frydlinger 2013).

Mätbara tjänster
Med mätbara tjänster förklaras att molntjänsten mäts när den används av kunden. Med begreppet som nämndes tidigare *"It på kran*" så bör användandet mätas så att molntjänstleverantören kan ta betalt för det kunden använt, det vill säga den faktiska förbrukningen**.** Mätningen varierar beroende på typ av molntjänst, men typiskt för mätningen är, upptagen lagerkapacitet, använd bandbredd, antal beräkningar med processorkraft, och antalet aktiva användare. Mätningen är dubbelsidig så både kunden och molntjänstleverantören kan övervaka och mäta av vad som används (Edvardsson & Frydlinger 2013).

3.2.2 Tjänstemodeller
NIST-definitionen definierar tre olika tjänstemodeller för molntjänster. Oftast talas det om SPI-modellen där förkortningarna står för vardera av de tre lagren (Software as a Service, Platform as a Service och Infrastructure as a Service) (Edvardsson & Frydlinger 2013). De vanligaste tjänstemodellerna är SaaS (Software as a Service), PaaS (Platform as a Service) och IaaS (Infrastructure as a Service) men det har också uppkommit fler som exempelvis

Security as a Service (säkerhet som molntjänst) och Business Process Outsourcing as a Service (outsourcing av affärsprocesser som molntjänst) menar Edvardsson och Frydlinger (2013). Det är bara några som har uppkommit.

IaaS

Med Infrastructure as a Service avses lagring, bandbredd och beräkningskapacitet, i ett virtuellt system. Kunden har visserligen inte kontroll över den faktiska hårdvaran och grundsystemet, men när varje kund arbetar med det virtuella systemet så skapas en upplevelse att kunden exempelvis har sin egen server. En snabbväxande IaaS-tjänst är CDN (Content Distribution Networks), nätverk för mediadistrubution för ”on-demand filmer” och TV-program. De största Tv-kanalerna i Sverige har i dag sina utbud via applikationer i mobila enheter, datorer och spelkonsoller och liknande (Edvardsson & Frydlinger 2013).

PaaS

Platfrom as a Service är en utvecklingsplattform där kunden eller någon av kundens IT-leverantörer kan utveckla, testa och arbeta med skräddarsydda program för kunden i en kontrollerad miljö (Edvardsson & Frydlinger 2013). PaaS innehåller inte bara en utvecklingsplattform utan också verktyg för att designa, programmera och testa systemet innan driftsättning. Några exempel på PaaS-system är Google Apps Engine (är en molntjänst som erbjuder molntjänster både enligt tjänstemodellen PaaS och SaaS) och Microsoft Azure (är en PaaS-tjänst som möjliggör utveckling och driftsättning av främst Windows-baserade applikationer under ramverket .NET).

SaaS

Med Software as a Service får kunden tillgång till molntjänstleverantörerns datorprogram som en molntjänst. Användaren har inte har någon kontroll över infrastrukturen eller utvecklingsplattformen och är helt låst till datorprogrammen som erbjuds. Det som kännetecknar SaaS är att flertalet kunder använder samma version av systemet. Detta medför att när molntjänstleverantören uppdaterar systemet får alla kunder samma version samtidigt. SaaS betyder inte att kunden är fast med en och samma version, utan kommer få sin programvara uppdaterad. Kunden och molntjänstleverantören kommer överens om hur programvaran kommer att uppdateras. Några exempel på SaaS-tjänster är Google Mail och Microsoft Outlook (Edvardsson & Frydlinger 2013).

3.2.3 Leveransmodeller - Typer av moln

Edvardsson och Frydlinger (2013) menar också att NIST-definitionen har fyra typer av leveransmodeller hur molntjänsterna ska tillhandahållas till kunderna eller till grupper av kunder. Dessa fyra är privata, gemensamma, publika och hybrider av de IaaS, PaaS och SaaS, se ovan.

Privata moln

Privata moln förutsätter att tjänsten levereras till en enskild organisation (kunden). Molntjänsten som levereras kan driftas och ägas av organisationen själv, medför att molnet kan placeras både i organisationens egen datorhall eller hos en molntjänstleverantörs datorhall (Edvardsson & Frydlinger 2013).

Gemensamma moln

Gemensamma molntjänster är som namnet beskriver en leveransmodell för gemenskap mellan olika organisationer, där flera delar på molnet för sina molntjänster. Det som är skillnaden jämfört med privata moln är att det finns en gemensam nämnare mellan organisationerna (kunderna), som likartade moln, uppdrag eller krav avseende säkerhet. Precis som ett privat moln så kan det ägas och driftas av någon av användarna eller av en extern leverantör. I tidigare versioner av NISTs definition fanns inte denna typ av modell med och den har kritiserats för att vara överflödig enligt Edvardsson och Frydlinger (2013). Ett gemensamt moln principiellt sett samma som ett privat fast det är fler som använder det i en mindre grupp (ibid).

Publika moln

Det publika molnet är den vanligaste tjänstemodeller och det är oftast den som vi ofta tänker på när det kommer till molntjänster. Med ett publikt moln menas att molntjänstleverantören gör resurs tillgängliga för allmänheten via internet. Exempel på publika molntjänster är Facebook och Google Gmail. Publika moln karaktäriseras att den erbjuds till allmänheten via internet, vilket medför att molntjänstleverantörens resurser alltid är externa i förhållande till molntjänstekunden (Edvardsson & Frydlinger 2013).

Hybrid moln

Om en kombination av två eller tre av ovanstående modeller kombineras med varandra skapas ett hybrid moln. Enligt definitionen ska varje enskilt moln som kombineras fortfarande vara en unik och separat enhet, men knytas samman av någon teknologi som möjliggör överflyttning av data eller datorprogram (Edvardsson & Frydlinger 2013).

3.3 Informationssäkerhet i molntjänster

Säkerheten är av mycket stor betydelse för användarnas förtroende för molntjänster. Vi vill i detta avsnitt belysa informationssäkerhetens betydelse för användningen av molntjänster och vilka risker som är störst och vanligast.

3.3.1 Informationssäkerhet

Informationssäkerhet är en åtgärd som görs för att skydda information och säkerställa att den inte läcker ut, blir ändrad eller förstörs. Information uttrycker kunskap och är en tillgång för individer och organisationer. *"Vi kan kommunicera information, vi kan lagra den, vi kan styra processer med den – vi behöver den för det mesta vi gör helt enkelt"* (Informationssäkerhet 2014). För organisationer kan informationssäkerhet handla om att skydda information mot hot som kan åstadkomma skada mot organisationen i sig. Det kan till exempel vara fråga om att skydda en källkod till en verksamhetskritisk programvara och andra organisationshemligheter och som med en utvecklad informationssäkerhetsstrategi hanterar hot och minimerar riskerna för missbruk (Wikipedia 2014a).

Edvardsson och Frydlinger (2013) menar att informationssäkerhet inte ska beaktas som någonting i sig själv utan mer som en process. För att beskriva processen hänvisar Edvardsson och Frydlinger (2013) till ITIL.

ITIL, Information Technology Infrastructure Library är en uppsättning principer för att hantera IT-tjänster som i sin tur har namngett processen (nämnt ovan) till ISM – Information Security Management (Malone et al. 2009). Processen syftar till för att skydda information och individer från obehöriga intressenter eller processer. ISM har tre olika områden som den reglerar.

Konfidentialitet: Information och data är enbart tillgänglig till behöriga individer och organisationer, exempel lösenord, brandväggar och passerkort (ibid).

Integritet: Informationen är komplett, korrekt och kan inte ändras av obehöriga, exempel rollback metoder, testmöjlighet, revision (ibid).

Tillgänglighet: Informationen ska vara tillgänglig och användbar efter bestämd tid samt vara skyddad mot attacker, exempel service desk och styrsystem (ibid).

ISM måste beaktas i organisationens struktur för att ge den strategiska inriktningen för säkerhetsaktiviter och säkerställer att de säkerhets mål uppfylls. Syftet med ISM är att ge en

utgångspunkt för alla aspekter av IT-säkerhet och hantera alla IT-verksamheter (Malone et al. 2009).
Edvardsson och Frydlinger (2013) anser att ISM utgör en viktig värdeskapande process eftersom informationssäkerhet är en grundkomponent för varje IT-tjänst, vilket ger en garanti att tjänsten fungerar samt att den bygger upp tjänstens värde.

Enligt datainspektionen (2014a) bör organisationer också ha en säkerhetspolicy, i alla fall om organisationen hanterar känslig data som personuppgifter eller behandlar personuppgifter i stor skala (Datainspektionen 2014a). Datainspektionen är en myndighet som genom sin tillsynsverksamhet ska bidra till att behandlingen av personuppgifter inte leder till otillbörliga intrång i enskilda individers personliga integritet (ibid). En policy tillhandahåller organisationers säkerhetsstrategi, ansvarsfördelning och övergripande mål för säkerheten. Det som är viktigt för policyn är att den är tydlig och lättbegriplig så det inte skapas några oklarheter.
En policy ska vara skriftlig och allmänt tillgänglig. Det är viktigt att hålla policyn uppdaterad så att den kan anpassas mot det aktuella behovet av skydd.*" Personuppgiftsansvarig är normalt en juridisk person (företag, stiftelse, myndighet etc.) som behandlar personuppgifter och bestämmer vilka uppgifter som ska behandlas och vad uppgifterna ska användas till. Det är alltså inte chefen eller någon anställd som är personuppgiftsansvarig"* (Datainspektionen 2014a).

3.3.2 Säkerhetsproblem inom molnet – Nya som gamla

Molnet har inte bara skapat smidiga lösningar för användarna, det har också givit upphov till nya säkerhetsproblem och säkerhetsfrågor. Enligt Cloud Security Alliance (CSA) så är en av de mest betydande riskerna att organisationer som använder molntjänster har en tendens att kringgå viktiga säkerhetspolicys, processer och bästa praxis (Edvardsson & Frydlinger 2013). Organisationer är sårbara för säkerhetsattacker vid användning av molntjänster och den vinst en organisation kan göra med en molntjänst kan lika väl övergå till förlust eftersom säkerheten inte är tillräckligt bra. CSA har skapat standarder inom molnsäkerhet och under de senaste åren publicerat olika dokument för att belysa hur viktigt säkerheten är. En viktig komponent för att hantera risker i molnet är att förstå vilken typ av säkerhetshot som finns. CSA har i en rapport (*"The Notorious Nine: Cloud Computing Top Threats in 2013")* visat på nio viktiga risker och med hjälp av rapporten vill CSA hjälpa organisationer att få en

professionell förståelse. Riskerna som tas upp är speciellt inriktade mot molntjänster och CSA har genomfört undersökningar av branschexperter för att sammanställa en professionell åsikt om de största sårbarheterna inom molnet. De nio riskerna är:

Data Breaches
Dataläcka kan uppstå när en molndatabas inte är korrekt utformad och ett fel kan finnas som gör det möjligt för en användare att komma åt annans data, det vill säga som inte är till för denne. Det kan också vara en menad attack mot organisationen från en kriminell individ eller organisation vars syfte är att komma över information eller att ändra i IT-systemen (Bailey 2012).

