



Avdelningen för Datavetenskap

205 06 Malmö, Sverige

Examensarbete

15 högskolepoäng, grundnivå

## Molntjänsts-kontraktering -

Aspekter att överväga vid kontraktering med molnleverantör

Cloud Computing Contracts –

Aspects to consider when contracting with a Cloud provider

Pierre Karlsson

Examen: Kandidatexamen 180 hp

Huvudämne: Informationssystem

Program: Affärssystem

Datum för slutinlämning: 2012-06-13

Handledare: Bengt J Nilsson

Examinator: Mia Persson

Intressent: C. Dan Ahlström

## Sammanfattning

Denna rapport belyser aspekter som kunder borde vara medveten om vid kontraktering med en molnleverantör. Molntekniken är effektiv, skalbar och relativt enkel att implementera, men det finns också ett antal nackdelar med tekniken som kunder borde vara uppmärksam på. I denna rapport är fokuseringen på hur villkoren och avtalen vid kontaktering med molnleverantörer ser ut, men fokus ligger också på att öka medvetenheten med riskerna vid kontraktering under en lång tidsperiod. Det finns fortfarande många frågetecken som behöver övervägas och analyseras när det gäller molntekniken. Inriktningen på denna rapport är därför kontrakten och designen av dessa ser ut och som leverantörerna oftast skriver ihop till sin egen fördel. Dessa leverantörsfördelar kommer att uppmärksammas i rapporten, dock är fördelarna med molntekniken lätta att upptäcka vid presentationer om tekniken, men kontrakten kan också innebära problem om beroendet på servicen är stor. För det är kontrakten leverantörerna hänvisar till om det skulle uppkomma fel på servicen. Exempelvis säger kontrakten att vid störningar på servicen kan maximalt 50 % av månadsbeloppen en kund betalar varje månad, återbetalas till kunden. Detta kan vid långvarigt störning innebära finansiella problem för kunden. Kontrakt-aspekterna integritet, prestanda och kontrakts ändringar är oftast till fördel för leverantören, men det finns även ytterligare aspekter att försöka förhandla sig till bättre villkor på. Dock finns det åtgärder kunder kan göra för att förbättra sitt kontrakt. Exempelvis kan företag arbeta tillsammans för att stärka inflytandet mot leverantören för att på det sättet kunna förhandla sig till bättre kontraktsdetaljer.

Sökord: Molntjänst, kontrakt, Service Level Agreement (SLA), kontraktering, Molnservice

Tack till:

Mentor/Handledare: Bengt J Nilsson, Malmö Högskola, Sverige

Examinator: Mia Persson, Malmö Högskola, Sverige

Intervju: Åke Jansson, Malmö Högskola, Sverige

Intervju: Andreas Helgegren, Adistics AB/ProspectEye, Malmö, Sverige

## **Abstract**

This report highlights the aspects for customers to be aware of before contracting with a cloud provider. Cloud technology is efficient, effective, scalable and easy to implement, but there are also drawbacks that customers or potential customers should know before contracting. The focus area in this report are the terms and agreements aspects when working with a cloud provider, but the report also highlights the risks with contracting with cloud providers in the long term. The focus is also on the design of the contracts that the providers want to design for their own winning. The report wants to make the reader aware of these pitfalls. There are several benefits with Cloud Computing and information about the technology is easy to find, but the information about the contracts are kept in the shadows and written in small letters by high paid lawyers. With maximum 50% payback of the monthly paid by the customer to the provider, if there is service disruption, the contracts can be an economical nightmare for the customers. With aspects such as privacy, performance and contract changes details that are in favor for the provider, are many aspects to consider when reading and negotiating about a contract. But there are things the customers can do to improve their contract. An example is that by working together with other companies when the procurement is underway, the leverage is strengthened against the providers to negotiate for better contract details.

Keyword: Cloud, Contract, Service Level Agreement (SLA), Outsourcing, Cloud-Service

Thanks to:

Mentor: Bengt J Nilsson, Malmö University, Sweden

Examiner: Mia Persson, Malmö University, Sweden

Interview: Åke Jansson, Malmö University, Sweden

Interview: Anderas Helgegren, Adistics/ProspectEye, Malmö, Sweden

# Innehållsförteckning

1. Introduktion.....	6
1.1 Bakgrund .....	6
1.2 Problemformulering.....	6
1.3 Syfte.....	6
1.4 Avgränsning .....	7
1.5 Definitionslista .....	7
2. Litteraturundersökning .....	8
2.1 Cloud Computing – Begreppsutredning.....	8
2.1.1 Definition .....	8
2.1.2 Vad är Cloud Computing?.....	8
2.1.3 Distributionsmodeller .....	9
2.1.4 Fördelar och nackdelar .....	11
2.2 Kontrakt .....	12
2.2.1 Dropbox.....	13
2.2.2 Amazon.....	13
2.2.3 Google.....	14
2.2.4 Microsoft.....	15
2.3 Risker med att kontraktera med en Cloud-leverantör.....	15
2.3.1 Integritet (Privacy).....	15
2.3.2 Avbrott.....	16
2.3.3 Mänskliga fel .....	17
2.3.4 Prestanda .....	17
2.3.5 Tredje part.....	18
2.3.6 Säkerhet .....	18
2.3.7 Övriga kontrakt klausuler.....	19
3. Metod.....	19
3.1 Kvalitativ data.....	19
3.2 Kvantitativ data .....	19
3.3 Frågeformulär .....	20
3.4 Intervju metodik .....	20
3.5 Alternativa metoder.....	20
3.6 Källkritik.....	21
4. Resultat .....	21
5. Diskussion .....	25

6. Fortsatt forskning .....	26
7. Referenser .....	28
7.1 Webbaserade källor.....	28
7.2 Publicerade källor .....	29
8. Bilagor .....	31
8.1 Åke Jansson, Malmö Högskola.....	31
8.2 Malmö Högskola & Office 365 .....	32
8.3 Andreas Hellegren .....	32
8.4 Kontrakt .....	34
8.4.1 Dropbox.....	34
8.4.2 Google.....	38
8.4.3 Microsoft.....	51
8.4.4 Amazon.....	55

# 1. Introduktion

## 1.1 Bakgrund

Uppfattningen kring att Cloud Computing i längden kommer slå ut klient-server teknologin har under de senaste åren ökat. Detta har skapat en hype-stämpel på Cloud-teknologin och fler personer och företag beslutar eller funderar på att flytta över data till extern aktör. Teknologin medför att datainnehav förvandlas till en servicetjänst som kunder betalar leverantören för. Regler och förutsättningar om hur denna service ska se ut skrivs in i kontrakten mellan kunden och leverantören och det är här problemen med teknologin börjar göra sig synliga. Leverantörerna skriver kontrakten till sin fördel och detta måste kunder eller potentiella kunder vara medveten om. Även Svenska försvarsmakten visar intresse för tekniken och ville i januari 2012 att studenter skulle hjälpa till att belysa ämnet ytterligare. De är intresserad hur de själv ska kunna använda tekniken och vilken data de kan lämna till en eventuell molnleverantör. Detta är bakgrunden till rapporten och eftersom Svenska försvarsmakten har visat intresse att möjligtvis bli kunder till en molnleverantör har vi valt att presentera och problematisera ämnet från ett kundperspektiv.

## 1.2 Problemformulering

Problemformuleringen för denna rapport handlar om problemen kring kontrakten mellan kund och leverantör inom molntjänster. Det handlar både om medvetenhet innan påskrift och även hur man kan förbättra sitt existerande kontrakt. Att implementera och börja arbeta med en molnleverantör är relativt enkelt och har låga startkostnader. Kunder behöver dock kontrollera och läsa igenom kontraktets alla delar för att förstå aspekterna kring integritet, avbrott, dataförlust, mänskliga fel, prestanda, tredjepart-inblandning, kontrakt ändringar och ekonomiska aspekter.

Målet med rapporten är lyfta fram och belysa problemen med kontraktering och samtidigt öka medvetenheten kring problemen som finns. Problem formuleringen för denna rapport är följande:

- Vilka risker bör kunder vara medveten om vid kontraktering med en molnleverantör?
- Hur kan kunder försöka förhandla sig till bättre kontrakt med sin leverantör?

## 1.3 Syfte

Denna rapport kan användas som ramverk för kunder som tittar på möjligheter att flytta data till extern part. Molnleverantörer attraherar nya kunder med löften om snabb implementering, skalbarhet, flexibilitet och att kunden inte betalar mer än vad de använder. De problem som finns med tekniken försöker företagen hålla dolda och framhäver istället de positiva aspekterna.

Syftet med denna rapport är inte att peka ut molnleverantörer eller tekniken på ett negativt sätt utan istället presentera fakta och data som visar på att tekniken fortfarande har brister. Tekniken har dock flertalet fördelar som är svåra att bortse

ifrån, och det är en av anledningarna till att tekniken har blivit så populär. Att sedan lyfta fram dessa problem och kunna analysera informationen som finns tillgänglig och på det sättet kunna komma fram till en bra lösning på de problem som existerar både för privatpersoner och för företag.

## 1.4 Avgränsning

Av anledning till begränsning av tid för denna rapportens färdigställande har det efter övervägning och rekommendationer från handledare bestämts att två intervjuer ska genomföras. Dessa intervjuer kommer utgöras av ett stort företag och ett litet, för att kunna påvisa om det finns några skillnader i företags förmåga att kunna förhandla sig till bättre kontrakt beroende på företagsstorlek. Båda dessa företag använder sig av molntekniken, dock på olika sätt. Mer detaljer kring detta finns läsa under Bilaga 8.1 och 8.3. En avgränsning är också gjord av tidsbrist för färdigställande att denna rapport enbart kommer behandla de största leverantörerna av molntjänster dvs.: Dropbox, Microsoft, Google och Amazon. En generalisering har också gjorts i tron på att mindre företag i stor mängd kopierar kontraktsdetaljer från de större leverantörerna för att därigenom kunna skydda sitt företag jämligt med de stora. Denna generalisering ligger också till grund för problematiken att kunna få tillgång till de mindre företagens kontrakt då kontraktsdetaljer kan ses som känslig information för mindre företag som de inte vill ska komma ut till allmänhet eller konkurrenter.

## 1.5 Definitionslista

**Adistics/ProspectEye:** Ett litet företag inom sektorn Business Intelligence (BI). De säljer ett säljstødsverktyg vars information hämtas och skickas med hjälp av molnteknik. Deras servrar är placerade hos en serviceleverantör. Deras säljstødsmodul är inriktad att fungera inom segmentet företag till företag (Business to Business, B2B). Adistics är ett av intervju-företagen i denna rapport.

**Cloud / Moln:** Se avsnitt 2.1

**Kund:** En kund till en leverantör av molntjänster som på något sätt använder sig av tjänster från denna leverantör.

**Datainspektionen:** Är en myndighet som har till uppgift att skydda människor från integritets problem vid hantering av personlig data.

**Malmö Högskola:** En högskola med 24'000 studenter och är baserad i södra delen av Sverige. Högskolan har 1400 anställda och har en stor variation av kurser och program i olika nivåer.

**PUL:** Person Uppgifts Lagen. Är en lag som skyddar människor mot personintrång och integritetskränkning i frågor om behandling av personlig data.

**Service Level Agreement (SLA):** Är en del av kontraktsdetaljerna vid en full kontraktering mellan en kund och en leverantör. Det är den kontraktsdel som säger vilken nivå på servicen kunden ska ta emot och kan förvänta sig.

**Serviceleverantör:** Kan också beskrivas som en molnleverantör och är ett annat ord för detta. En serviceleverantör tillhandahåller olika It-teknologier och i detta fall inom Molnteknologi.

**Tjänstekrediter:** En tjänstekredit är något en tjänsteleverantör kan bli tvungen att betala tillbaka till en kund vid bortfall av service. Detaljer kring detta och antalet krediter vid felaktigheter är överrenskomet av både kund och leverantör vid påskrift av kontraktet.

## 2. Litteraturundersökning

### 2.1 Cloud Computing – Begreppsutredning

Cloud Computing är en stor trend inom IT just nu. I denna del så kommer begreppet molnet eller Cloud Computing att redas ut och varför denna teknik har fått en sådan genomslagskraft.

#### 2.1.1 Definition

Definitionen för molntekniken är inte helt överrenskomet bland experterna. Detta beror på att tekniken fortfarande utvecklas och att begreppet innefattar ett område som samtidigt är väldigt omfattande. Att hitta en exakt definition på en sådan teknologi är därför svår. Olika experter har olika definitioner och detta är den Plummer (2009) tycker stämmer mest in på Cloud Computing:

*”A style of Computing where Scalable and elastic IT capabilities are provided as a service to multiple customers using Intern technologies”*

En annan definition som innefattar både en personlig definition och samtidigt sammanfattar en definition från Gartner presenterar Geelan (2009) som följande:

*”The way I understand it, “cloud computing” refers to the bigger picture...basically the broad concept of using the internet to allow people to access technology-enabled services. According to Gartner, those services must be 'massively scalable' to qualify as true 'cloud computing'. So according to that definition, every time I log into Facebook, or search for flights online, I am taking advantage of cloud computing.”*

#### 2.1.2 Vad är Cloud Computing?

Cloud Computing är som sagt inte tillfullo definierat och därför skiljer definitionen sig i vissa beskrivningar beroende på vart ifrån man samlar in informationen. Cloud Computing kan dock fastställas som ett koncept som har resurser placerat externt på en server park och är tillgängligt med Internet teknologi. Denna resurs är baserad på dator kraft, mjukvara, data tillgänglighet och lagringsutrymme. Det finns tre olika servicemodeller av Cloud Computing. (Mell & Grance 2011)

### IaaS

IaaS är en förkortning som står för: Infrastructure as a Service, och är en resurs som är helt eller delvis är placerad hos en extern leverantör. Leverantörerna av denna modell är ansvariga för driften, resursunderhåll och servicen till kunden.

Mängden resurs eller service som önskas av kunden är kontrollerat av leverantören och kunden betalar bara för vad de använder. Kunden kan också vid vilken tidpunkt som helst välja att minska eller öka sitt resurskrav och kan då sänka eller höja sina kostnader beroende på hur mycket resurser kunden vid tillfället behöver. Detta kallas att teknologin är skalbar.

## Paas

PaaS kan också kallas vid sitt fulla namn: Platform as a Service. Denna teknologimodell stödjer en hel dataplattform genom användning av internetteknologi. Servicen från modellen kan delas, lagras, utvecklas, byggas ut och hanteras genom molnteknologin. Ett exempel på denna modell är force.com, som är ett verktyg där kunden kan bygga sina egna applikationer och därigenom själv bygga sina egna affärsmoduler vilket gör denna modell flexibel.

## SaaS

Förkortningen står för Software as a Service och precis som namnet antyder så är det kortfattat mjukvara genom internet. Denna mjukvara levereras av en molnleverantör och är teknologin är också skalbar.

Dessa modeller är också som uttrycket Cloud Computing inte fullständigt definierat ännu men för att göra det lättare att förstå skillnaden mellan vanlig mjukvara och SaaS presenteras nedan en tabell med inspiration från Janssen & Joha (2010) som visar på skillnaderna på ett välordnat sätt.

<b>Egenskaper</b>	<b>Traditionell mjukvara</b>	<b>SaaS</b>
<b>Ägande</b>	Inköp av mjukvara	"Hyrning" av mjukvara utan ägandeskap
<b>Prismodell</b>	Direkt investering och kostnad för installation/implementering, inklusive licensinköp	Betala för användandet eller månadsbetalning
<b>IT funktioner</b>	Inköpt, installerar, utvecklar och underhåller deras egen mjukvara	Kontraktering, "Plug-in" och använd. Inget direkt behov av IT-kunskap och ingen oro över uppdateringar
<b>Expert hjälp</b>	Mjukvaraspecialister som underhåller och kontrollerar	Användarexpertis behövs

### 2.1.3 Distributionsmodeller

Enligt Nist (2011) så finns det dessutom fyra olika sorters distributionsmodeller inom Cloud Computing. För att kunna förstå tekniken fullständigt behövs en förklaring till dessa fyra modeller. Dessa modeller är Private Cloud, Public Cloud, Community Cloud och Hybrid Cloud.

## Private Cloud

Ett "privat moln" kännetecknas av att det verkar inom ett slutet nätverk, till exempel inom en organisation och körs oftast i infrastrukturen inom organisationen. Organisationen har även ansvaret att förvalta tekniken men kan också låta molnleverantören förvalta och sköta underhållet åt organisationen.

## Public Cloud

"Publikt moln" är en öppen service som tillhandahålls av serviceleverantörer. Detta är exempel på en modell som handlar mycket om lagring och service där kunden som oftast loggar in via en webbplats för att kunna komma åt sin data eller tjänst. Denna tjänst är öppen för alla, dock med undantag för en inloggningsfunktion för att skilja användarna från varandra.

## Community Cloud

Community Cloud kan beskrivas som en infrastruktur som kan styras av en tredje part. Det kan också i många fall styras även av en organisation som köper tjänsten. Community Cloud används, delas och integreras ofta av fler än en organisation, där vissa ansvarsområden är uppdelade i organisationen. Som exempel på ansvarsområden som kan vara delade: säkerhetsaspekter, order och inköp, företagsstrategier, uppdrag och produktion.

## Hybrid Cloud

Infrastrukturen i modellen Hybrid Cloud är en blandning av två eller flera av ovanstående servicemodeller. Blandningen kan vara i vilken ordning som helst mellan de tre olika molnmodellerna, Private Cloud, Public Cloud och Community Cloud. Alla modellerna behåller sina unika egenskaper men är sammankopplade genom lagerteknik (layers) som gör det informationsutbyte möjligt mellan de olika modellerna. För att få en bättre förståelse hur dessa modeller hänger samman så har jag utgått från Johnston's modell, Development Models of Cloud computing, se bild 1.

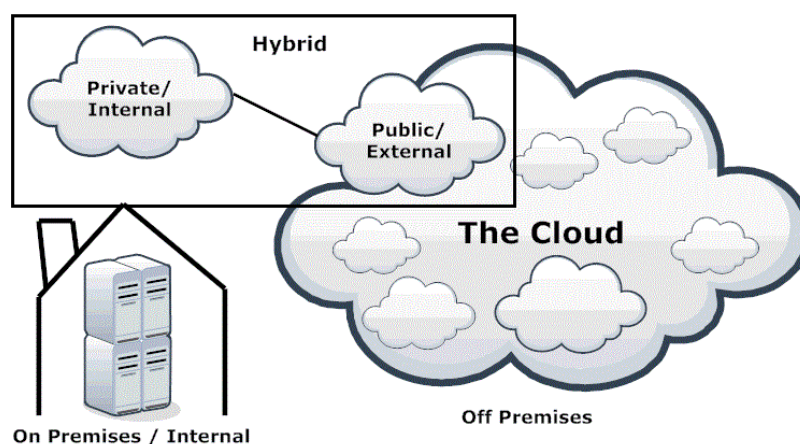


Bild 1, Cloud Computing Types, ursprungligen från Johnston (2010)

#### **2.1.4 Fördelar och nackdelar**

Det är en pågående och omstridd diskussion om fördelarna och nackdelarna med molntekniken. Man kan kort säga att experterna är oense i stort. Dock gjorde Janssen och Joha en sammanställande rapport om molntekniken 2011 som denna del av rapporten är baserad på.

##### **Fördelar**

Fördelarna med att arbeta med en molnleverantör och deras tjänster är att kunden inte generellt behöver kontrollera, installera eller underhålla deras mjukvara. Kunderna betalar molnleverantörerna för lagring och/eller tjänster av kundens egen data som dessa leverantörer ger kunden tillgång till. Fördelen med detta är att kunden själv inte behöver lika stor datorkraft i sina klientdatorer eller någon stor serverpark, dvs. hårdvaru-antalet för kunderna minskar drastiskt. När hårdvaru-antalet sjunker behövs inte i lika stor utsträckning människor med arbetsuppgifter att underhålla och uppdatera hårdvaran. Detta leder för företagen minskade kostnader i lön och minskad kostnad för att utbilda personal. Tekniken minskar även antalet inköp av hårdvara. Även minskade kostnader för personal som kräver högre lön eftersom de flesta som använder molntjänster är i allmänhet slutanvändare som inte behöver hög utbildning för att klara av systemen då också lönekraven på personalsidan minskar.

Att implementera en "in-house"-lösning är dyrare än att implementera en molntjänst. Stora implementeringsprojekt har också problem med att hålla projektplanen för tid och kostnad vilket leder till stora utgifter i implementeringsfasen vilket gör att projekten blir svårkalkylerade. Skillnad med molntekniken är att det oftast finns en fast kostnad för implementering och sedan en kostnad per användande, vilket gör att detta är en teknik som är lätt att kalkylera och genererar små kostnader vid införandet. Om kunder skulle se behov att behöva ytterligare lagringsutrymme eller tjänster så är det enbart ytterligare kostnader per användande, vilket också är lättkalkylerat. Molntekniken lämpar sig bra mot konkurrenter i hänseendet att det går snabbt att starta igång och lämpar sig bra mot nystartade företag eller företag med begränsade resurser.

##### **Nackdelar**

Nackdelar med molnteknik är omdebatterad, där leverantörerna inte ser några problem med det de själva säljer. Företag och organisationer som funderar på investera i tekniken bör vara medvetna om nackdelarna som dock finns med tekniken. Aspekten där företag eller organisationer som väljer en molnleverantör bör ta i beaktning är att om kundernas företag är inne i en expanderande fas, att det då finns tillräcklig med tjänster eller applikationer via leverantören för att tillgodose kundernas kommande behov. Eftersom kunder låses till en leverantör av servicen, när väl kontraktet är påskrivet, kan det vara problematiskt att byta leverantör. Det är tyvärr inte helt enkelt att bara flytta kundernas data till en annan leverantör. Vidare har Cloudteknologin inte heller i samma utsträckning som inhouse-systemen arbetat i samma utsträckning med "best of breed". Detta är ett begrepp som mer används av de större IT systemen som är det bästa systemet för

att lösa de problem kunderna har inom ett specifikt område och genom att arbeta på ett specifikt sätt effektivisera verksamheten. Detta är något som fortfarande saknas inom molntekniken.