Data Loss
Dataförlust handlar om förlust av data. Naturligtvis kan data som är lagrat i molnet förloras, avsiktligen eller avsiktligen. Det kan ske genom skadliga attacker eller oavsiktlig radering från molntjänstleverantören. Det kan också vara fråga om olyckshändelser till exempel en brand där molntjänstleverantören har molnservrarna. Detta kan leda till en permanent förlust av viktig information för kunderna om inte molntjänstleverantören har lämpliga åtgärder för att säkerhetskopiera data. Kunden kan dock inte lägga allt ansvar på molntjänstleverantören utan kan behöva att kryptera data innan den laddas upp till molnet. Men att betänka är om krypteringsnyckeln förloras kommer informationen också förloras (Bailey 2012).

Account Hijacking
Kontostöld är inget nytt begrepp och attacker som phising är en metod att lura innehavare till bankkonton och andra elektroniska resurser att delge kreditkortsnummer, lösenord eller annan känslig information, bedrägeri och utnyttjande av sårbarheter i mjukvara finns inom molntjänsterna (Wikipedia 2014b). Genom att en angripare får tillgång till ett användarnamn går allt att komma åt i molntjänsterna som individen vanligtvis använder. Om angriparen får tillgång till tjänster så kan personen avlyssna aktiviteter, manipulera data, returnera falsk data eller omredigera kunder till illegala webbplatser med mera. Andra effekter kan bli att angriparen använder kontot för att utnyttja organisationers rykte för att lansera andra attacker. Till exempel cross site scripting som handlar om att stjäla informationen som annars inte visas på en hemsida, eller att förstöra en webbsidas utseende (Wikipedia 2014c). Ett exempel är Amazon.com som under 2009 blev utsatt för en attack där konsekvenserna blev konto- och servicekapning (McMillan 2009).

Insecure APIs

Molntjänstleverantörer exponerar en uppsättning av programvarugränssnitt eller API: er som kunderna använder för att hantera och integrera med molntjänsterna (ledning, uppföljning, styrning med mera). Säkerheten och tillgängligheten av allmänna molntjänster är beroende av säkerheten i dessa grundläggande gränssnitt (Los et al. 2013). Gränssnitten måste vara utformade så att skydd mot både oavsiktliga och illegala försök att kringgå regelverken hur molntjänsterna körs.

Gränssnitten byggs ofta så det ska gå att erbjuda mervärde till kunder och kunders kunder. Det är viktigt att organisationer som konsumerar molntjänster förstår att konsekvenserna för säkerheten har ett samband med användningen av tjänsterna. Beroendet av en svag uppsättning av gränssnitten och API: er utsätter organisationen sig för en rad olika säkerhetsfrågor som rör sekretess, integritet, tillgänglighet och ansvar (Bailey 2012).

Denial of Service

Denial of Service är attacker som är avsedda att förhindra åtkomst för användaren till molntjänsterna. Detta görs genom att tvinga offrets molntjänst att använda överdrivna mängder av resurser som processorkraft, minne, diskutrymme och bandbredd. Attack kallas DDoS (distributed denial-of- service) och orsakar en systemnedgång. Den typen av attack utnyttjar sårbarheter i webbservrar, databaser eller andra molnkällor, vilket gör att en person med illvillig attityd kan omkullkasta ett program med en enda attack. Det är som att sitta fast i rusningstrafiken när det skett en olycka och det enda som går att göra är att vänta tills trafiken börjar flyta igen.

Driftstörningar inte bara hindra åtkomst och användning till viktig data, utan kan också tvinga organisationen att tänka om det verkligen är värt att använda molntjänsterna.

Molntjänstleverantörer fakturerar ofta kunderna baserade på beräkningsprocesser och diskutrymme som de använder. En angripare kanske inte kan slå ut tjänsten helt men se till att tjänsten konsumerar mycket datorkraft. Organisationen kan bli tvingad att betala för något som normalt inte behövts och att det därför blir för dyrt. Så länge molnet växer så kommer DDoS attackerna öka (Linthicum 2014).

Malicious Insiders

Malicious Insiders handlar om hotet med individer som utnyttjar sin ställning inom organisationen, även kallad ”*Insider*”. Det kan vara en anställd eller en före detta anställd, en entreprenör eller annan affärspartner som har eller har haft behörig tillgång till

organisationens IT-system. Som kan missbruka användandet av organisationens IT-resurser. Bailey (2012) namnger fyra olika typer av insiders:

- Skadliga administratören – Individer som hanterar data, filer och privilegierade resurser inom en organisation. Som exempelvis kan sprida konfidentiell information som är skadligt för organisationen.

- Tekniskt kunniga – Individer som använder sitt tekniska kunnande för att utnyttja organisationens svagheter och bryta sig igenom säkerheten för att få tillgång till hemlig information. Det kan exempelvis handla om att en individ vill komma åt företagets konfidentiella data för att sälja den till högstbjudande.

- Individer som attackerar sina egna organisationer – Individer som väljer att hämnas på organisationer på grund av konflikt, exempelvis om den anställde känner sig illa behandlad av organisationen så använder dem sina externa verktyg eller rättigheter för att bryta mot säkerhetsprotokollen.

- Dåligt internt upprätthållande – Organisationer antar att molntjänster drivs av sig själva. För organisationer är molntjänsterna självreglerande och självhanterliga, så det spelar ingen roll hur hanteringen av tjänsten är. Detta görs i flesta fall av okunskap eller inkompetens inom organisationer. Vilket medför att angripare och insiders kan hitta sådana system och kan lätt bryta sig in eftersom cheferna ”sover” på sina jobb. Detta är ett vanligt problem hos organisationer där ansvaret inte är strömlinjeformat. Istället så måste organisationer bli proaktiva och hitta lösningar mot säkerhetshoten.

Abuse of Cloud Services

Molnets största fördel är möjligheten att få tillgång till enorm mängd datorkraft, både för stora och små organisationer (Bailey 2012). Vilket inte hade varit möjligt för alla organisationer annars. Dock så vill inte alla använda den möjligheten till gott utan kan också användas av illasinnade individer. Som exempel, det kan ta år för en individ att med sin egen datorkraft knäcka en krypteringsnyckel, men med hjälp av molnservrarnas resursers skulle detta kunna gå från år till minuter. Eller så kan individen använda molnserverarna för DDoS-attacker, implementera skadlig kod samt distribuera privatkopierad programvara. Denna typ av hot är

mest riktad mot molntjänstleverantörer eftersom det är deras tjänst som blir angripen (Bailey 2012).

Insufficient Due Diligence

Molntjänster har medfört att organisationer hoppar in och skriver avtal om tjänster för att med lov om konstandsbesparingar, effektiviseringsvinster och förbättrad säkerhet. Men utan att egentligen ha en förståelse hur molnmiljön fungerar. Hur program och tjänster skjuts till molnet, och hur det operativa ansvaret så som incidenthantering, kryptering och säkerhetsövervakning fungerar. Vilket medför att organisationer tar risker som inte förstås. Till exempel som att inte behandla avtalen ordentligt, eller att okända operativa och arkitektoniska frågor uppstår när designer och arkitekter ska implementera tjänster till molnet. Bailey (2012) menar att organisationer som flyttar till molnet måste förstå vad det innebär.

Shared Technology Issues

Molntjänstleverantörer levererar normalt tjänsterna på ett skalbart sätt genom att dela infrastruktur, plattformar och applikationer, vilket medför risk för att det uppstår ett gemensamt hot mot modellerna (IaaS, PaaS och SaaS). En enskild sårbarhet eller felaktig konfiguration kan leda till en kompromiss som hela molnet blir drabbad av. Organisationer bör ha en defensiv strategi till tjänstemodellerna IaaS, PaaS och SaaS som omfattar användarsäkerhet, övervakning, lagring, nätverk, program och beräkningar (Bailey 2012).

3.4 Legala aspekter kring molntjänster

I detta avsnitt vill vi förklara kort hur regler och lagar knyts samman i molntjänster och vad det kan innebära för användaren. Både som kund och molntjänstleverantör. Då vi anser att lagar är en viktig del av molntjänsterna och det är viktigt att förstå hur regelverken appliceras i molnmiljön.

3.4.1 Juridik

Syftet med användning av molntjänster är med största sannolikhet effektivitetsförändring, ökning, förbättring i affärssystemet. Vilket gör det viktigt för organisationer att inta rätt perspektiv på de legala frågorna menar Edvardsson och Frydlinger (2013). Lagarna ska bedömas och värderas utifrån organisationens verksamhet. Lagar och föreskrifter kan i vissa fall sätta upp hinder, eller gynna organisationers affärsmässiga mål. Därför är det viktigt att organisationer gör en kommersiell analys vars utgångspunkt är att reda ut vilka legala frågor som är viktiga för organisationen (Edvardsson & Frydlinger 2013).

Edvardsson och Frydlinger (2013) tar fram tre typer av legala frågor:

- *Indispositiva regler eller föreskrifter som begränsar företags eller organisationer handlingsutrymme och som inte kan avtalas bort (exempelvis personuppgiftsregler).*
- *Dispositiva regler eller föreskrifter som skapar begränsningar men som parterna kan styra över genom avtal (exempelvis regler om lagval och tvistlösning).*
- *Frågor som inte alls är lagreglerade men som ändå berör risker som kan och bör hanteras genom avtal (exempelvis specifikation av tjänstens funktionalitet).*

(Edvardsson & Frydlinger 2013 s.91).

När organisationer går över till molntjänster finns det oftast en grunduppställning av legala frågor som behöver behandlas. Frågor som oftast är relevanta till molnmiljön är:

- *Lagval* – Vilket lands lagar är det som gäller och om det är flera länder som är involverade och hur kommer eventuella konflikter att hanteras samt hur ska andra länders lagstiftning hanteras om lagval inte är möjligt.
- *Integritet och personuppgiftshantering* – Hur ska den personliga integriteten behandlas utan att den blir kränkt.