Som nämntes i fördelaravsnittet så är molnteknik billig att investera i. Dock kan det visa sig att under en lång tidsperiod kan molnteknik visa sig mer kostsam vid vissa tidsperioder än ett inhouse-system. Bersin (2009) har skapat en modell för att visuellt visa hur kostnader mellan dessa två tekniker skiljer sig, se bild 2

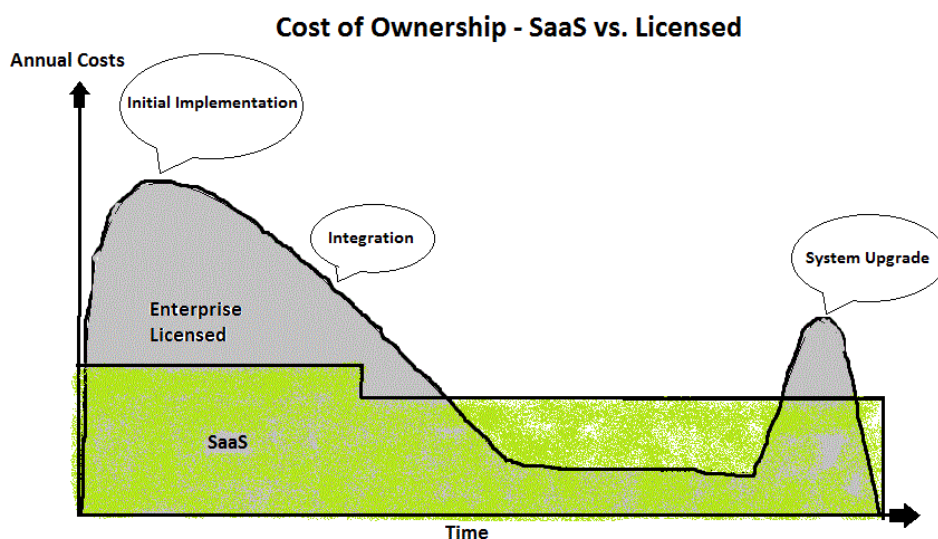


Bild 2, Cost of Ownership, Egenritad bild med inspiration av Bersin (2009).

En stor nackdel för kunder som ska kontraktera med molnleverantör är just själva kontraktet. Kontraktet mellan leverantören och kunden berättar hur tekniken ska fungera och vad kunden ska få från leverantören. Bryts detta kontrakt kan leverantören bli återbetalningsskyldig till kunden. Dock visar det sig när kontraktet noga läses igenom att dessa straffsummor är låga summor i sammanhanget. Detta är en aspekt av problematiken som finns i kontraktutformningen i de standardkontrakt som finns med de stora bolagen idag. I denna rapport kommer det nedan i mer ingående detaljer gå in på vad som egentligen står i kontrakten mellan molnleverantören och kunden och vad kunder bör veta om innan ett kontrakt skrivs under.

## 2.2 Kontrakt

Kontrakten mellan molnleverantören och kunden är en överenskommelse över hur servicen mellan aktörerna ska fungera och hur hög servicenivån ska vara. Kontrakten ska vara till fördel för båda aktörer då de behöver kunna referera till kontrakt detaljerna ifall något skulle inträffa med servicen. Detta gäller från båda aktörernas håll, då kunden vill veta att den får sin service och vet att dennes data är placerad säkert. Vidare vill också molnleverantören skydda sin verksamhet och inte skriva in för höga straffkostnader för utebliven service som skadar leverantörens verksamhet ekonomiskt. Kontraktet ska vara till fördel för alla parter i bästa fall. Dock skriver oftast molnleverantörerna sina egna kontrakt i förväg eftersom de har duktiga jurister som kontrollerar så inga detaljer kan tydas på ett,

från deras håll felaktigt sätt, och som oftast gagnar leverantörerna mer än kunderna.

Enligt Bradshaw, Millard och Walden (2011) så har bara 10 % av molnanvändare förhandlat sig till ett bättre kontrakt med sin leverantör. Dock visar inte studien om kunderna som blev tillfrågade ville ändra något i sitt kontrakt eller om det var leverantörerna som inte godkände ändringar som kunden ville göra. Dock är 10 % av användare av molnteknik som har kunnat ändra sitt kontrakt en låg siffra. Kontraktet är till för att skydda kunden om det uppstår fel på servicen från leverantören och att kunden då kan påvisa kontraktsbrytning, vilket ska leda till ersättning. Utebliven service från leverantörer kan ha stor ekonomisk effekt på kunders ekonomiska intäkter. Vance (2010) skriver att 1-2 % av intäkterna kan gå förlorade vid utebliven service. För ett mindre företag med begränsade resurser kan dessa procent vara viktiga för företaget fortsatta existens. Vidare säger Vance att leverantörerna oftast är duktiga på att skylla orsaker till stop i servicen på kunden eller att hitta orsaker som kontraktet inte täcker, vilket leder till att de kan hävda att de inte är deras fel och därmed kan de inte bli återbetalningsskyldiga.

### **2.2.1 Dropbox**

Dropbox är en av de stora leverantörerna av lagringsutrymme via molnteknik. Kunden placerar data hos Dropbox för att kunna göra data tillgänglig överallt där kunden har internetuppkoppling. Dropbox köper i sin tur lagringsutrymme via Amazons molntjänst, vilket i korta ordalag menas att kunden har placerat data med Dropbox hos Amazon. Men kontraktet som gäller, är mellan kunden och Dropbox och inkluderar inte Amazon alls.

I Dropbox Service Terms (2010), kontraktsdetaljer kan man läsa att Dropbox bland annat inte delar ut någon som helst data lagrad med dem till någon brottsförebyggande verksamhet. Med detta menas att om Dropbox blev ombedd av polisen att öppna ett speciellt konto så skulle detta inte bli av, just för att de har skrivit med detta i kontraktet. Vidare skriver Dropbox att det maximala belopp som en kund kan få tillbaka som ersättning vid avbrott i servicen eller förlorad data är 20 amerikanska dollar, vilket i skrivande stund är ungefär 140 svenska kronor. Deras kontrakt säger också att "*We may stop, suspend, or modify the services at any time without prior notice to you*", vilket inger en otrygghet hos kunden att när som helst kan Dropbox ändra i servicen som du som kund skrivit under på och i vissa fall betalar för.

### **2.2.2 Amazon**

Amazon S3 är en av de två största molnleverantörerna som finns på marknaden. De arbetar också i samarbete med Dropbox som togs upp under rubriken 2.2.1. I kontraktet Amazon Terms and Agreements (2012), skriver Amazon att de placerar in sina kunders data i regioner vilket är de geografiska platser där data är placerad. Dessa regioner är uppdelade enligt Amazon i Europa, USA och Asien, där kunderna kan välja om de vill placera dina data på en specifik geografiskt område. Detta kostar kunden en högre avgift men kan då bli garanterad att kundens data bara blir placerad inom en av dessa regioner. Detta är något som Amazon lovar. Kunden har även rätt att flytta över dennes data till en annan region om den önskar.

Amazon säljer två olika sorters service nivåer som de har döpt till Standard och RRS (Reduced Redundancy Storage). RRS nivån är mindre redundant än standard nivån men är också mindre kostsam för kunden. Väljer kunden att placera sin data via RSS så placeras data på flera enheter, vilket ger 400 gånger mer pålitlighet än en vanlig hårddisk. Enligt Amazon så är systemet utformat för att kunna hantera förlust av data från två olika fysiska platser med deras Standard modell. Vidare lovar Amazon att kunden kommer att ha 99,9999% pålitlighet och 99,99% tillgänglig service på sina kunders data. Vidare utformades Standard tjänsten för att upprätthålla en förlust av data i två anläggningarna samtidigt.

Amazon anger vidare i sitt kontrakt att de: "*will use commercially reasonable efforts to make Amazon S3 available with a monthly uptime percentage of at least 99.9% during any monthly billing cycle.*" De har vidare anfört att om tjänsten inte uppfyller tillgänglighetsnivån så kommer kunden att få "Service Krediter". Detta är krediter som kunderna bara kan använda för att betala nästa månads räkning. Procentsatsen beräknas på den totala kostnad som kunden betalar per månad till leverantören. Återbetalningen i Amazons standard avtal ser ut som följande:

- 99,9% - 99 % = 10 % av totala månadskostnaden som betalas av kunden
- Mindre än 99 % = 25 % av totala månadskostnaden som betalas av kunden

Så om kunden betalar 1000 dollar för service från Amazon blir högsta tillåtna avgiften att få tillbaka 250 kronor, som kan användas för att betala den andra månadens räkning för servicen.

Tillgängligheten beräknas och loggas för varje felmeddelande med intervallet fem minuter i en månad. Med innebär att om du som kund gör 20 förfrågningar och två förfrågningar genereras som fel, blir drifttillgängligheten 90 %.

Dock har molnleverantörerna vissa undantag för fel som inte räknas som fel. Dessa fel är tillagda i Amazons kontrakt och dessa faktorer inkluderar de fel som ligger utanför Amazon rimliga kontroll som: force majeure, internetåtkomst, tredjepart-inblandning och kundens utrustning.

### **2.2.3 Google**

Googles kontrakt detaljer är väldigt snarlika Amazons kontrakt innehållsmässigt. Enligt Google kontrakt (2012) i jämförelse med Amazons, så har Google bara en servicenivå vilket gör det lättare för kunden att förstå avtalet. Googles kontrakt innehåller bland annat att de kan göra förändringar i avtalet för tjänsten innan kunderna blir underrättade, men att kunden i efter hand kommer att bli informerad om förändringen eller de nya förutsättningarna. Google säger också i sitt kontrakt att de vill att kunden ska: "*use commercially reasonable efforts to resolve support issues before escalation them to Google.*" Dessutom har Google en detalj i en av deras klausuler, under rubriken "Required Disclosure", som säger: "*Each party disclose the other party's Confidential Information when required by law but only after it, if legally permissible: (a) uses commercially reasonable efforts to notify the other party; an (b) gives the other party the change to challenge the disclosure.*" Detta innebär att Google har rätt dela ut privat data, som är lagrad i deras servrar, till en

brottsbekämpande myndighet utan att behöva meddela detta till kunden i förväg. Precis som Amazon, har Google samma servicekredit nivå, om/när 100 % drifttillgänglighet av deras tjänst inte uppnås. Det som står skrivet i kontraktet är:

- 99,9 % - 99 % = 10 % tillbaka på avgiftsbelagd tjänst
- Mindre än 99 % = 25 % tillbaka på avgiftsbelagd tjänst.

#### **2.2.4 Microsoft**

Microsoft standard kontrakt är även det, väldigt likt de andra kontrakten som finns beskrivna ovan, dock finns det vissa skillnader. Enligt Microsofts Terms and Agreements (2012), måste kunden kontakta Microsofts kundtjänst efter en incident eller fel på servicen och man måste som kund gå igenom de rätta kanalerna för att kunna få rätt till återbetalning. Villkoren för detta förklaras i kontraktet och vad kunden ska göra när en incident hänt. Återbetalningssumman från Microsoft kan aldrig överstiga det belopp som kunden betalar under en månad för tjänsten av Microsoft. Detta betyder att om ett företag betalar 4500 kr för en molntjänst, kan maximalt återbetalningsbelopp för förlorad service bli 4500 kr och inte mer. Här nedan visas nivån av det belopp som återbetalning blir vid utebliven service. Det är samma nivåer som de andra stora leverantörerna har:

- 99,9 % - 99 % = 10 % tillbaka på tjänsten debiteras (betalas månadsvis av kunderna 100 %)
- Mindre än 99 % = 25 - 100 % (betalas varje månad av de kunder 100 %)

Vidare säger Bott (2011), att användare av molnservice från Microsoft bara kan tillåtas att skicka 500 e-post-meddelanden från samma konto med Microsoft tjänst Exchange, som är en av modulerna i Microsoft 365. Detta anges i det allmänna avtalet mellan Microsoft 365 och kunden.

### **2.3 Risker med att kontraktera med en Cloud-leverantör**

Jansen och Joha (2011) hävdar att de största nackdelarna de har hittat i sin undersökning av molnleverantörskontrakt är inkräktande på privatlivet, förlorad kontroll över datautbyte och möjligheten att förlora viktig data. Många av de intervjuade företagen i deras rapport ansåg att de förlorar kontrollen på deras data om den lagras någon annanstans än i en inhouse-lösning. De intervjuade företagen nämner också i denna rapport att de känner bristande säkerhet och ökad osäkerhet kring molntechniken, vilket också visar på problem vid kontraktering med molnleverantörer.

#### **2.3.1 Integritet (Privacy)**

Enligt Eurobarometer (2008) visade 64 % av EU-medborgarna oro när organisationer hanterar medborgarnas personuppgifter och de känner oro för att datan inte hanteras korrekt. Svenskarna visade störst oro hur organisationer hanterar integriteten med deras data. Hela 75 % av svenskarna i undersökningen säger sig vara bekymrade över sin integritet i detta sammanhang.

I en artikel från Baker (2011), säger Theo Bosboom att Safe Harbor avtalet är ett föråldrat avtal. Han fortsätter: *"I'm afraid that safe harbor has very little value anymore, since it came out that it might be possible that U.S. companies that offer to*

*keep data in a European cloud are still obliged to allow the U.S. government access to these data on the basis of the Patriot Act". Vidare säger även Theo Bosboom att: "Europeans would be better to keep their data in Europe. If a European contract partner for a European cloud solution offers the guarantee that data stays within the European Union, which is without a doubt the best choice, legally."*

Apple har även i deras kontrakt till deras tjänst Icloud, som är en molntjänst, har uppfört deras integritet-ställning, vilket kunderna måste godkänna för att kunna nyttja tjänsten: *"You acknowledge and agree that Apple may, without liability to you, access, use, preserve and/or disclose your Account information and Content to law enforcement authorities, government officials, and/or a third party, as Apple believes is reasonably necessary or appropriate, if legally required to do so or if we have a good faith belief that such access, use, disclosure, or preservation is reasonably necessary to: (a) comply with legal process or request; (b) enforce this Agreement, including investigation of any potential violation thereof; (c) detect, prevent or otherwise address security, fraud or technical issues; or (d) protect the rights, property or safety of Apple, its users, a third party, or the public as required or permitted by law."*

Med denna klausul säger Apple att om de hade gjort en fullständig kryptering av data som lagras på Apple så hade inte vara möjligt att granska data som det är nu. Dock är bara data transporten krypterad. Det innebär att Apple kan komma åt kundernas filer, och läsa innehållet på dessa utan problem, för all data är lagrat utan kryptering och är läsbart för de anställda på Apple och för en eventuell inkräktare.

### **2.3.1.1 PUL och Salems kommun**

Salems kommun är en kommun i Sverige som flyttade en del av kommunens data utanför Sverige med molnteknik via Google och Dropbox. Detta granskades av Datainspektionen och enligt Datainspektionen (2011) visade resultatet på granskningen att upphandlingen inte kunde godkännas av Data Inspektionen, eftersom den bröt mot den svenska PUL (Personuppgiftslagen). Undersökningen visade att Salems kommun på flera olika sätt bröt mot integritetsaspekter genom att placera datauppgifter om svenska medborgare i ett annat land än Sverige. Det största problemet, som Datainspektionen såg var att e-postsystem som Salem använder inte krypterar när data skickas och att de länder som datan lagras i inte var med i Safe Harbor-avtalet.

### **2.3.2 Avbrott**

Om tjänsten från kundernas molnleverantör går ner kan det ha en stor effekt för kunders företag. Tjänsten kommer i 99 % av fallen komma tillbaka, men vad händer om kunden vid nergången förlorar data? Även en stor storm kan svepa över molnleverantörer lagringsanläggningar eller en massiv översvämning kan förekomma. Hur skyddas kunder och företags data från det, som använder sig av molntjänster? I en undersökning gjord av Williams (2010), hittade han att de senaste 2 åren har 23 rapporter om avbrott rapporterats inom området Cloud Computing. Bakom dessa siffror står Microsoft för fyra avbrott, Salesforce hade två, Google står för 12 och Amazon hade fem avbrott. Williams fortsätter och nämner ett

exempel där Googles e-post tjänst Gmail hade ett avbrott på sammanhängande 30 timmar under 2008. Google har fortfarande ingen aning om hur många människor som påverkades av avbrottet. Lärdomen av detta är enligt Williams att kunder alltid bör ha säkerhetskopior av e-post för att undvika detta problem. Ett annat exempel är Microsoft Sidekick som var nere i 6 dagar under 2009. Microsofts kunder kunde inte komma åt sin adressbok, kalender och andra viktiga tjänster under dessa dagar. Incidenten skapade en viss dataförlust, men de flesta av Microsofts kunder fick tillslut all data tillbaka. Avbrottet berodde på, enligt en talesman på Microsoft, ett systemfel i kärnan på databasen och på deras säkerhetskopiering (backup). Detta avbrott resulterade i att Microsoft installerade en backup-process för deras databas för att minimera att denna incident inträffar igen. Lärdom av detta är enligt Williams att kunder bör kontrollera deras Disaster Recovery Policy med sin molnleverantör. Författaren rekommenderar också att kunder säkerhetskopierar över deras data på mer än ett ställe.

Att förlora kontrollen på sin egen data kan vara en av många aspekter som blir verklighet med avtal med ett molnleverantör. Enligt Greene (2011), förlorade Amazon en liten del data i ett avbrott under 2011. Exakt 0,07 procent data lagrad i Amazons östra region försvann och datan kunde inte återställas till deras kunder. I detta avbrott blev en kunds skador så grova att deras företags webbplats var nere i 72 timmar. Detta kan bli stora förluster för företag som inte har några backup webbplatser eller liknande.

### **2.3.3 Mänskliga fel**

Mänskliga fel är en viktig aspekt att ta i beaktning vid kontraktering med en molnleverantör. Exempelvis vid underhåll på datacenter, har den människor och inte bara maskiner stora och många beslut att fatta. Molnleverantörer försöker oftast framhäva sitt företag som en enhet, men som vi vet består denna enhet av många människor och människor kan göra misstag. Dessa misstag kan kosta molnleverantören stora pengar men också drabba kundens företag hårt. När människor arbetar med databaser och datorkodning är det lätt att göra något fel, även om människorna har gjort samma sak tusen gånger eller om det inte var just en persons mening. Att glömma en symbol i stort kodsträng kan ha en enorm inverkan på tjänsten och att göra fel är dock ett normalt mänskligt beteende. Detta är förståeligt men är en sak att fundera på när ett annat företag styr tillgången till andra företags filer.

Enligt Kern (2011), hade Amazon en incident inom detta område med sin SaaS Cloud den 21 april 2011. Enligt Kern, skiftade en anställd på Amazon, felaktigt redundant data medan en uppgradering på företaget var igång. Detta gjorde att SaaS tjänsten gick ner, vilket ledde till avbrott i tjänsten där datatrafiken inte fungerade. Avbrottet pågick i mer än 2 dagar där Amazons datacenter i North Carolina var drabbat värst, vilket ledde till att dessa kunder som hade sin data placerad där blev drabbade.

### **2.3.4 Prestanda**

Hur snabbt kan kunder få tillgång till sin data från sin leverantör? Enligt Google, Microsoft, Dropbox och Amazons avtal och SLA, omnämns prestanda som begrepp

inte alls i något av kontrakten. Kunder kan inte beviljas några prestandaparametrar från sina leverantörer i de standardavtal som de stora leverantörerna presenterar på sina hemsidor. Att detta låter konstigt kan förstärkas genom att titta på ett exempel från en annan bransch: En kund köper en mobiltelefon från en mobiloperatör och registrera sig för ett kontrakt som varar i två år. Efter kontraktet är undertecknat märker kunden, att hastigheten på 3G-nätet inte alls är i den hastigheten att det går att använda 3G-nätet på telefonen på ett gynnsamt sätt. Vem skulle idag köpa en abonnemang med en mobiloperatör och inte veta vilken prestanda 3G-nätet höll? Detta är exakt likadant som är fallet med molnleverantörerna, där leverantörerna inte utlovar några som helst prestandanivåer alls på sina tjänster. Pettey (2011), säger så här i hans rapport om ämnet: *“Despite the significant business-criticality of certain cloud applications, Gartner analysts have seen numerous contracts that have no uptime or performance-service-level guarantees at all, or that are only provided as a changeable URL link. Cloud contract negotiators must be aware of the performance service levels required and ensure that they are documented contractually, ideally with penalties, if the performance standards are not achieved.”*

### **2.3.5 Tredje part**

Om och när kunden får ett felmeddelande från leverantörens service och rapporterar detta till leverantören, måste kunden vara helt säker på att det inte är något fel med deras nätverk mellan kunden och leverantören. Detta är viktigt för i alla standardavtal med leverantörerna står det att om inte tjänsten är tillgänglig och leverantören kan visa att det fanns en tredje part som orsakade felet kan leverantören påvisa att de inte längre är ansvarig för felet. Detta kan innebära att det kan bli verkligen svårt som kund att kunna bevisa att det inte är kundens fel att det är fel eller problem med tjänsten kunden betalar för. Detta kan även innebära att det kan bli ett problem att kunna påvisa att det just är fel på leverantörens tjänst och inte någonting annat.

### **2.3.6 Säkerhet**

Säkerhet kring Cloud Computing har mycket likheter med IT-säkerhet i allmänhet där illasinnade personer försöker införskaffa sig andra personers data eller information för att omsätta detta till pengar eller för att skaffa sig ett större rykte i undre världen. Enligt Chen, Paxson och Katz (2010), som delar upp de antal säkerhetsincidenter som inträffat inom Cloud Computing som nya och gamla incidenter. De gamla incidenterna kan kopplas likaväl till traditionella webbapplikations- och datalagrings- problem men tekniken är likaså använd inom Cloud Computing. Dessa ”gamla” incidenter som förekommer inom många områden inom IT är lösenordsfiskning, driftstopp, dataförlust, brister i lösenord och botnet-attacker. Vidare skriver författarna att Amazon drabbades av en botnet-attack i slutet på 2009 och är en av de första incidenterna som drabbar en stor molnleverantör.