- *Rätten till data* – Hur ser rätten till data ut mellan kund och molntjänstleverantör som finns lagrad i molntjänsten. Hur kan kunden förhindra inlåsningseffekter vid exempelvis uppsägning av avtal eller molntjänstleverantörens oförmåga att leverera.
- *Licens och immateriella rättigheter* – Hur hanteringen av immateriella rättigheter i molnet och hur tillåts licenser att eventuella datorprogram körs i molnet.
- *Tjänstebeskrivning* – Definiera balansen mellan molntjänstleverantörens behov av standardiserade tjänster och kundens egna behov av anpassning till molntjänstleverantörens affärsmodell och behov samt hantering av förändringar.
- *Tjänstenivå* – Definiera vilken kvalitet som molntjänsten ska levereras och vad som händer om en leverans brister.
- *Ansvarsfördelning* – Hur kommer ansvaret att fördelas mellan kund och molntjänstleverantör samt hur ska begränsningar i ansvaret definieras.
- *Branschspecifika frågor* – Hur branscher ser ut som kunden är verksam i och vilka legala krav är specifika för branschen.

(Edvarsson & Frydlinger 2013 s.92).

Den allmänna globaliseringen och funktionen att kunden inte egentligen skall behöva bry sig om vart molntjänstleverantören har sin infrastruktur så är det svårt att på förhand veta vilket land molntjänstleverantören använder sig av samt vilka lagar som gäller. Eftersom tecknandet av en molntjänst ofta görs via en applikation på internet hos molntjänstleverantörens hemsida så tecknas också ett avtal med molntjänstleverantören där det finns ett innehåll av lagval. Det finns också tvingande lagstiftning som kan förändra vilken lag som faktiskt ska tillämpas på hela eller delar av avtalet (Edvardsson & Frydlinger 2013).

Ta som exempel en organisation som köper en SaaS-tjänst och gör ett omedvetet antagande att svensk rätt gäller, när det i själva verket inte är så. Utan istället är det ett annat lands lagar som gäller, vilket kan leda till att organisationens kalkyl för inköpet av tjänster spricker eftersom organisationen utgick från att det var svensk lag som gällde (ibid).

3.4.2 Personuppgiftslagen

”Syftet med denna lag är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter” (SFS 1998:204).

Personuppgiftslagen (PUL) är den lag som är mest omdiskuterad inom molnmiljön menar Edvardsson och Frydlinger (2013). *”Den som använder en molntjänst för lagring av personuppgifter, till exempel i ett löneregister, förlorar den faktiska kontrollen över personuppgifter som lagras”* (Datainspektionen 2014b). Molntjänstleverantörer brukar ofta använda standardavtal som är fördefinierade med användarvillkor. Enligt datainspektionen (2014b) så är den som använder en molntjänst som hanterar personuppgifter ansvarig för personuppgifterna och behandlingen av dem. Så molntjänstleverantören och underleverantören som molnkunden använder i sina molntjänster är inte ansvariga för personuppgifterna. Det är molnkunden som bär ansvaret att lagar följs, till exempel myndighetsspecifika registerförfattningar och offentlighets- och sekretesslagen (Datainspektionen 2014b).

För att en molntjänst kan tas i bruk måste personuppgiftsansvarige bedöma om den personuppgiftsbehandling som molntjänstleverantören kan utföra vara tillåten enligt personuppgiftslagen. ”*Enligt personuppgiftslagen får personuppgiftsbiträden bara behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige”* (Datainspektionen 2014b). Standard är att den som är personuppgiftsansvarig utformar själv instruktionerna. Vid köp av molntjänster så blir kunden oftast hänvisad till villkor som gäller enligt molntjänstleverantörens standardavtal, i sådana fall måste personuppgiftsansvarige granska avtalsvillkoren och riktlinjerna som molntjänstleverantören erbjuder. Den ansvarige måste göra en bedömning utifrån personuppgiftslagens bestämmelser med hjälp av egen risk och sårbarhetsanalys. Enligt datainspektionen måste den personuppgiftsansvarige ta ställning till olika punkter som rör molnmiljön:

- Ta ställning vilken risk det finns att personuppgifter kan komma att behandlas för andra ändamål än de ursprungliga.
- Ta ställning till om molntjänstleverantören kan komma att lämna över personuppgifter till tredje land (ett land som står utanför EU/ESS) och om det finns stöd i personuppgiftslagen för det.
- Bedöma vilka säkerhetsåtgärder som måste finnas för att skydda personuppgifterna som behandlas i tjänsten.
- Se till att det finns ett personuppgiftsbiträdesavtal med molntjänstleverantören.
- Beakta att det kan finnas annan lagstiftning, som exempel sekretesslagstiftning.

(Datainspektionen 2014b).

Personuppgiftsansvarige måste i regel se till att det finns ett personuppgiftsbiträdesavtal med molntjänstleverantören som lever upp till kraven i personuppgiftslagen. Enligt datainspektionen ska: ”*villkoren i avtalet vara urskiljbara från övriga villkor som gäller mellan parterna och de ska inte ensidigt kunna förändras av personuppgiftsbiträdet”* (ibid). Avtalet kan innebära följande:

- Att personuppgiftsbiträdet är skyldig att tillämpa svensk lagstiftning när det gäller behandling av personuppgifter
- Att personuppgiftsbiträdet är skyldig att vidta lämpliga säkerhetsåtgärder enligt 31 § personuppgiftslagen.
- Att personuppgiftsbiträden endast får behandla personuppgifter i enlighet med personuppgiftsansvariges instruktioner och inte för andra ändamål.
- Att säkerhetsställa så att personuppgiftsansvarige har kännedom vilka som är personuppgiftsbiträden.
- Att säkerhetsställa att personuppgiftsansvarige kan på ett lämpligt sätt följa upp biträden så att instruktioner och krav följs.
- Att det finns tekniska och praktiska förutsättningar att utreda misstankar om att någon hos personuppgiftsansvarige eller hos något biträde haft obehörig åtkomst till personuppgifterna.
- Slutligen att parterna vet vilka åtgärder som ska vidtas när avtalet upphörs.

  (Datainspektionen 2014b)

3.4.3 Avtal

Som nämnt i tidigare avsnitt angående köp av molntjänster så sker det oftast genom en websida (se avsnitt 3). Vilket leder till att organisationer inte kan ställa frågor om avtalet och därför inte kan påverka det. Thorslund (2013) tar upp frågor som berör standardavtal för molntjänster:

- Kommer molntjänstleverantören att använda sig av underleverantörer?
- Var kommer informationen att lagras?

- Var kommer informationen att bearbetas?
- Vem har rätt att få åtkomst till informationen?
- Vad händer med informationen när avtalet avslutas?
- Går det att få ut logginformation så att det kan kontrolleras vem som har haft åtkomst till informationen?
- Vilken säkerhet finns för informationen?

Dessa frågor är bara några exempel som kan ställas mot molntjänstleverantörer (Thorslund 2013).

Ett annat avtal som används är Service Level Agreement (SLA) som är till för att definiera relationen mellan kund och molntjänstleverantör. SLA är en viktig källa till dokumentation för båda parter. SLA används för att:

- Identifiera och definiera kundens behov
- Ta fram en verksamhetsförståelse
- Göra komplexa frågor enklare.
- Minska konflikter mellan parterna.
- Uppmuntra till en dialog vid tvister mellan parterna.
- Minska orealistiska förväntningar.

(Reddy Kandukuri et al. 2009)

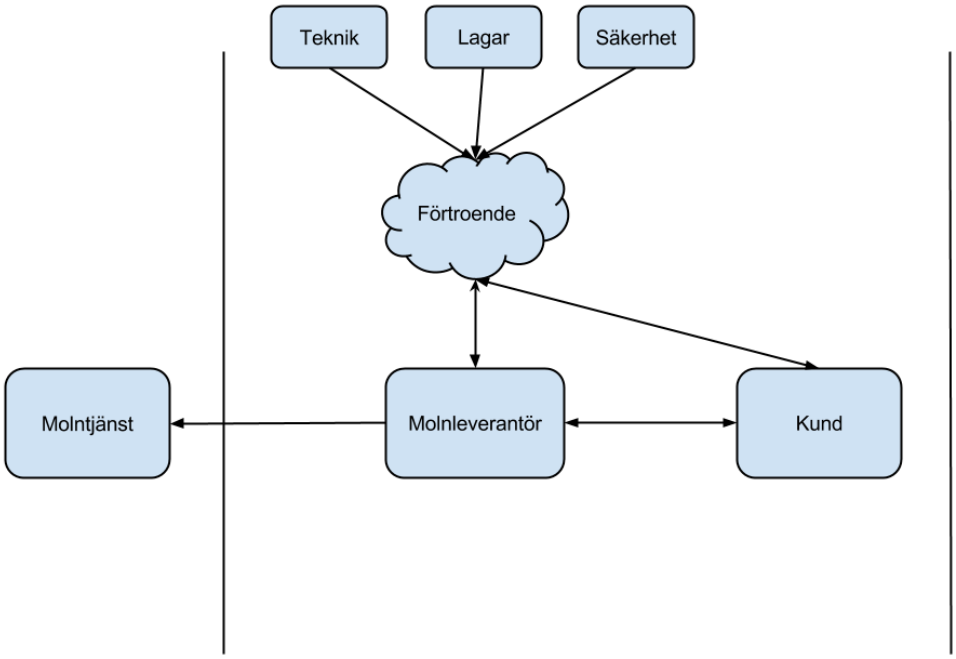
Eftersom molnet har fått en betydande uppmärksamhet så har det också tillkommit viktiga utmaningar och SLA är ett sätt för kund och molntjänstleverantör att hantera det tillsammans. SLA är ett sätt att formellt ange villkoren hur tjänster ska levereras från molntjänstleverantör till kund inom molnbranschen (Wieder et al. 2012).

3.4.4 Legala konflikter

Avslutningsvis vill vi belysa två situationer där det har varit en konflikt mellan två eller fler parter. Edvardsson och Frydlinger (2013) beskriver ett fall om SWIFT (The global provider of secure financial messaging services) som är en organisation som står mellan amerikansk säkerhetslagstiftning och europeisk integritetslagstiftning.

USA antog ett antal lagar i samband med kampen mot terrorism efter 11 september 2001 och enligt lagarna så krävdes det att amerikanska myndigheter skulle få tillgång till SWIFT:s uppgifter och därmed lämna ut personuppgifter till myndigheter i USA. SWIFT bedömde att lagstiftningen omfattade dem och lämnade ut uppgifterna. Efteråt fastslog den belgiska dataskyddsmyndigheten att SWIFT:s agerande stred mot belgisk dataskyddslag och att individer vars personuppgifter överlämnats till USA hade fått sin integritet kränkt (Edvardsson & Frydlinger 2013).

Andra fallet vi vill ta upp är Google Inc. och Salems kommun. Salems kommun avsåg att teckna med en molntjänstleverantör inte uppfyllde kraven enligt personuppgiftslagen (1998:204). Datainspektionen förelade i samma beslut att kommunen skulle upphöra med behandlingen av personuppgifter i molntjänsten eller vidta åtgärder för att personuppgiftsbiträdesavtalet ska vara förenligt med PUL. (Se bilaga 2 för att läsa mer) (Kammarrätten i Stockholm 2014).



Figur 1. *Översikt hur teoriavsnitten förhåller sig till varandra och varför avsnitten är viktiga i uppsatsen*

4. Resultat

4.1 Informant A

Informant A säger att det viktigaste vid beställande av en ny tjänst är att de ska uppfylla ett verksamhetskrav och skapa verksamhetsnytta. Efter det kommer allt annat, exempelvis att det finns kontinuitet, bra säkerhet, lagringskrav, bra support och så vidare. Som myndighet har de också andra krav med bland annat PUL, att information måste arkiveras och som informanten säger *”Vi måste vara så öppna som möjligt som myndighet, men med rätt säkerhet”*.
Informanten anser att en viktig fråga när det gäller tjänster som är outsourcade i molnet är informationsklassning. Som en myndighet har de strikta regler för detta, informanten säger också att den som lägger upp informationen också måste vara ansvarig för att den läggs upp på korrekt sätt. Informanten tycker att den tjänst som används för delad data är smidig och lättillgänglig. Som myndighet har de extra antal riktlinjer och lagar att ta hänsyn till. Företaget de använder för delad data är därför med i det så kallade Safe Harbour avtalet (2000) och stödjer därmed EU:s lagar om personuppgifter (Datainspektionen 2014b)
Informanten anser att andra fördelar med molntjänster är att komma igång väldigt fort, lösa ett problem väldigt fort och då, som informanten anser är det viktigaste, skapa nytta för verksamheten väldigt fort. Skulle interna processer användas för installering, testning och utbildning skulle detta vara betydligt trögare. Informanten säger att det också långsiktigt är en tröghet, då kompetensen också måste behållas. Molntjänster erbjuder därmed en lösning på det och som myndighet kan de dela kostnader med liknande myndigheter för att minska dessa.
Informanten anser att när de ska välja en leverantör är det främst bra kompetens som behövs så att de kan ställa rätt krav för att få en leverantör de kan känna förtroende för. Informanten fortsätter med att säga att det inte handlar om priset främst, även om det självklart måste tas hänsyn till. De undersöker istället exempelvis hur den ekonomiska redovisningen ser ut för leverantörerna från flera år tillbaka och de ställer krav på referenser från andra kunder till leverantören, främst andra myndigheter. Som myndighet vill de veta om hur leverantören arbetar med sociala frågor, arbetsmiljö och jämställdhet.
Ett problem med detta anger informanten är att allt detta kan se väldigt bra ut när avtalet skrivs, men då dessa oftast löper under flera år, kan mycket hinna hända, inte minst inom IT världen; Leverantören kan bli uppköpt, gå i konkurs, eller i sin tur outsourca tjänsterna till underleverantörer.
Informanten tror att en lösning på detta är att först och främst ha ett mindre antal leverantörer för att sedan skapa bättre beställarkompetens och sedan jobba närmare leverantören, skapa ett

så kallat partnerskap. Informanten tycker också att det måste finnas en leverantörsstrategi och som informanten säger *”Leverantören och beställaren måste se till att båda vinner på att ha ett stabilt förhållande”*.
Informanten tror att i framtiden kommer mer och mer hamna i molnet och outsourcas. För att *”alla går den vägen”*. Myndighetens ledning förväntar sig hela tiden att mer görs för samma pengar och blir effektivare. Informanten säger att det bara går att effektivisera till en viss grad internt, då stora kostnader såsom personal och lokaler finns kvar. Informanten säger att *”man måste ta ett steg ut (i molnet) för att nå nästa steg av effektivisering”*. Speciellt bra är det som myndighet, då det går att samverka smidigare genom molnet och även dela på kostnaderna.

4.2 Informant B

Informant B berättar att när kunder pratar om molntjänster så är den viktigaste faktorn för dem tillgängligheten. De flesta av kunderna har redan gått förbi säkerhetstänket och den ekonomiska aspekten och är därför mer inne på hur det fungerar med tillgängligheten. ”*De flesta organisationer som jag jobbar med är beredda att betala så länge dem kan bli garanterade en bra tillgänglighet*”. Det värsta som kan hända är att tjänsten går segt eller till och med inte går att nå.

Informanten berättar att några av kunderna fortfarande inte är sugna att gå över till molnet medan andra redan har börjat använda molntjänster. ”*Jag blev förvånad att så många av mina kunder faktiskt hade börjat använda någon form av molntjänst”. ”Vissa av mina kunder är väldigt försiktiga inom IT-utvecklingen och inte riktigt vågat låta data behandlas av molntjänster”.* Det beror på okunskap till molnteknologin och att organisationerna hellre kör sin egen server. *”Molntjänster är väldigt luddigt definierat och det är svårt att förstå vad de innebär”.* Informanten tycker att det vore en bra idé att anställda konsulter när molntjänster skall inköpas.

Skillnaden från att köra en lokal server och en molntjänst får inte märkas av så mycket och att det kan skickas stora mängder data i molnet men blir det segt så förloras tid, och tid är en ekonomisk faktor anser informanten.

Vi går in på säkerheten och frågar hur kunderna tänker kring säkerheten i molntjänsterna. ”*Kunderna som har gått över till molntjänsterna tycker att säkerheten är bättre än sin egna säkerhet som de använder. Kunderna berättar att de anser sin egen säkerhet som låg och att molntjänsterna har högre säkerhet, att en server som kunden äger är lättare att hacka.”*

Kunderna litar mer på leverantörerna eftersom de sysslar med det på heltid och att det inte gör kunderna själva. Det kan vara på grund av okunskap menar informanten. Att kunderna får ett förtroende att leverantören kan sin sak och därför går över i gott förtroende till tjänsterna.

Samtalet fortsätter mot förtroende och informanten berättar: ”*Förtroende kan ta lång tid att bygga upp inom en bransch, men lika så går det väldigt fort att förlora det. Om en kund använder en leverantör som har lovat att ha en tillgänglighet för att sedan inte hålla det faller förtroendet fort och leverantören kommer få svårt att återställa det förlorade förtroendet”.*

4.3 Fokusgrupp

De intervjuade i fokusgruppen börjar med att berätta att 99 % av företagets data lagras nu i egna datorhallar. Det som är undantaget är en del data som lagras i Sharefile, som beskrivs som ett Dropbox för företag. Dem är intresserade av molntjänster och de fördelar som de kan dra av dessa. Bland annat nämns flexibiliteten och snabbheten, för exempelvis testning som en fördel. En annan är ett system eller applikation i molnet som skulle vara åtkomlig från alla länder med samma prestanda. Det som lyfts fram allra främst är dock skalbarheten, att snabbt kunna öka eller minska kapacitet. Ett av företagen i organisationen har exempelvis en peakperiod på 10 veckor. Under denna period hade det varit utmärkt att kunna köpa upp mer kapacitet för att sedan minska den resten av året. De nämner även automatisering som en klar fördel, till exempel när det gäller att få upp en server snabbt – *”En slide och några knapptryckningar så bestämmer jag hur stor server jag ska ha så är den igång på väldigt kort tid”* säger en informant.

Däremot anser de inte att det är självklart att de skulle spara pengar på molnlösningar. Organisationen har byggt upp en enorm infrastruktur under många år, där allt är sammanvävt i stora komplexa system. Informanterna berättar att de kör billig intern drift där de äger både servrar och serverhallar, att flytta ut detta skulle alltså eventuellt kosta mer än det smakar. Det finns också en ekonomisk osäkerhet för informanterna kring viktiga tjänster i molnet, exempelvis berättar de att de har en mycket bra lösning för backuptagning internt, men om de skulle ta backuplösningar från molnet och dra ner all data skulle detta troligtvis kosta mycket och samma skulle gälla för säkerhetsuppdateringar som skulle behöva göras annorlunda. Detta är dolda kostnader, anser informanterna, som man normalt inte tänker på eller ser när man överväger molnlösningar. De är också osäkra på att ifall de skulle köpa tjänster i molnet, hur väl dessa skulle fungera med deras interna system, hur synergierna skulle fungera.

Fokusgruppen är relativt överens om att det faktiskt är upp till dem att vara tydliga över vad som ska finnas i molnlösningen, exempelvis var servrarna står, vilka upptider som krävs av tjänsterna eller hur ofta backuper körs. Om molnlösningen är tillräckligt bra behövs det inte funderas mer över det, säger en av informanterna. En av informanterna säger att man ska se molnet som en abstraktionsnivå: man ska se molnet men under där ska kunden inte behöva bry sig om. Man måste ställa krav på molntjänstleverantörerna, annars får man bara precis det man frågar efter, alltså vara noga med krav på exempelvis dubbla eller multipla serverar, reservkraft, upptid med mera.

En av informanterna drar en parallell med telekommunikation. Där köps tjänsten av telebolagen, inga egna kablar läggs. Telebolagen måste leverera den kapacitet och tillgänglighet som organisationen har ställt som krav. Resten kommer ner till förtroende, om inte telebolaget håller vad de lovat och sviker förtroendet, så byter företaget leverantör. Samma skulle gälla molntjänster, dock är dessa mer komplexa påpekar en informant, i och med att det är data och inte bara ren kommunikation som hanteras. Om tjänsten stängs ner skulle de förlora massa data. De vill försäkra sig mot det genom att dra backuper från molntjänsterna, men som de påpekar, att hade de litat på molntjänstleverantören, så hade det inte behövt göras. En informant säger ”*Förtroende är ett grymt viktigt ord i sammanhanget, jurister skulle påstå att man kan lösa detta med straffklausuler, men vi vill inte ha straffklausuler. Vi vill ha en tjänst som fungerar. Samma ögonblick vi har börjat lösa ut straffklausuler är det ju något som gått riktigt illa”.*

Andra osäkerheter fokusgruppen uttrycker är data som är lagrad hos molntjänstleverantören, hur de kan vara säkra på att ingen annan, exempelvis myndigheter som NSA eller FRA, går in och läser denna. En informant säger också att det värsta han anser skulle kunna hände med data dock är ifall någon går in och ändrar på data. Det skulle krävas enormt mycket tid att hitta vad som är ändrat och åtgärda det.