En av de nya incidenterna som författarna har hittat förklara författarna på detta sätt: *“Because cloud computing introduces a shared resource environment, unexpected side channels (passively observing information) and covert channels (actively sending data) can arise.”* Med detta menar författarna att genom fördelen

att mycket information är delad så finns också säkerhetsmässigt nackdelar med detta. Är en illasinnad person väl inne i systemet så kan personen ifråga, beroende på hur molnsystemet är uppbyggt, komma åt information från flera "moln" via olika kanaler i systemet. Dock menar också Chen, Paxson och Katz att molnleverantörerna oftast använder sig av den senaste säkerhetstekniken, såkallad "best of practice".

### **2.3.7 Övriga kontrakt klausuler**

Enligt en undersökning som utförts av Bradshaw, Millard och Walden (2011), det mest oroande kontraktsfrågan som kunder bör vara medvetna om är att leverantörerna kan när de vill, utan att i förväg informera kunden, kan ändra i avtalsdetaljerna i det kontrakt som är undertecknat av de båda parterna. Enligt Googles användarvillkor (2012), hittar man följande klausul: "*Google may make commercially reasonable changes to the Services, from time to time. If Google makes a material change to the Services, Google will inform Customer, provided that Customer has subscribed with Google to be informed about such change.*" I vilka andra affärsavtal kan en leverantör, av produkter eller tjänster, ändra detaljerna i ett kontrakt mellan två affärspartners? Som sig bör är fallet ofta att avtalet är fast och kan inte ändras, för både leverantör eller kund. Detta används som ett skydd för båda parterna som både vet vad de båda har undertecknat.

## **3. Metod**

Merparten av datainsamlingen är genomförd genom att forska på nätet på IT-relaterade webbplatser med fokus på Cloud Computing och kontraktering. Det finns begränsat antal publicerade böcker i ämnet, men mycket relevant information har hittas från undersökningar av studenter och yrkesverksamma på olika plattformar för rapporter, till exempel Google Scholar.

För att kunna förstå förfarandet med avtalen hos Cloud-leverantörer har vi samlat data från två olika intervjuer. Dessa intervjuer utgörs av en stor organisation med många användare och ett litet Business2Business företag. Detta för att försöka se på skillnader mellan olika storlekar på företag har betydelse för företagets förmåga att kunna förhandla sig ett bättre kontrakt, med vikt på riskerna som är belysta i detta arbete.

### **3.1 Kvalitativ data**

Den kvalitativa datan i denna rapport har samlats in vid två besöksintervjuer. Den kvalitativa datan kommer att generera, kombinerat med den kvantitativa datan, ett resultat på problemformuleringen som har angetts under rubrik 1.2. Kvalitativ data kan också kallas primärdata. Att samla in data med en kvalitativ metod är bra för mer få mer djup i sin undersökning och för att enklare påvisa kopplingar i forskningen, enligt Bryman (2011).

### **3.2 Kvantitativ data**

Den kvantitativa datan i denna rapport har samlats in av fakta och uttalanden från både experter inom området Cloud Computing och från akademiska artiklar inom området. Genom att söka efter data från Google.com, Google Scholar och ACM

Digital Library hittade vi tillförlitliga uttalanden och fakta att använda i rapporten. Dessa data kommer att kombineras med den kvalitativa datan för att försöka besvara definition av problemet som är presenterat under rubrik 1.2. Enligt Bryman (2011), fokuserar denna metod att samla in uppgifter på ord istället för siffror, och innebörden av de ord som talas.

### **3.3 Frågeformulär**

Frågorna som ställdes till intervjuobjekten arbetades fram efter att undersökningen inom området var definierat och informationen om Cloud Computing hade införskaffats. Även var problemformuleringen framarbetad och klar innan frågorna togs fram för att kunna få med alla aspekter från intervjuobjekten, för att kunna på så bra sätt som möjligt kunna besvara problemformuleringen.

För att frågorna skulle passa till just intervjuobjektet med namn på företag och deras leverantör var frågeformuläret tvungna ändras innan intervjun. Enligt Andersen och Schwenke (2009) bör frågorna i intervjun rikta sig mot din problemformulering och att i förväg ta till vara på den information som företagen tillhandahåller på exempelvis deras hemsida så att inte tid går till spillo i intervjutillfället. Dessa aspekter tillämpades när frågorna till intervjuerna arbetades fram.

Eftersom arbetet i första skedet var skrivit på det engelska språket har intervjuerna blivit översatta från svenska till engelska och sedan till svenska igen. Detta är gjord efter författarens bästa förmåga. Även har intervjuobjekten godkänt båda översättningarna på frågorna de besvarade.

### **3.4 Intervju metodik**

I de båda intervjuerna som gjordes i denna rapport har samma typ av intervju genomförts. Intervjun med Åke Jansson på Malmö högskola utfördes vid ett fysiskt möte och är mer känd som en besöksintervju. Vi hade först kontakt med Åke via E-mail i förväg och han visste vilket ämne vi ville behandla och vad vi skulle intervjua honom om. Enligt Eriksson och Wiedersheim-Paul (2006), är denna typ av intervju bra för uppföljningsfrågor vid svar som intervjupersonen behöver få mer förklarat och man kan använda intervjuobjektets kroppsspråk för att förse intervjupersonen med ytterligare information om svaren på frågorna. Intervjun var planerad av Åke och vi träffades den 27 mars 2012 kl 01:00 och Åke Jansson kontor på Orkanen rumsnummer E127.

Den andra intervjun genomfördes med Andreas Helgesson vid Adistics och gjordes med samma intervjufrågor som användes under intervjun med Åke Jansson. Först E-mailade vi Andreas Helgegren frågorna klockan 11.42 den 2 april 2012, men utfallet på Helgegrens svar var inte tillfredställande, och därför frågades han om han kunde undvara ett möte istället. Mötet genomfördes 25 april 2012 kl 17.00 på Adistics AB huvudkontor på Stortorget 19 i Malmö.

### **3.5 Alternativa metoder**

Alternativa metoder skulle kunnat användas inom området som rapporten behandlar. Exempelvis skulle en mer fokuserad inriktning på problemet

behandlats, där vi alternativt skulle kunna försöka framställa ett mindre datorprogram där prestandan i olika molnlösningar mäts för att få fram ett resultat av hastigheten på dataöverföringen. Detta program skulle kunna skicka en pingförfrågan till diverse mottagare och på så sätt kunna mäta hastigheten på överföringen. Ett annat tekniskt tillvägagångssätt skulle kunna vara att i tidigt skede kontakta ett IT-säkerhetsföretag och tillsammans med företaget göra kontrollerade White-hat attacker på de olika molnlösningarna för att kunna få fram ett mätvärde av hur säkra dessa lösningar är och jämföra dessa data med vad som står i molnleverantörernas kontrakt.

### **3.6 Källkritik**

Pågrund av det snabbt växande området Cloud Computing och att begreppet har utvecklats väldigt snabbt så har forskningen i ämnet naturligtvis inte kunnat följa i samma hastighet. Därför är det svårt att enbart samla data från akademisk forskning till denna rapport. Vi var tvungna att samla in data till litteraturöversikten från experter inom området som kanske inte har varit 100 % korrekt akademiskt verifierat. Vi har tagit denna aspekt i beaktande vid insamlandet av dessa data. Vid insamlingen av den empiriska datan under intervjuerna finns också en aspekt att tänka på att betrakta kroppsspråket på intervjuobjektet och vad intervjuobjektet säger. När vi märkte något när intervjuobjektets ord och kroppsspråk inte överrensstämde, från ett icke-professionellt perspektiv, försökte vi att ställa följdfrågor för att verkligen gå till botten med frågan vi ville ha besvarad. Vi försökte vårt bästa att vara objektiv under intervjun och vi försökte i så stor utsträckning möjlig att ställa frågorna på samma sätt i båda intervjuerna.

Dessutom ville vi samla in data från både ett stort företag och en liten för att få mer och rätt dynamik i resultatet och se om det finns några skillnader mellan hur molnleverantörerna besvarar förfrågningar på ändringar på kontraktsdetaljer när ett liten jämfört med ett stort företag vill kontraktera med en leverantör.

## **4. Resultat**

Rapporten ligger till grund för den problemformulering som presenterades av den Svenska Försvarsmakten till Malmö Högskola. De hade varit intresserade av tekniken men ville ändå veta mer. Själva upphandlingen med en leverantör är för försvarsmakten det mest problematiska faktorn och som det oftast också är för den allmänna kunden. Även om det är mer en säkerhetsfråga för försvaret, än för den allmänna kunden behöver oroa sig för är dock själva tjänsten och frågorna företagen behöver beakta runt upphandlingen oftast liknande. Aspekterna i denna rapport ska ses som en utgångspunkt för varje företag, där riskerna och aspekterna att behandla kring upphandlingen kan skilja sig från företag till företag. Problemformuleringen för denna rapport är angiven nedan:

- Vilka risker bör kunder vara medveten om vid kontraktering med en molnleverantör?

- Hur kan kunder försöka förhandla sig till bättre kontrakt med sin leverantör?

För att besvara denna problemställning kommer vi att använda både data från litteraturundersökningen och från den empirisk datan (som finns att betrakta i sin helhet i bilagorna 8.1 och 8.3) och kombinera dessa två för att generera ett svar. När man går igenom informationen kan vi se ett mönster i de data som visar på fem aspekter som kunden bör ha i åtanke eller tänka på vid kontraktering med en molnleverantör. Dessa aspekter innefattar:

- Integritet
- Avbrott
- Prestanda
- Avtal-förändring
- Ekonomisk

Integritet är ett av de största orosmomenten kunder känner när de överväger att använda tjänster från en molnleverantör. Detta framgår av såväl Jansen och Joha (2011) och Eurobarometern (2008), där de kan påvisa problem i områdena runt integritet och molnteknik. I intervjun med Åke Jansson (2012) nämnde han sin oro om integritetsproblem med molntekniken. Denna oro skulle vi säga är problem som flera personer inom området har uppmärksammat. I intervjun med Andreas Helgegren (2012), nämnde han inte någon oro över samma aspekt, mest på grund av att hans företag inte hanterat någon data som kan skada personers integritet. Även säger Åke Jansson (2012), att det är viktigt vart man som företag lagrar sin data. Detta ska enligt Jansson placeras i Europa på grund av incidenten med Data Inspektionen och Salems kommun som han använder som referenspunkt. Eftersom Jansson arbetar för det statligt styrda universitetet behöver han följa ett större regelverk och fler lagar för att kunna lagra juridiskt data enligt PUL. Jansson i jämförelse med Helgegren ser också problem med safe harbor-avtalet och den amerikanska Patriot Act. Jansson ser Safe Harbour avtalet som inte lika starkt som den amerikanska Patriot Act avtalet. Han visar också en oro för att Patriot Act kan spela ut Safe Harbour avtalet, om de båda avtalen skulle stå mot varandra. Denna aspekt håller även Baker (2011), med om. Han menar att USA Patriot Act "tar bort" de juridiska aspekterna av Safe Harbour-avtalet, som då blir ett direkt hot mot den personliga integriteten även när person eller företag skulle använda Safe Harbour-avtalet. Baker rekommenderar också att försöka hålla data som lagrade i Europa utan någon koppling till ett amerikanskt-baserat företag är det bästa alternativet, om företaget hanterar känslig information och integriteten värderas som viktig aspekt. Åke Jansson ser också exakt denna lösning på samma problem med USA Patriot Act. Jansson sa så här under intervjun med honom: "Om du håller dina data i Europa, med ett icke amerikanskt företag, kommer du att bli bra, ur min synvinkel".