Fokusgruppen anser gemensamt att det som ligger mest efter i detta sammanhang, är lagarna. *”Molnleverantörerna pratar väldigt gärna teknik, bit och bytes, men så fort man närmar sig juridik så blir det tyst. Då vill inte de vara med och prata längre”* säger en av informanterna. En annan berättar om en klausul som Microsoft har i sina tjänster, där den säger att de har rätt att gå in och läsa det som eventuellt hotar deras intressen. Det anser informanterna inte vara bra för varken företag eller myndigheter och lägger fram kryptering som en eventuell lösning på detta. Han fortsätter med att säga att *”Man kan tänka sig att kryptering är lösning på även lagfrågan, om du lagrar något som är oläsligt, bara ettor och nollor och som du inte kan*

härleda där det går att avkryptera informationen. Men så långt har vi inte kommit ännu, det är bara en gråzon.”.

De uttrycker en önskan om att göra molnet mer tydligt också och dels att de själva kan göra det genom att ställa krav på exempelvis var lagringen ska ske och så vidare. De föreslår också en idé att använda en extern auditör som kan gå in granska kvaliteten och sätta sitt ok på detta som en slags certifiering. Detta skulle öka deras förtroende men de säger också att *”förtroende är bra, kontroll är bättre”*. De skulle önska en ökad kontroll och en ökad transparens från molntjänstleverantörens sida.

Intervjun avslutas med att vi ber informanterna kortfattat säga något om förtroende, de säger:

”Förtroende är något man måste förtjäna, det är inget du kan få. Sen kanske du kan förtjäna det nästan direkt hos mig eller genom att se på andra du jobbat med att man kan lita på dig.”

”Förtroende i ordet i sig är ju att lita på varandra, lojalitet har med det att göra och det är ju ömsesidigt. Relationer är ju ett sätt.”

”Det tar lång tid att förtjäna förtroende, men det går väldigt snabbt att rasera det”

”När t.ex. en läcka sker, så tar det väldigt lång tid att bygga upp förtroendet igen, det kanske inte ens går.”

5. Analys

Analys av reslutatet av intervjuerna kombinerat med tidigare presenterad teorier.

5.1 Molnet i stort - Vad tycker informanterna om molnet. Vad gör det bra/dåligt?

Informanterna vi intervjuat arbetar alla inom IT och är väl pålästa vad gäller molnet och hur teknologin fungerar. Tidigare visar vi på att det finns en okunskap gällande molntjänster och hur teknologin egentligen fungerar och att detta eventuellt skulle kunna bidra till en lägre förtroendegrad (se inledningen). Informanterna menar på att man ofta är osäker på någonting man inte förstår sig på till fullo. I vårt fall med de vi har intervjuat, så är bör detta inte vara en faktor som påverkar. Samtliga är pålästa och känner till de olika begreppen, termerna och teknologierna, exempelvis Software-as-a-Service, skalbarhet och hur teknologin går till. De är också bekanta med många av de större företag och organisationer som säljer olika sorters molntjänster som till exempel Microsoft, Google och Amazon. Informanterna säger sig också vara medvetna om att detta är det nästa stora som kommer och att detta är framtiden, precis som vi funnit i både populärmedia och branschtidningar. De säger sig också vara övervägande

positiva till teknologin, om än med vissa reservationer. Främst lockar tillgängligheten och de skalfördelar som molntjänsterna kan erbjuda. Informanterna skulle även lockas av priset, men samtliga är inte helt övertygade om att det är någon självklarhet att det skulle bli billigare. Informanten från en myndighet säger att om flera liknande myndigheter kan samarbeta genom molntjänster, så är detta både en ekonomisk och praktisk vinst. I intervjun med fokusgruppen, berättar dem att de redan har en såpass utbyggd infrastruktur och billig intern drift att det skulle vara olönsamt att flytta allt till molnet. Däremot tror informant A att allt succesivt kommer att flyttas ut i molnet. Vi kände att informanterna var väl pålästa om hur molnet fungerar. Att en låg förtroenderåd skulle bero på okunskap i själva teknologin känns därför inte speciellt troligt.

5.2 Säkerhet - Vad tycker informanterna om säkerhet och hur tänker dem kring det.

Säkerhetsfrågan är en stor del av det som de intervjuade bygger sitt förtroende igenom. Ur de nio riskerna som CSA tog upp så är det Data Breaches, Data Loss och Insufficient Due Diligence som var de överlägset största orosmomenten för informanterna. Känslan under alla intervjuerna var att de känner sig betydligt säkrare att ha sin data och tjänster in-house än att använda diverse molntjänster. Rent tekniskt är det inte alls säkert att det är så, då det rimligtvis inte behöver vara svårare att hacka sig in på ett slumpvis utvalt svenskt företag än att hacka sig in på Microsoft eller Google. Däremot tyckte informanterna att data breaches är ett problem i molnteknologin, då företagen *"lägger alla äpplen i samma korg"*. Hackare som tar sig in hos molntjänstleverantörerna kan alltså komma över data från mängder av företag istället för endast en, vilket gör det till ett attraktivare mål och detta var en faktor för de intervjuade. I fokusgruppen var de klart överens om att det kommer ut att ett företag haft sådana data breaches, så tappas allt förtroende för detta företag. Data loss var en annan risk som informanterna uttryckte oro över. De sa bland annat att när de själva har allting in-house, vet de hur rutinerna för backup och säkerhetsuppdateringar går till, men i en molntjänst får de lita på molntjänstleverantören. I fokusgruppen berättar dem att de annars skulle dra ner data från molnet på en egen backup, men att detta skulle vara mycket kostsamt att dra ner så mycket data. Här visas ett bra exempel på att avsaknaden av förtroende kan innebära högre kostnader (Papazoglou & Ribbers 2006). Det tredje som de intervjuade uttryckte oro över är det som CSA kallar Insufficient Due Diligence. Det handlar alltså om att veta hur det operativa ansvaret ser ut för exempelvis kryptering och säkerhetsövervakning. Informanterna vill inte att olika myndigheter som till exempel NSA eller FRA ska kunna gå in och läsa deras data, men de tyckte att det är svårt med molntjänstleverantörer att veta ifall de har avtal med

sådana här myndigheter eller om molntjänstleverantören ägs av ett företag som ägs av ett annat företag som har avtal med dessa, vilket skulle kunna ge dem rätt att gå och läsa data. En av de intervjuade ur fokusgruppen föreslår kryptering som en lösning på detta, men säger också att teknologin inte riktigt nått dit ännu.

5.3 Legala frågor - Vad tycker informanter om lagar och regelverk som är kopplade till molntjänster

Informanterna uttryckte både en osäkerhet kring lagarna och regelverken som är kopplade till molntjänster och molntjänstleverantören och en tydlig åsikt om att lagarna behöver förändras. Likt Edvardsson och Frydlinger (2013) uttrycker, så är många av grundfrågorna angående lagar av stor osäkerhet för informanterna, exempelvis lagval, integritet och personuppgiftshantering, rätten till data och tjänstenivå. I frågan om lagval tycker samtliga informanter att det är svårt att veta vilket lands lagar som gäller när data lagras i molnet. Informant A menar också att personuppgiftshanteringen gör det extra krångligt, framför allt för dem som en myndighet, att de måste veta var data lagras och om den i så fall omfattas av EUs personuppgiftslag. Även avtalen är svårtydda enligt informanterna. Precis som det Thorslund (2013) tar upp så undrade informanterna främst var informationen lagras, vem som kan läsa den och om molntjänstleverantören använder sig av underleverantörer. De uttryckte en oro kring lagar och hur det är svårt att vara säker på att de får det de vill. Som en ur fokusgruppen säger: *”Molnleverantörerna pratar väldigt gärna teknik, bit och bytes, men så fort man närmar sig juridik så blir det tyst. Då vill inte de vara med och prata längre”*. Det var det intrycket vi också fick efter att ha pratat med alla informanter, de får väldigt bra information om hur allting fungerar rent tekniskt och praktiskt, till och med säkerheten, men lite om det legala och hur detta fungerar. Däremot är dem väldigt medvetna om hur viktigt detta är och vi får intrycket av att detta medför en stor osäkerhet kring molntjänster på grund av det legala. Fokusgruppen anser att det är juridiken som ligger efter.

5.4 Förtroende - Vad tycker informanterna om förtroendet. Hur kan det ökas och vad är förtroende för dem.

Samtliga av informanterna håller med om att förtroende är en viktig del i valet av tjänster och molntjänstleverantörer. Precis som Papazoglou och Ribbers (2006) argumenterar så säger informanterna att förtroende är något som förändras över tiden beroende på de erfarenheter man har av varandra. Om till exempel en molnleveratör skulle drabbas av en stor läcka, tappas allt förtroendet helt för denna molntjänstleverantör och detta kanske aldrig kan byggas upp igen som en av informanterna säger. I och med att en del prestandaproblem (MyNewsDesk 2014) och säkerhetsproblem (McMillan 2009) har förekommit, så kan detta ha bidragit till att

informanterna inte känner alltför starkt förtroende till molntjänster. För precis som Khaled et al. (2010) säger så måste all ny teknologi gradvis måste bygga upp sitt rykte för bra prestanda och säkerhet och på så sätt förtjäna förtroende över tid. I två av de tre intervjuer vi genomförde sas det uttryckligen att *"förtroende tar lång tid att bygga, men kan raseras ögonblickligen"*. Samtliga informanter säger också, precis som vi i teorin fastställt från Lim et al. (2010), att en av de viktigaste punkterna de undersöker är att skapa ett förtroende för en molntjänstleverantör, är att kolla på vilka andra kunder de har och vilka andra företag de associerar sig med. I detta fall tittar de både på vilka företag molntjänstleverantörerna marknadsför sig med och vilka företag som liknar ens eget som är kunder. Detta gäller speciellt informanten från myndigheten, där de ofta undersöker vad det är för tjänster som andra myndigheter använder. Informanterna är dock oense om hur nära samarbetet med molntjänstleverantören bör vara för att bäst få ett starkt förtroende till varandra. Informant A anser att partnerskap skulle vara vägen att gå, det vill säga jobba starkt nära varandra och kanske ha personliga kontaktpersoner. Ser vi tillbaka på Papazoglou och Ribbers (2006) så innebär detta alltså att typen av förtroende byts från företagsbaserat eller institutionsbaserat förtroende till personbaserat förtroende och som Lim et al. (2006) fastställer, så är det lättare att ha ett förtroende för en fysisk person än att ha förtroende i en onlinemiljö. I fokusgruppen var de inte lika säkra på att detta skulle vara optimalt. De ansåg att det skulle bli alltför vänskapligt och att det skulle vara svårt att hålla en professionell nivå i ett sådant partnerskap. De eftersträvade istället tydlig och rak kommunikation där de som kund måste ta sitt ansvar att ställa krav på tjänsten och molntjänstleverantören och därefter lita på att molntjänstleverantören håller det som lovats.