Avbrott i servicen från sin molnleverantör är något som en kund måste också ha i åtanke vid kontrakterande. Denna aspekt kan vara väldigt avgörande om tjänsten kunden betalar för är viktigt för att kunden ska göra affärer. Kan kunden inte göra affärer förlorar kunden inkomst på att servicen från molnleverantören ligger nere. I

denna rapport har det presenterats ett antal fall leveransen av tjänsten från olika leverantörer har misslyckats. Enligt Williams (2010), har 23 rapporter om avbrott har rapporterats under de 2 åren mellan 2008 till 2010. Greene (2011) säger även att Amazon har förlorat data som de inte kunde återskapa. Avbrott i molntekniken inträffar, och även vid vissa incidenter försvinner data vid avbrotten. Ingen av de intervjuade hade någon erfarenhet av något avbrott i sin tjänst, men de var medvetna om problemet. Åke Jansson och Andreas Hellegren hade tidigare använt andra tjänster som inte riktigt tillfredsställde deras behov, men de hade inte upplevt avbrott på någon sin tjänst. Andreas Hellegren anser att tillgänglighet på servicen som den viktigaste aspekten för sitt företag när de använder molntjänster. Detta beror på det höga beroendet Adistics har på sin tjänst för att kunna ge sina kunder den service de i sin tur säljer. Ingen service är lika med låg eller ingen inkomst alls.

Ingen av de stora leverantörernas standardavtal nämner inget om prestanda i någon av deras SLA. Enligt Pettey (2011), som också har studerat kontrakten, ser bristen på prestationsnivån i kontrakt till något som behöver tas upp vid förhandlingarna om kontrakt detaljerna mellan kunden och leverantören. I intervjun med Åke Jansson, på frågan om prestanda, säger han att Malmö högskola inte har något verktyg för att mäta prestanda från leverantören. Han säger dock att frågan har tagits upp men inte behandlats än. Vidare säger han att det inte funnits några klagomål på denna aspekt så att de inte ansett sig lägga ner tid eller pengar på att mäta prestanda. Andreas Hellegren säger i intervjun att de gör egna externa mätningar till deras tracker för att mäta prestanda och han anser att kvaliteten på tjänsten från sin leverantör är tillfredsställande för deras behov. Eftersom kunderna till Adistics är beroende på hastigheten från trackern är det viktigt att hastigheten och prestanda är konstant hög, säger Hellegren.

En annan aspekt att tänka på är att molnleverantören, när de vill, kan ändra kontrakt detaljer och ibland även utan att meddela kunden. Detta är de kontraktsdetaljer kunden och leverantören har kommit överrens om vid godkännandet av det som står i kontrakten. Denna aspekt är en av de mest oroväckande problem man kan läsa i kontrakten och något som ska beaktas när kunder gör sin förhandling med leverantören om kontraktsdetaljerna. (Bradshaw, Millard och Walden, 2011) Denna kontraktsdetalj kan också hittas i stora leverantörernas officiella avtal där till exempel Google uppger att användaren kommer att meddelas om kontraktet ändras, men bara om användaren själv har godkänt att ta emot sådan information.

En annan aspekt är att molnleverantörerna marknadsför molntekniken som det billigaste alternativet för att kunna lagra data, och detta faktum är sant. På grund av att tekniken är tidseffektiv att implementera och att integrera så är tekniken ett lågkostnadsalternativ. (Bersin 2009). Dock är molntekniken fortfarande inte en perfekt lösning, ur en ekonomisk synvinkel. Om kunden har sin inkomst baserad på tjänsten från leverantören, kan det visa sig vara en ekonomisk mardröm. Som anges i avtalet mellan kunder och Microsoft (2012), Google (2012) och Amazon (2012), är den maximala återbetalningen för avbrott i tjänsten på 50 % av den månadskostnad som betalas av kunden. Åke Jansson visar också oro över denna

aspekt under intervjun och han ser ett problem i att universitetet inte betalar något för tjänsten och har därför ingen inflytande på leverantören. Enligt Vance (2010) kan företag lätt förlora 1-2% av intäkterna om det blir något avbrott i tjänsten som köps. Denna procentsats kan tyckas lite men kan vara mycket för ett företag med begränsad likviditet.

För att kunna förhandla fram ett bättre avtal med hänsyn till de aspekter som beskrivs ovan kan kunden arbeta med dessa fyra aspekter:

- Arbeta tillsammans med andra kunder
- Öka straffavgifter på avbrott och prestanda
- Placera din data i Europa
- Arbeta med en andra leverantör och/eller behålla lokal backup

För att kunna lagra känslig och personlig data i molnet, studerade Åke Jansson rapporten från Data Inspektionen om Salems kommun och tvingade de, med hjälp från de andra universitetet, Microsoft till att förhandla om att lagra deras data enbart i Europa. Anledningen till att universitetet kunde göra denna förändring i avtalet, tror Åke Jansson är att de var tre universitet som arbetar tillsammans med samma intresse och behov, vilket ökade hävstångskraften mot Microsoft. För att kunna använda Microsofts molntechnik, var universitetet tvungna att kunna lagra sin data i Europa på grund av den svenska PUL. Andreas Helgegren å andra sidan, vet var deras servrar är lokaliserade och är mestadels intresserad av hastigheten och tillförlitligheten av tjänsten och lägger inte stor vikt vid integritets detaljer i kontraktet. Detta för att den information de transporterar genom servicen hanterar inte några personliga uppgifter. De använder tjänsten för allmän information om företaget och deras telefonnummer.

Att försöka förhandla fram ett bättre Recovery Policy med leverantören, tror vi kommer bli svårt. Denna aspekt skyddar leverantören måste vara med för att kunna skydda leverantören annars skulle företaget riskera att placeras i konkurs om tjänsten är nere eller data förloras. Med detta faktum känt så tror vi att det är svårt att förhandla sig till ett bättre kontrakt i denna aspekt med någon leverantör på marknaden. Enligt Williams (2010), är det bättre och lättare att lagra sin data lokalt eller hos någon annan leverantör, för att kunna hantera denna risk bättre.

För att kunna veta att servicen levereras med den prestanda som kunden kräver och behöver så behöver kunden sätta press på leverantörens prestanda klausul i kontraktet. Som visat i denna rapport så är prestandanivåerna ickeexisterande i de stora leverantörernas avtal. Pettay (2011) tycker att kunder ska försöka förhandla sig till att leverantörerna kontrakt ska innefatta prestandanivåer och dessa nivåer bör vara i nivå med kraven från kunderna. Pettay menar också att kunderna ska ge ett förslag till att inkludera straffavgiftsnivåer för leverantören då överrenskommande prestandanivå bryts eller om nivåerna är lägre än överrenskommet i avtalet, vilket också bör ses som ett brott av avtalet. Pettay anser att dessa straffnivåer kommer att göra att leverantören arbetar hårdare för att hålla prestandanivån på eller över den överenskomna nivån. Enligt intervjuerna har

Andreas Hellegren mer oro över prestandan på servicen på grund av prestandan som Adistics kunder förväntar sig.

Ur en ekonomisk aspekt så är det svårt att hitta hängstångskraft i kontraktet på leverantörerna. Priserna på tjänsterna sjunker, vilket gör att hävstångskraften på servicen för kunderna blir nästan obefintlig. Om kunden använder en tjänst som är nästan gratis, är det svårt att hålla leverantörerna ansvariga för någonting. Å andra sidan, om kunderna är ekonomiskt beroende att tjänsten från molnleverantör fungerar, borde kunden skaffa sig en backup lokalt eller ha en annan leverantör att kunna luta sig tillbaka på vid avbrott.

## 5. Diskussion

I den ekonomiska aspekten av Cloud Computing, är vi inte riktigt överens med Cost of Ownership modellen i avsnitt: 2.1.3.2. Modellen visar vad som händer vid företagets tillväxt eller vid utveckling av verksamheten. Om företaget växer och måste investera i fler tjänster från en molnleverantör är "hyran" är inte konstant utan ökar då, vilket inte visas i modellen. Den är konstant om företaget inte växer, men varje företag vill växa i något avseende. En annan sak är att om modellen skulle visa kostnaden under en längre tid efter systemuppgraderingen, så skulle inhouse-lösning i längden bli billigare eller lika kostsam än molnlösningen. Om alla intäkter går genom användning av molnleverantörens tjänster det skulle detta kunna vara sant.

En annan aspekt som handlar om den ekonomiska aspekten är att om den ekonomiska förlusten inte är större per månad än 25 % av vad kunden betalar för tjänsten till leverantören, är det ekonomiskt motiverat om riskanalysen kunden gör visar att det kommer att ske ett eller flera avbrott på servicen?

Enligt Bradshaw, Millard och Walden (2011) har 10 % av kunderna förhandlat sig till ett bättre och säkrare SLA mellan sig själva och leverantörerna. Denna rapport är mer än ett år gammalt och 10 % är inte mycket när man talar om kontraktering. Ett ekonomisk, juridisk eller producerande avtal mellan två parter kan förhandlas om, men det är inte så enkelt att förhandla om service kontrakt. Åke Jansson kan, enligt honom själv, ändra avtalet mellan Malmö högskola och Microsoft på grund av universitetet gick tillsammans med två andra universitet och kunde därigenom göra större påtryckningar på Microsoft. Dock var universiteten tvungna att göra förändringarna kring att deras data endast skulle lagras i Europa, annars var en flytt till molnleverantör inte möjlig. Universitetet var såklart rädda att om de inte kunde ändra avtalet, skulle samma sak hända med dem som med Salems kommun. Företagen måste vara noga med att uppfylla lagarna kring PUL för att kunna vara säkra på att det fungerar med leverantörernas kontrakt. Annars går inte personuppgifter från Sverige att lagras utanför Sveriges gränser enligt Data Inspektionen och PUL om inte leverantörerna kan lova kunderna specifik lokaliseringsplats av datan.

Under intervjuerna kände vi att i jämförelse med de två intervjuobjekten att det fanns en olik syn på Cloud Computing. En aspekt på detta kan vara skillnaden i

ålder mellan Åke Jansson och Andreas Hellegren. Vi tror att yngre människor har lättare att lita på teknik än äldre generellt. Riera (2011) säger så här om ålder och teknik: "Furthermore, youth feels much more comfortable in the current era of information technology and is much more likely to adapt to new technologies and to promote innovation in this field." Detta stödjer också dessa tankar.

Den andra aspekten i denna rapport om kontraktering är att många kunder känner att de tappar kontrollen på egen data då den "lämnas iväg" till extern part. Jansen och Joha (2011) tror att detta har en stor betydelse för kunderna. Enligt författarna är det mer en känsla av otrygghet än den verkliga aspekten att lämna ifrån sig data och är mer kopplad till rädslan för avbrott på servicen. Det är också en känsla av att släppa iväg data, där kunderna inte känner att de inte längre har kontroll, vilket ökar oron hos kunder eller blivande kunder till molnleverantörer.

Det är markant skillnad mellan Åke Janssons och Andreas Hellegrens syn på prestanda. För ett företag är det verkligen viktigt att kunna få tillräckligt hög prestanda för att kunderna till det egna företaget ska vara nöjda. Som kund vill du inte betala för något som är tänkt att vara en tidsbesparande säljverktyg och som visar sig vara ett långsam och ineffektiv molnbaserat verktyg. Åke Jansson ser inte vikten i hastighet på deras tjänst på samma sätt, kanske på grund av ett att det E-mail system de inte känner att de behöver ha en viss prestandanivå på, eftersom trafiken är väldigt kontrollerad och informationen skickas enbart på användarens begäran.

Vi tror att avtalet mellan kunden och leverantören kommer att spela en viktig roll att tänka på vid kontraktering med en molnleverantör. Eftersom utvecklingen i affärsområdet ökar, hoppas vi att det förs en utveckling också i kontrakten mellan de två parterna. Utvecklingen kräver dock en högre medvetenhet om att detta är ett problem i samhället och detta får man genom att läsa igenom det avtal som ligger framför kunden, förhandla med leverantörerna och sedan ställa högre krav än det görs idag. Eftersom mer och mer data placeras i molnet borde också starkare tillgängligheten utlovas och att detta sköts bättre av leverantörerna.

## **6. Fortsatt forskning**

Forskningen i ämnet är enligt vår mening oändliga och i just detta område inte djup. Men under denna forskning har vi funnit några områden som har fångat vårt intresse, men har utanför vårt fokusområde för denna rapport. Dessa områden är presenterade nedanför här och är de viktigaste frågorna eller områden vi fann mest intressant under den här rapporten. Vi hoppas att rapporten kan leda till vidare forskning i ämnet.

- Är en Cloud Computing-lösning mer lönsamt för ett företag i längden än en inhouse-lösning?
- En mer djupgående forskning om US Patriot Act och Safe Harbour och hur de används och hur de interagerar med varandra.

- Riskanalysering med ekonomisk vinning vid kontraktering med en molnleverantör. Hur stor risk är det och vad kan det ekonomiska utfallet bli vid avbrott i servicen?

## 7. Referenser

### 7.1 Webbaserade källor

Amazon. 2012. "Amazon Simple Storage Service, Amazon S3", Hämtad den 8 Februari 2012 från: <http://aws.amazon.com/s3/>

Apple, 2012, "iCloud Terms and Conditions", Hämtad den 4 April 2012 från: <http://www.apple.com/legal/icloud/en/terms.html>

Baker, J., 2011, "European distrust of US data security creates market for local Cloud service", Hämtad den 2 April 2012 från: <http://www.cfoworld.com/operations/26526/european-distrust-us-data-security-creates-market-local-cloud-service>

Bersin J. 2009, "How SaaS-y is your HR software vendor? What does SaaS mean to you?", Bersin Research, 29 Augusti 2009, Hämtad den 29 Februari 2012 från: <http://joshbersin.com/2009/08/29/how-saas-y-is-your-hr-software-vendor-what-does-saas-mean-to-you/>

Bott, E. 2011 "Small businesses, beware the Office 365 fine print", ZDNet, 21 Oktober 2011, Hämtad den 19 April 2012 från: <http://www.zdnet.com/blog/bott/small-businesses-beware-the-office-365-fine-print/4151>

Datainspektionen, 2011 "Tillsyn enligt personuppgiftslagen (1998:204) – Salems kommun", 28 September 2011, Hämtad den 20 April 2012 från: <http://www.datainspektionen.se/Documents/beslut/2011-09-30-salems-kommun.pdf>

Dropbox, 2012, "Service Terms 2012" Hämtad den 16 Februari 2012 från: <http://www.dropbox.com/terms>

Geelan J. 2009, "Twenty-one experts define cloud computing", Cloud Expo, 24 Januari 2009, Hämtad den 11 Mars 2012 från: <http://cloudcomputing.sys-con.com/node/612375>

Google, 2012, "Google Apps for Business (Online) Agreement", Google Inc., Hämtad den 16 Februari 2012 från: [http://www.google.com/apps/intl/en/terms/premier\\_terms.html](http://www.google.com/apps/intl/en/terms/premier_terms.html)

Greene, A. 2011, "Amazon: Some data lost in cloud outage is not recoverable", TechFlash, 28 April 2011, Hämtad den 23 April 2012 från: <http://www.techflash.com/seattle/2011/04/Amazon-says-some-data-lost-in-cloud.html>

Johnston S. 2010, "Development Models of Cloud Computing", It Cloud NIBM blog, 3 November 2010, Hämtad den 23 Februari 2012 från: [http://itcloudnibm.blogspot.com/2010\\_11\\_01\\_archive.html](http://itcloudnibm.blogspot.com/2010_11_01_archive.html)

Kern, J., 2011, "Amazon Apologizes, Cites Human Error in Cloud Interruption",

Information Management, 29 April, 2011, Hämtad den 27 Mars 2012 från:  
[http://www.information-management.com/news/cloud\\_SaaS\\_data\\_center\\_downtime\\_storage\\_Amazon-10020215-1.html](http://www.information-management.com/news/cloud_SaaS_data_center_downtime_storage_Amazon-10020215-1.html)

Microsoft, 2012, "Service-Nivå-Avtal" Hämtad den 22 Mars 2012 från:  
<http://www.windowsazure.com/sv-se/support/sla/>

Ni, R. 2008, "The Significant Potential Impact on IT Procurement and Vendor Management as Cloud Computing Matures", Gartner Research, Hämtad den 28 Februari 2012 från: <http://www.gartner.com/DisplayDocument?id=695307>

Petty, C., 2011, "Gartner Highlights IT procurement Best Practices to Reduce Risk in Cloud Contracts", 19 Maj 2011, Hämtad den 23 April 2012 från:  
<http://www.gartner.com/it/page.jsp?id=1689914>

Plummer, D., 2009, "Experts define Cloud Computing: Can we get a little definition in our definitions", 27 Januari 2009, Hämtad den 15 Mars 2012 från:  
[http://blogs.gartner.com/daryl\\_plummer/2009/01/27/experts-define-cloud-computing-can-we-get-a-little-definition-in-our-definitions/](http://blogs.gartner.com/daryl_plummer/2009/01/27/experts-define-cloud-computing-can-we-get-a-little-definition-in-our-definitions/)

Riera, I., 2011, "Trust in Young People" New Europe Post, 27 November 2011, Hämtad den 2 Maj 2012 från: <http://www.neurope.eu/blog/trust-young-people>

Subashini, S. & Kavitha, V., 2010, "A Survey on security issues in service delivery models of cloud computing", 3 Mars 2010, Hämtad den 15 Mars 2012 från:  
<http://www.sciencedirect.com/science/article/pii/S1084804510001281>

Vance J. 2010, "Top 10 reasons cloud computing deployments fail", Datamation, 26 Juli 2010, Hämtad den 11 Mars 2012 från:  
[http://itmanagement.earthweb.com/netsys/article.php/11075\\_3894891\\_1/Top-10-Reasons-Cloud-Computing-Deployments-Fail.htm](http://itmanagement.earthweb.com/netsys/article.php/11075_3894891_1/Top-10-Reasons-Cloud-Computing-Deployments-Fail.htm)

Williams A. 2010 "Top 5 Cloud Outages of the past two years: Lessons Learned", readwriteweb.com, 1 Februari 2010, Hämtad den 12 Mars 2012 från:  
<http://www.readwriteweb.com/cloud/2010/02/top-5-cloud-outages-of-the-pas.php>

## **7.2 Publicerade källor**

Andersen, E. & Schwenke, E., 2009, "Projektarbete – En vägledning för studenter", Studentlitteratur.

Bradshaw, S., Millard, C. & Walden, I., 2011, "The Terms They Are A-Changin'...Watching Cloud Contracts Take Shape". URL:  
[http://www.brookings.edu/~media/Files/rc/papers/2011/03\\_cloud\\_computing\\_contracts/03\\_cloud\\_computing\\_contracts.pdf](http://www.brookings.edu/~media/Files/rc/papers/2011/03_cloud_computing_contracts/03_cloud_computing_contracts.pdf)

Bryman, A., 2011, Samhällsvetenskapliga metoder. Sverige: Liber AB.

Chen Y., Paxson V., Katz R., 2010, "What's New About Cloud Computing Security?". Sida 3-4, URL:

[http://www.utdallas.edu/~mxk055100/courses/cloud11f\\_files/what-is-new-in-cloud-security.pdf](http://www.utdallas.edu/~mxk055100/courses/cloud11f_files/what-is-new-in-cloud-security.pdf)

Eriksson, L. T. & Wiedersheim-Paul, F., 2006, "Att Utreda, Forska och Rapportera", Liber, Sida 98-103.

Eurobarometer, Gallup, 2008 "Data Protection in the European Union", Hämtad den 4 April 2012, Sida 5-6, URL:

[http://ec.europa.eu/public\\_opinion/flash/fl\\_225\\_en.pdf](http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf)

Jansen M. & Joha A., 2011, "Challenges for Adopting Cloud-Based Software as a Service (SaaS) in the Public Sector".

Mell P. & Grance T., 2011, "The NIST Definition of Cloud Computing", Publication of National Institute of Standards and Technology.

## 8. Bilagor

Dessa är bilagorna från intervjuerna med Åke Jansson på Malmö högskola och Andreas Helgesson från Adistics AB. Intervjuerna är godkända av de intervjuade personerna efteråt.

### 8.1 Åke Jansson, Malmö Högskola

1. Varför måste ni placera Malmö Högskolas mailsystem i molnet?

Vi hade problem med gammal IT hårdvara och mjukvara. Vi använde ett gammalt katalogsystem som heter Novell som vi tyckte inte hade utvecklingsmöjligheterna för att kunna hantera all den nya teknik som vi behövde. Vi hade en mycket dålig driftsäkerhet med en kombination av stigande antal användare på systemet. Vi underhöll även ett ägt spamfilter som tog mycket kunskap och arbetstimmar för att hålla uppdaterad.

En annan aspekt var såklart pengar, som vi behövde för att hålla systemet igång och plus att det kräver personal. I november 2011 flyttade vi hela Malmö högskola personal till Microsoft Exchange.

2. Har ni undersökt andra leverantörer då Microsoft? (Varför har ni inte registrerat med dem?)

Nej, inte riktigt. Vi hade en diskussion om att välja Google eller Microsoft, men på grund av Campus kontraktet mellan högskolan och Microsoft Office så kände vi att det skulle vara bäst att ha en leverantör för alla program. Dessutom är Microsoft en av världens ledande leverantörer och vi är bekväma med att använda deras produkter.

3. Vilken typ av ett moln är det?

Tjänsten heter Microsoft 365 och är en SaaS-lösning för Cloud baserade tjänster. All data lagras i Europa enligt avtalet, antingen i Holland eller i Irland.

4. Kunde ni förhandla eller ändra något i avtalet med Microsoft? Hur svarade de på er eventuella förfrågan?

Malmö högskola, med hjälp av Göteborgs universitet och Linköpings universitet, gick ihop tillsammans och begärde en ändring i avtalet om PUL (Person Uppgifts Lagen). Detta var en central fråga att lösa, för om inte förhandlingen gick igenom så skulle hela "Lagra personuppgifter i ett annat land" inte kunde genomförts enligt Svenska Datainspektionens regler om att flytta personuppgifter utomlands.