6. Diskussion

I denna studie har vi undersökt hur ökat förtroende skapas mellan kund och molntjänstleverantör. Efter att ha utfört litteraturstudier och intervjuer kan vi först och främst konstatera att förtroende är en väldigt viktig faktor inom molnmiljön. Både i litteraturen och från intervjuerna kan vi fastslå att det innebär ökade kostnader vid lägre förtroendenivå för varandra och ett mer trögt affärsutbyte. En hög grad av förtroende vinner både molntjänstleverantör och kunder på. När vi försökt undersöka varför inte molntjänster har så hög grad av förtroende så fann vi flera förklaringar till detta. I våra informanters fall berodde det inte på okunskap om själva molnteknologin utan mer på okunskap kring molnet angående

exempelvis med lagar och säkerhet. Det finns en ovilja att lämna ifrån sig information till en annan part och detta skapar en osäkerhet. Att lagarna inte är tydliga och att det finns få prejudicerade fall är något som skapar ännu större osäkerhet. Här tror vi dock att det fungerar från båda hållen, molntjänstleverantörerna är otydliga gällande lagarna och vad det är som gäller, samtidigt som den potentiella kunden inte ställer tillräckligt höga krav eller har satt sig in tillräckligt i situationen. Vi vill föreslå ett ökat samarbete vid införskaffande av molntjänster och bättre möjligheter för kunderna att förhandla kring avtal som möter deras behov. Gällande säkerhetsaspekten har större läckor som kommit ut i media påverkat opinionen negativt. Att hindra sådana läckor är självklart svårt, men bör vara något som går att förbättra. Att skaffa en slags certifiering eller auditörer för hur molntjänstleverantören hanterar data tycker vi låter som en bra idé. Kortsiktigt kan det visa på brist av förtroende men om ett företag har en certifiering i flera år, så visar detta kunden att de kan lita på företaget och skapar på så sätt förtroende. Kunderna efterfrågar också större transparens från molntjänstleverantören och mer tydlighet gällande både lagar och säkerhet. Som kund vill man veta så att det inte finns dolda avtal med andra organisationer, exempelvis myndigheter. Detta tror vi också skulle hjälpa molntjänstleverantören att nå ut till sina kunder och skapa ett ökat förtroende. Sedan är det inte bara upp till molntjänstleverantörerna utan själva tjänsten behöver få hjälp med att skapa ett ökat förtroende. Lagar angående molnteknologi behöver ses över och förtydligas för att skapa en större klarhet för kunden. En närmare kontakt med kunden tror vi skulle gynna molntjänstleverantörerna och skapa en ökad förtroendekänsla hos kunden.

7. Slutsats

Syftet med studien var att påvisa hur viktigt förtroende är vid införskaffande av molntjänster och att ge en ökad kunskap och medvetenhet gällande molntjänster. Syftet med studien var också att undersöka hur man skulle kunna göra för att skapa ett ökat förtroende för molntjänster och molntjänstleverantörer. Vi har i vår studie dragit slutsatsen att det inte bara är molntjänstleverantörerna i sig som har lågt förtroende, utan att det även finns en skeptism för molntjänsterna i sig. Lagarna om molntjänster har inte hängt med i utvecklingen och det är främst där det finns både en osäkerhet och okunskap hos kunderna.

- Vår slutsats är att lagarna bör ses över och uppdateras för att kunderna ska känna ett större förtroende för molntjänster.

- Vi tror att med ökad transparens från molntjänstleverantören och ett tydligare regelverk skulle öka kundernas förtroende. Om kunden kan få mer insyn i hur allt fungerar och inte känner att molntjänstleverantören gömmer sig bakom avtal och lagar skapas en ökad känsla av förtroende.

- Vi har också kommit fram till att en närmare och mer personlig kontakt mellan kund och molntjänstleverantör skulle öka förtroendet och att en eventuell klassning eller certifiering av molntjänstleverantören skulle skapa en förtroendekänsla hos kunden om denne ser att molntjänstleverantören håller vad de lovar.

- Till sist konstaterar vi att även kunden måste ta sitt ansvar och vara pålästa och ställa krav på molntjänstleverantören. Om molntjänstleverantören då kan motsvara dessa krav skapas ett större förtroende mellan dem och kunden.

8. Förslag till fortsatt forskning

Fortsatt forskning hade kunnat utvidga denna studie på fler företag. På grund av tidsbrist kunde vi endast ta med tre företag och det hade varit intressant att få informanter från många fler företag, även utanför Sverige. Vi tror också det hade varit intressant att undersöka huruvida mindre företag känner större förtroende till molntjänster än de större företagen gör eller tvärtom. En annan intressant studie hade varit om det undersöks på ett mer kvantitativt sätt hur mycket förtroende, eller brist på det, faktiskt kan kosta ett företag.

Ett annat förslag är att utgå från domen mot Google (se bilaga 2) och undersöka hur Google ställer sig mot andra verksamheter. Hur deras normer och integritet ställer sig mot andra organisationer.

9. Referenser

Bailey, W. (2012). *Insider threats to cloud*. Cloud Tweaks.

Cloud Magazine. (2014). http://cloud.idg.se/ [2014-05-22]

Datainspektionen. (2014a). *Informationssäkerhet faktablad*. http://www.datainspektionen.se/Documents/faktablad-informationssakerhet.pdf [2014-05-11]

Datainspektionen. (2014b). *Molntjänster och personuppgiftslagen*. http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/molntjanster/ [2014-05-12]

Edvardsson, T. & Frydlinger, D. (2013). *Molntjänster*. *Juridik, affärer och säkerhet*. Upplaga 1:1 Norstedts Juridik AB.

Export.gov. (2013). *U.S.-EU Safe Harbor*. http://export.gov/safeharbor/eu/index.asp [2014-05-22]

Google (2014). Molntjänster. https://www.google.se/#q=molntj%C3%A4nster [2014-05-22]

Hassan, T. (2011) Molnet, upplevda kontra faktiska risker - vägen till ökad medvetenhet. Kandidatuppsats, institutionen för tillämpad informationsteknologi. Göteborgs universitet.

Höcke,K., Pihlström,S., & Helenius,S. (2012) Ägandeskap av data i molnet. En studie om företags attityder och resonemang kring ägandeskap när de placerar sin data i molntjänster. Kandidatuppsats, institutionen för tillämpad informationsteknologi. Göteborgs universitet.

Informationssäkerhet (2014). *Vad är informationssäkerhet?* https://www.informationssakerhet.se/sv/informationssakerhet/allmant/ [2014-05-01]

Khan, K. & Malluhi, Q. (2010). Establishing Trust in Cloud Computing. *IT-Pro*, September/October 2010. IEEE Computer Society.

Lexin (2014). Förtroende. http://lexin2.nada.kth.se/lexin/#searchinfo=both,swe_swe,F%C3%B6rtroende [2014-05-19]

Lim, K., Sia, C., Lee, M. & Benbasat, I. (2006). Do I Trust Online, and if so, will I buy? *Journal of Management Information Systems*. Fall 2006, Vol. 23, No. 2, pp. 233–266

Linthicum, D. *As cloud use grows, so will rate of DDoS attacks*. InfoWorld Home (2013). http://www.infoworld.com/d/cloud-computing/cloud-use-grows-so-will-rate-of-ddos-attacks-211876 [2014-05-05]

Los, R., Shackleford, D., Sullvian, B., Ginsburg, A., Santos, L JR., Scoboria, E., Scoboria, K. & Yeoh, J. *The Notorious Nine: Cloud Computing Top Threats in 2013*. Cloud Security Alliance. (2013). https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf [2014-05-11]

Malone, T., Menken, I., & Blokdijk, G. (2009*). Itil V3 Foundation Complete Certification Kit*

Mattmar, U. & Holmin, M. (2013). *Snabbväxande molntjänster väcker farhågor*. http://www.svt.se/agenda/snabbvaxande-molntjanster-vacker-farhagor. [2014-04-15]

McMillan, R. (2009). Hackers find a home in Amazon´s EC2 cloud. *Computer World*. http://www.computerworld.com/s/article/9142058/Hackers_find_a_home_in_Amazon_s_EC2_cloud [2014-05-11]

Mell, P. & Grace, T. (2011). *The NIST Definition of Cloud Computing*. http://www.nist.gov/itl/cloud/publications.cfm [2014-05-08]

MyNewsDesk. (2014). *73% av företagen befarar att molnleverentörerna inte informerar om prestandaproblem*. http://www.mynewsdesk.com/se/compuware-sverige/pressreleases/73-av-foeretagen-befarar-att-molnleverantoererna-inte-informerar-om-prestandaproblem-992329 [2014-05-22]

Papazoglou, M. & Ribbers, P. (2006). *E-Business*. *Organizational and technical foundations*. John Wiley & Sons, Ltd.

Patel, R. & Davidsson, B. (2013). *Forskingsmetodikens grunder - Att planera, genomföra och rapportera en undersökning*. Upplaga 4:4. Studentlitteratur.

Reddy Kandukuri, B., Paturi V, R., Dr. Rakshit, A. (2009). Cloud Security Issues. *Advanced Software Technologies International Institute of Information Technology Pune, India*.

SFS 1998:204. *Personuppgiftslag*. *Stockholm: Justitiedepartementet*

Smyth, H., Gustafsson, M. & Ganskau, E. (2010). The value of trust in project business. *International Journal of Project Management 28* 2010, pp 117-129.

Thorslund, J. (2013*). E-samhället i praktiken*. *Använd molntjänster på rätt sätt*. SKL. http://www.skl.se/MediaBinaryLoader.axd?MediaArchive_FileID=6a340881-1b38-47e6-b8a3-fae23fbc95f8&FileName=E-samh%C3%A4llet+i+praktiken+-+molntj%C3%A4nster.pdf [2014-05-12]

Vetenskapsrådet (2009). *Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning* . http://www.codex.vr.se/texts/HSFR.pdf [2014-05-19]

Wieder, P., M. Butler, J., Theilmann, W., Ramin Yahyapour, R. (2012). *Service Level Agreements for Cloud Computing*.

Wikipedia (2014a). Informationssäkerhet. http://sv.wikipedia.org/wiki/Informationss%C3%A4kerhet [2014-05-10]

Wikipedia (2014b). Phising. http://sv.wikipedia.org/wiki/N%C3%A4tfiske [2014-05-15]

Wikipedia (2014c). Cross site scripting. http://sv.wikipedia.org/wiki/Cross_site_scripting [2014-05-15]

Wiktionary (2014). Förtroende. http://sv.wiktionary.org/wiki/f%C3%B6rtroende [2014-05-22]

Åhlin, D. (2013). *Sju av tio vägrar lagring i molnet*. http://techworld.idg.se/2.2524/1.534271/sju-av-tio-vagrar-lagring-i-molnet. [2014-05-22]

Älmeblad, J. (2011) Molnet och dess möjligheter och utmaningar. Kandidatuppsats, institutionen för informatik. Umeå universitet.

10. Bilagor

10.1 Bilaga 1 – Intervjufrågor

Förklara syfte med undersökningen och den intervjuades bidrag. Tratt-teknik

Tema 1, Bakgrund

Vad jobbar du med och vilka är dina arbetsuppgifter?

Tema 2, Nuvarande IT-stöd

Vad är det för IT-system ni använder nu? Varför valde ni denna lösning?

Är ni nöjda med IT-Systemet idag (varför?)

Hur går beställningen av en IT-tjänst till?

Vad har ni för förväntningar på ett system?

Tema 3, Molnlösningar

Använder ni er av någon slags molnlösning i dagsläget? (om inte, är det aktuellt/vad får er att tveka?)

Finns det något typiskt problem med molnlösningar? (Hur känner du inför säkerheten med molnet)?

Tema 4, Utmaningar

Litar ni på era IT-leverantörer? Varför tror du att ni gör det?

Vad ser du som största utmaningar med molnlösningar? Vad behövs göra bättre?

Hur tror du att man som kund kan få större förtroende för en IT leverantör och kanske främst molntjänster?

10.2 Bilaga 2 - Kammarrätten

KAMMARRÄTTEN I STOCKHOLM
Avdelning 01

DOM

2014 -04- 07
Meddelad i Stockholm

Mål nr 7123-13

KLAGANDE
1. Google Inc.
2. Google Ireland Ltd.

Ombud: Advokat Niklas Thörnestad
Advokatfirman Cederquist KB
Box 1670
111 96 Stockholm

Ombud: Advokat Erik Wernberg
Adress som ovan

MOTPART
Datainspektionen
Box 8114
104 20 Stockholm

ÖVERKLAGAT AVGÖRANDE
Förvaltningsrätten i Stockholms beslut den 31 oktober 2013 i mål nr 15637-13 och 15643-13, se bilaga A

SAKEN
Avvisat överklagande

KAMMARRÄTTENS AVGÖRANDE

1. Kammarrätten meddelar prövningstillstånd.

2. Kammarrätten avslår överklagandet.

Postadress	Besöksadress	Telefon	Telefax	Expeditionstid
Box 2302 103 17 Stockholm	Birger Jarls Torg 5	08-561 690 00 **E-post**: kammarrattenistockholm@dom.se www.kammarrattenistockholm.domstol.se	08-14 98 89	måndag – fredag 08:00-16:00

YRKANDEN M.M.

Google Inc. och Google Ireland Ltd. yrkar att kammarrätten förklarar att bolagen äger rätt att föra talan mot Datainspektionens beslut och visar målet åter till förvaltningsrätten för erforderlig prövning i sak. Bolagen vidhåller vad som tidigare har anförts och tillägger bl.a. följande. Nya tjänster, såsom molntjänster, har kommit till i tiden efter merparten av Högsta förvaltningsdomstolens praxis. För att anpassa sig till ny teknik måste domstolarna göra andra hänsynstaganden än de som förvaltningsrätten har gjort.

Av 30 § andra stycket och 31 § personuppgiftslagen (1998:204) – PuL framgår att ett personuppgiftsbiträde ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Återgärderna ska vidare åstadkomma en säkerhetsnivå som är lämplig med beaktande av bl.a. de tekniska möjligheter som finns samt vad det skulle kosta att genomföra åtgärderna. Både de tekniska möjligheterna och kostnaden för genomförandet av säkerhetsåtgärderna är omständigheter hänförliga till framför allt molntjänsten som sådan. Bolagen har således intresse i saken av en natur som får och ska beaktas vid prövningen av om personuppgiftsbiträdesavtalet lever upp till de krav som ställs i PuL.

SKÄLEN FÖR KAMMARRÄTTENS AVGÖRANDE

Kammarrätten finner skäl att meddela prövningstillstånd och tar upp målet till omedelbart avgörande.

Vad bolagen har anfört i kammarrätten föranleder inte kammarrätten att göra någon annan bedömning än den förvaltningsrätten har gjort. Överklagandet ska därför avslås.

HUR MAN ÖVERKLAGAR, se bilaga B (formulär 1).

Eva Jagander
kammarrättsråd
ordförande

Catharina Brege
kammarrättsråd

Eva Edwardsson
kammarrättsråd
referent

Erika Uddén
föredragande

Bilaga 1

FÖRVALTNINGSRÄTTEN I STOCKHOLM
Allmänna avdelningen
Enhet 12

BESLUT
2013-10-31
Meddelat i Stockholm

Mål nr
15637-13
15643-13
Enhet 12

KLAGANDE
1. Google Inc.

2. Google Ireland Ltd.

Ombud för 1 och 2: Advokaterna Eric Johnson och Erik Wernberg
Advokatfirman Cederquist KB
Box 1670
111 96 Stockholm

MOTPART
Datainspektionen
Box 8114
104 20 Stockholm

ÖVERKLAGAT BESLUT
Datainspektionens beslut 2013-05-31 (dnr 1351-2012)

SAKEN
Tillämpning av personuppgiftslagen; fråga om talerätt

Förvaltningsrätten avvisar överklagandena.

Postadress	Besöksadress	Telefon	Telefax	Expeditionstid
115 76 Stockholm	Tegeluddsvägen 1	08-561 68000	08-561 68001	måndag – fredag 09:00-15:00
		E-post: förvaltningsrätten.stockholm@dom.se		

BAKGRUND

Datainspektionen konstaterade i ett beslut den 31 maj 2013 att personuppgiftsbiträdesavtalet som Kommunstyrelsen i Salems kommun (kommunen) avsåg att teckna med en molntjänstleverantör inte uppfyllde kraven enligt personuppgiftslagen (1998:204) (PuL). Datainspektionen förelade i samma beslut kommunen att upphöra med behandlingen av personuppgifter i molntjänsten eller vidta åtgärder för att personuppgiftsbiträdesavtalet ska vara förenligt med PuL.

Kommunen avsåg att teckna det aktuella personuppgiftsbiträdesavtalet med Google Ireland Ltd. och Google Inc. (bolagen).

YRKANDEN M.M.

Bolagen överklagar Datainspektionens beslut och yrkar i första hand att beslutet ska undanröjas. I andra hand yrkar bolagen att beslutet ska undanröjas och ärendet återförvisas till Datainspektionen för ny handläggning. Till stöd för att bolagen har rätt att överklaga Datainspektionens beslut anför de i huvudsak följande.

Klagorätt på grund av partsställning hos Datainspektionen

Under handläggningen hos Datainspektionen betraktades bolagen som part av bolagen själva, kommunen och Datainspektionen. Bolagen har deltagit i kommunens inlagor till Datainspektionen, deltagit i möten med Datainspektionen, svarat på frågor från Datainspektionen och förelagts att inkomma med information i ärendet till Datainspektionen. Bolagen har även uttryckligen blivit angivna som berörda parter på sidan två i det överklagade beslutet.

Bolagens uppdrag som personuppgiftsbiträde baseras på bestämmelser i PuL, som utgör en implementering av ett EU-direktiv. En grundläggande princip är att ett beslut som baserar sig på EU-rätt måste tillåtas bli föremål för överprövning i domstol.

Om några förändringar inte vidtas i personuppgiftsbiträdesavtalet mellan kommunen och bolagen är bolagens uppdrag avslutat, som en direkt konsekvens av det överklagande beslutet. Om beslutet i stället leder till materiella ändringar av personuppgiftsbiträdesavtalet är det bolagen som kommer att tvingas utföra allt praktiskt arbete under processen. Dessa ändringar kan komma att bli omfattande, tidskrävande och kostsamma. Beslutet kan även ha en negativ inverkan på bolagens affärsverksamhet. Bolagens hela molntjänstsystem kan tvingas genomgå mycket omfattande och kostsamma förändringar. Att inte tillerkänna bolagen talerätt skulle strida mot den princip som har fastställt av Högsta förvaltningsdomstolen i RÅ 2006 ref 9.

Datainspektionen bestrider att bolagen har rätt att överklaga det aktuella beslutet och anför i huvudsak följande till stöd för sin talan.

Bolagen uppfyller inte de kriterier som uppställs i 22 § förvaltingslagen (1986:223) (FL) för att ha talerätt i målen. Bolagen intog inte partsställning hos Datainspektionen, de saknar ett av rättsordningen erkänt intresse i saken och de har inte heller en rättsställning som påverkas av beslutet.

I det överklagade beslutet har Datainspektionen granskat kommunen i dess roll som personuppgiftsansvarig. Som personuppgiftsansvarig är det kommunen som bestämmer ändamålen med och medlen för den behandling av personuppgifter som utförs. Det är därmed även kommunen som exempelvis är skadeståndsskyldig gentemot den registrerade för den

Bolagens rättsliga ställning påverkas av beslutet

Bolagen är personuppgiftsbiträde åt kommunen. Detta uppdrag regleras av bestämmelser i PuL. Som en följd härav kan bolagens uppdrag åt kommunen bli föremål för och påverkas av ingripanden från Datainspektionen. Genom det överklagade beslutet har Datainspektionen permanent avslutat eller väsentligen ändrat innehållet i bolagens uppdrag åt kommunen. Effekten av beslutet är därför direkt för bolagen. Deras rättsliga ställning som personuppgiftsbiträde i enlighet med PuL upphör (eller förändras väsentligt).

Bolagen har ett intresse i saken som har erkänts av rättsordningen

Bolagen deltog i förfarandet hos Datainspektionen. Med undantag för att bolagen inte fick chans att slutföra sin talan gjorde Datainspektionen ingen åtskillnad mellan bolagen och kommunen under myndighetens handläggning av ärendet. Det är tillräckligt att intresseerkännandet kan härledas ur lag, förarbeten, syftet bakom lagstiftningen eller beslutsmyndighetens faktiska handlande. Bekräftelsen kan alltså komma till uttryck genom att klaganden (som i förevarande fall) rent faktiskt har beretts tillfälle att framföra sin sak under handläggningen hos beslutsmyndigheten.

Bolagen har ett rättsskyddsintresse

Med hänvisning till bl.a. EU-rättsliga principer och till artikel 6 i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna har i doktrin betonats att en överklaganderätt ska medges så snart det föreligger ett praktiskt behov därav och att detta behov ska bedömas utifrån vilka praktiska konsekvenser beslutet i fråga har för klaganden.

eventuella skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med PuL har orsakat.

En personuppgiftsansvarig kan anlita ett personuppgiftsbiträde för att utföra en personuppgiftsbehandling. Biträdets uppgift är att behandla personuppgifter för den ansvariges räkning och efter dennes instruktioner. Den personuppgiftsansvarige kan aldrig överlåta sitt ansvar enligt PuL till ett personuppgiftsbiträde. När Datainspektionen granskar en personuppgiftsbehandling är det alltid den som bestämmer ändamålen med och medlen för behandlingen, dvs. den personuppgiftsansvarige, som är tillsynsobjekt.

Bolagen har inte haft partsställning hos Datainspektionen

Det är kommunen som har varit föremål för Datainspektionens granskning och beslutet är ställt till kommunen i egenskap av personuppgiftsansvarig. Bolagen har inte haft partsställning i ärendet.

Den omständighet att kommunen väljer att rådgöra med sitt personuppgiftsbiträde under Datainspektionens handläggning av ärendet medför inte att biträdet får ställning som part i ärendet. Att bolagen har ett betydande intresse i saken innebär inte att bolagen har haft, eller ska få, partsställning i målen.

Bolagen har inget av rättsordningen erkänt intresse i saken

För att bolagen ska anses ha ett av rättsordningen erkänt intresse i saken är det avgörande att bolagen har ett intresse som det varit möjligt att beakta vid sakens prövning. Bolagens ekonomiska intresse i saken är inte ett av rättsordningen erkänt intresse.

Bolagens rättsställning påverkas inte av beslutet

Vid bedömningen av om tredje mans rättsställning påverkas av ett beslut är det avgörande huruvida beslutets verkningar mot en part i förvaltningsärendet enligt lag direkt leds över till dennes motpart i det civilrättsliga förhållandet. Det saknar betydelse att en avtalspart drabbas ekonomiskt av ett beslut som enbart är riktat mot adressaten. I den mån Datainspektionens beslut påverkar bolagens affärmässiga verksamhet negativt är denna påverkan endast indirekt.

SKÄLEN FÖR AVGÖRANDET

Enligt 22 § FL får ett beslut överklagas av den som beslutet angår, om det har gått honom emot och beslutet kan överklagas. Frågan i målet är om Datainspektionens beslut beträffande kommunens hantering av personuppgifter angår bolagen på ett sådant sätt att de har rätt att föra talan mot beslutet. 22 § FL ger enbart en allmän riktlinje för hur frågan om talerätt ska bedömas. De principer som har utbildats i rättspraxis blir därmed avgörande för bedömningen.

Bolagen har inte haft partsställning hos Datainspektionen

Den som har haft ställning som part hos beslutsmyndigheten har alltid klagorätt enligt 22 § FL om beslutet går denne emot. Datainspektionens beslut är inte ställt till bolagen. Datainspektionen har emellertid berett bolagen tillfälle att yttra sig i ärendet. Bolagen har även deltagit i kommunens yttranden till och möten med Datainspektionen.

Förvaltningsmyndigheter har ett ansvar för att deras ärenden blir tillräckligt utredda. Enligt 13 § FL har förvaltningsmyndigheter möjlighet att inhämta yttranden från andra myndigheter och företag. Att bolagen har beretts möjlighet att bidra till utredningen i ärendet, både på egen hand och genom kommunen, leder enligt förvaltningsrätten inte till att bolagen har haft partsställning i ärendet hos Datainspektionen.

Inte heller vad bolagen har anfört om att de anges som berörda parter på sidan två i Datainspektionens beslut föranleder att bolagen kan anses ha haft partsställning då där endast anges vilka som har yttrat sig i ärendet till Datainspektionen.

Bolagens rättsställning har inte påverkats av beslutet

Talerätt enligt 22 § FL har i rättspraxis även tillerkänts enskild som inte har haft ställning som part hos beslutsmyndigheten men vars rättsställning påverkas av beslutet (se t.ex. RÅ 1963 ref. 20 och RÅ 82 2:27). För att tredje mans rättsställning ska anses påverkad av ett beslut måste beslutets rättsverkningar enligt lag direkt ledas över till denne. I RÅ 82 2:27 kunde t.ex. en fastighetsförsäljare överklaga ett beslut att vägra köparen förvärvstillstånd eftersom beslutet enligt lag medförde att köpeavtalet blev ogiltigt.

Bolagen har genom ett avtal uppdraget att gemensamt vara personuppgiftsbiträde åt kommunen. Datainspektionens beslut att bl.a. förelägga kommunen att vidta åtgärder för att personuppgiftsbiträdes-avtalet ska vara förenligt med bestämmelserna i PuL påverkar bolagen genom deras avtalsförhållande med kommunen. Beslutets verkningar är därmed inte direkt överförda genom lag till bolagen.

Bolagen företräder inte ett intresse som är möjligt att beakta vid sakens prövning

Förutom parter hos beslutsmyndigheten, och enskilda som får sin rättsställning påverkad av ett beslut, så har även enskilda som har *ett intresse i saken som erkänns av rättsordningen* eller som har *ett beaktansvärt intresse att få sin talan prövad* tillerkänts talerätt enligt 22 § FL (se t.ex. RÅ 1994 ref. 30 och RÅ 2006 ref. 9). En förutsättning för att annan än den som har varit part hos beslutsmyndigheten ska ha talerätt är ändå att klaganden kan åberopa ett intresse som är möjligt att beakta vid sakens prövning (se HFD 2012 ref. 24).

Datainspektionen har granskat kommunens behandling av personuppgifter i egenskap av personuppgiftsansvarig. En personuppgiftsansvarig kan enligt PuL ge i uppdrag åt ett personuppgiftsbiträde att hantera personuppgifter för den personuppgiftsansvariges räkning. Datainspektionen har i det överklagade beslutet kommit fram till att kommunens personuppgiftsbiträdesavtal med bolagen inte uppfyller bestämmelserna i PuL. Vid bedömningen av om kommunen lever upp till bestämmelserna i PuL har Datainspektionen inte haft möjlighet att beakta de ekonomiska intressen som bolagen har i saken. Bolagen har därmed inte något intresse som är möjligt att beakta vid sakens prövning.

FÖRVALTNINGSRÄTTEN I STOCKHOLM
Allmänna avdelningen

BESLUT

Inte heller vad bolagen har anfört i övrigt föranleder att de kan anses ha rätt att föra talan mot Datainspektionens beslut. Sammanfattningsvis anser därför förvaltningsrätten att Datainspektionens beslut inte angår bolagen på ett sådant sätt att de har rätt att överklaga beslutet. Överklagandena ska därför avvisas.

HUR MAN ÖVERKLAGAR, se bilaga (DV 3109/1a)

Madeleine Benndorf
rådman

Förvaltningsrättsfiskalen Ulrika Moberg har föredragit målet.

Bilaga B

HUR MAN ÖVERKLAGAR

Den som vill överklaga kammarrättens avgörande ska skriva till Högsta förvaltningsdomstolen. Skrivelsen ställs alltså till Högsta förvaltningsdomstolen *men ska skickas eller lämnas till kammarrätten.*

Överklagandet ska ha kommit in till kammarrätten *inom tre veckor* från den dag då klaganden fick del av beslutet. Om beslutet har meddelats vid en muntlig förhandling, eller det vid en sådan förhandling har angetts när beslutet kommer att meddelas, ska dock överklagandet ha kommit in inom tre veckor från den dag domstolens beslut meddelades. Tiden för överklagande för det allmänna räknas dock från den dag beslutet meddelades.

Om sista dagen för överklagande infaller på en lördag, söndag eller helgdag, midsommar-, jul- eller nyårsafton, räcker det att skrivelsen kommer in nästa vardag.

För att ett överklagande ska kunna tas upp i Högsta förvaltningsdomstolen krävs att *prövningstillstånd* meddelas. Högsta förvaltningsdomstolen lämnar prövningstillstånd om det är av vikt för ledning av rättstillämpningen att överklagandet prövas eller om det finns synnerliga skäl till sådan prövning, såsom att det finns grund för resning eller att målets utgång i kammarrätten uppenbarligen beror på grovt förbiseende eller grovt misstag.

Om prövningstillstånd inte meddelas står kammarrättens beslut fast. Det är därför viktigt att det klart och tydligt framgår av överklagandet till Högsta förvaltningsdomstolen varför man anser att prövningstillstånd bör meddelas.

Skrivelsen med överklagande ska innehålla följande uppgifter;

1. den klagandes namn, person-/organisationsnummer, postadress, e-postadress och telefonnummer till bostaden och mobiltelefon. Dessutom ska adress och telefonnummer till arbetsplatsen och eventuell annan plats där klaganden kan nås för delgivning lämnas om dessa uppgifter inte tidigare uppgetts i målet. Om klaganden anlitar ombud, ska ombudets namn, postadress, e-postadress, telefonnummer till arbetsplatsen och mobiltelefonnummer anges.Om någon person- eller adressuppgift ändras är det viktigt att anmälan snarast görs till Högsta förvaltningsdomstolen
2. det beslut som överklagas med uppgift om kammarrättens namn, målnummer samt dagen för beslutet
3. de skäl som klaganden vill åberopa för sin begäran om att få prövningstillstånd
4. den ändring av kammarrättens beslut som klaganden vill få till stånd och skälen för detta
5. de bevis som klaganden vill åberopa och vad han/hon vill styrka med varje särskilt bevis.

DV 681 *Formulär 1*