5. Finns det någon aspekt i kontraktet som du skulle vilja göra bättre?

Om jag bara kunde välja, skulle jag ta bort "Safe Harbour"-avtalet, vilket gör det lättare för USA att komma åt filer som lagras med ett amerikanskt företag. Jag vet att de behöver för att få ett domstolsbeslut för att kunna komma åt data men Safe Harbour och den amerikanska Patriot Act är fortfarande en aspekt som skulle kunna vara bättre ur integritetssynsätt. Om du placerar din data i Europa, med ett icke amerikanskt företag, kommer det att vara bättre, från min synvinkel. Eftersom

vi på högskolan inte betalar något för att använda Microsoft 360 kan vi inte räkna med någon återbetalning vid driftstopp. Om systemet kraschar vi inte får någon ersättning från Microsoft.

6. Har ni haft något avbrott på tjänsten?

Nej, inte ännu. Vi har inte upplevt någon driftstopp alls på tjänsten. Eleverna är väldigt bra på att berätta när något inte fungerar och vi har inte fått någon indikation om tjänsten är nere.

7. Om Ja på fråga 6, har du använda Microsoft standard för Felrapportering? (Hur fungerade det?)

Inget svar.

8. Mäter du prestanda från leverantören? Varför inte?

Nej, för tillfället gör vi inte det. Du kan be om rapporter från Microsoft om prestanda, men vi har inte gjort det. Vi har talat om att installera ett verktyg för att läsa trafiken hastigheten från Microsoft, men vi har inte tagit tanken längre än så. Vi anser att tjänsten fungerar väl, och mycket få klagomål har rapporterats. Så vi har inte riktigt haft någon bra anledning att göra det. Men ja, vi har pratat om det.

## 8.2 Malmö Högskola & Office 365

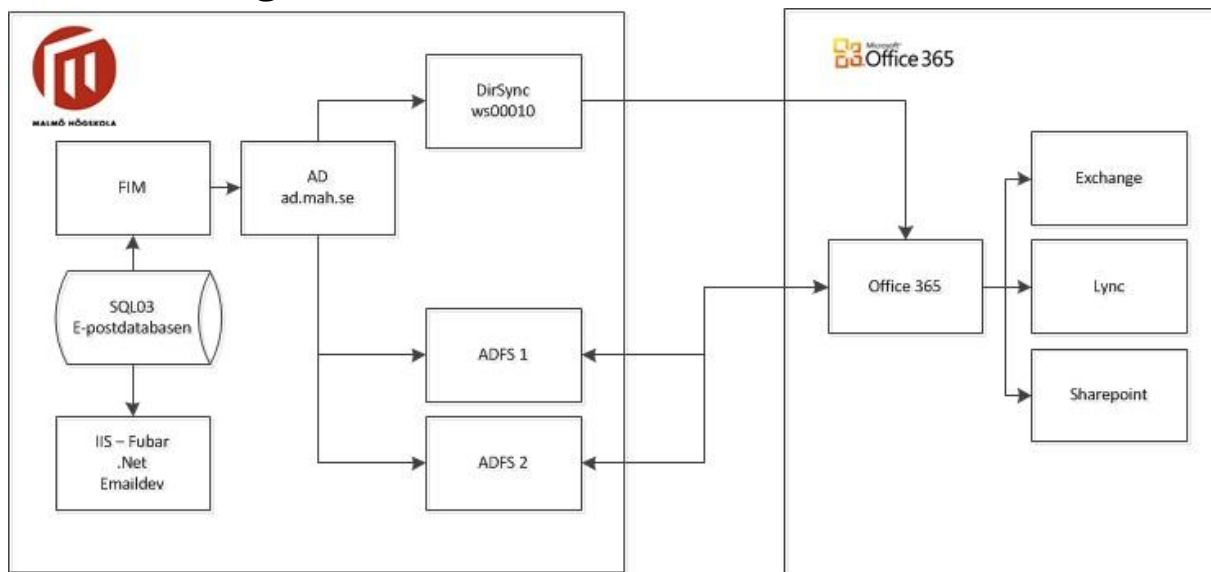


Bild 3, Malmö högskolas samverkningskarta med Microsoft Office 365.

## 8.3 Andreas Helgeregren

1. Varför kände ni behovet av att outsourca?

Eftersom vi använder en tracker baserat program måste vi vara säkra på att våra servrar ger 100 % drifttillgänglighet. Detta krav är verkligen svårt att övervaka själv, och kräver mycket tid. Kostnaden för att driva en server som denna lösning, tror vi är billigare att lägga ut än att göra backup och underhåll själv.

2. Har du forskning gäller andra tjänsteleverantörer då IT Gården? (Om Nej, varför du inte inloggad med dem?)

IT Gården är placerad geografiskt bra för oss, så vi lätt kan resa fram och tillbaka om det visar sig vissa problem med serverna eller tjänster. Innan dess hyrde vi Virtual PC speglar från Ipeer.com. Detta var inte fungerar tillfredsställande bra eftersom serverna inte har tillräckligt drifttid för att kunna driva vår tracker. Men vi fortfarande använder de virtuella serverna, men för flera icke kritiskt arbete.

3. Vilken typ av tjänst är det ni för närvarande köper?

Vi köper serverutrymme. Vi köpte serverna oss själva och installerat vår egen programvara, och vi köper tillgång service och underhåll av IT Gården.

4. Kunde ni förhandla eller ändra något i avtalet eller SLA med IT Gården? Hur svarade de på din eventuella förfrågan?

Pågrund av IT Gårdens goda rykte om deras tjänster, såg vi inget behov av att förhandla någon av de kontrakterade detaljerna. Sitt goda rykte och bra service var orsaken till varför vi valde dem. Så du kan säga att vi köpte affären utan att tveka.

5. Hur bra är ert avtal med IT Gården enligt dig från en skala 0-10? Hur bra täcker IT-säkerhet, integritet och tillgänglighet?

Vi tror att IT Gården är en av de bästa svenska leverantörerna av molntjänster. De täcker våra krav som en leverantör i enlighet med säkerhet, integritet och aspekter tillgänglighet. Vi känner oss trygga med sina tjänster och det stöd vi får från dem är alltid riktigt bra.

6. Om du kunde ändra någon kontraktsdetalj med IT Gården, vilken skulle ändra och varför?

För vårt syfte så passar IT Gården oss perfekt. Jag kan inte komma på någon detalj som vi skulle vilja ändra i vårt avtal med IT Gården. Eftersom vi är tvungna från våra kunder att ha 100 % tillgänglighet, känner vi oss trygga med valet av IT Gården. De får oss att sova gott varje natt.

7. Vilka är de tre viktigaste aspekterna, när man går igenom kontraktet med leverantören, enligt dig?

Med service vi använder de viktigaste aspekterna är för oss: tillgänglighet, kostnad och säkerhet. Detta är de viktigaste sakerna för oss, men dessa aspekter beror mycket på vilken typ av programvara du är har och använder.

8. Har du haft någon avbrott av tjänster från din leverantör?

Jag tror inte att vi har haft något avbrott sedan vi flyttade till IT Gården. Inte vad jag kan minnas i alla fall. Detta var ett av våra kriterier för att flytta till en annan leverantör. Vi anser att IT Gården är en pålitlig och säker leverantör som passar oss bra.

9. Mäter du prestanda från leverantören? (Om inte, varför inte? Om ja, hur?)

Vi mäter vår tracker-hastighet varje timme från ett externt ping till trackern. Detta görs automatiskt och denna ping bör vara under 0.03 sekunder att vi ska kunna få den hastighet på vår programvara som vi behöver. Om hastigheten går upp över 0.03 sekunder kommer vi att bli varnad via e-post. Vi följer också tillgänglighet på våra servrar med pingdom.com, men detta görs manuellt och efter behov.

## **8.4 Kontrakt**

Nedan är kontrakten från Dropbox, Amazon, Google och Microsoft tillagda till denna rapport som bilagor.

### **8.4.1 Dropbox**

Last Modified: March 26, 2012

Thank you for using Dropbox! These terms of service (the “**Terms**”) govern your access to and use of Dropbox (“**we**” or “**our**”) websites and services (the “**Services**”), so please carefully read them before using the Services.

By using the Services you agree to be bound by these Terms. If you are using the Services on behalf of an organization, you are agreeing to these Terms for that organization and promising that you have the authority to bind that organization to these terms. In that case, “you” and “your” will refer to that organization.

You may use the Services only in compliance with these Terms. You may use the Services only if you have the power to form a contract with Dropbox and are not barred under any applicable laws from doing so. The Services may continue to change over time as we refine and add more features. We may stop, suspend, or modify the Services at any time without prior notice to you. We may also remove any content from our Services at our discretion.

#### Your Stuff & Your Privacy

By using our Services you provide us with information, files, and folders that you submit to Dropbox (together, “your stuff”). You retain full ownership to your stuff. We don’t claim any ownership to any of it. These Terms do not grant us any rights to your stuff or intellectual property except for the limited rights that are needed to run the Services, as explained below.

We may need your permission to do things you ask us to do with your stuff, for example, hosting your files, or sharing them at your direction. This includes product features visible to you, for example, image thumbnails or document previews. It also includes design choices we make to technically administer our Services, for example, how we redundantly backup data to keep it safe. You give us the permissions we need to do those things solely to provide the Services. This permission also extends to trusted third parties we work with to provide the Services, for example Amazon, which provides our storage space (again, only to provide the Services).

To be clear, aside from the rare exceptions we identify in our Privacy Policy, no matter how the Services change, we won't share your content with others, including law enforcement, for any purpose unless you direct us to. How we collect and use your information generally is also explained in our Privacy Policy.

You are solely responsible for your conduct, the content of your files and folders, and your communications with others while using the Services. For example, it's your responsibility to ensure that you have the rights or permission needed to comply with these Terms.

We may choose to review public content for compliance with our community guidelines, but you acknowledge that Dropbox has no obligation to monitor any information on the Services. We are not responsible for the accuracy, completeness, appropriateness, or legality of files, user posts, or any other information you may be able to access using the Services.

### Sharing Your Stuff

The Services provide features that allow you to share your stuff with others or to make it public. There are many things that users may do with that stuff (for example, copy it, modify it, re-share it). Please consider carefully what you choose to share or make public. Dropbox has no responsibility for that activity.

### Your Responsibilities

Files and other content in the Services may be protected by intellectual property rights of others. Please do not copy, upload, download, or share files unless you have the right to do so. You, not Dropbox, will be fully responsible and liable for what you copy, share, upload, download or otherwise use while using the Services. You must not upload spyware or any other malicious software to the Service.

You, and not Dropbox, are responsible for maintaining and protecting all of your stuff. Dropbox will not be liable for any loss or corruption of your stuff, or for any costs or expenses associated with backing up or restoring any of your stuff.

If your contact information, or other information related to your account, changes, you must notify us promptly and keep your information current. The Services are not intended for use by you if you are under 13 years of age. By agreeing to these Terms, you are representing to us that you are over 13.

### Account Security

You are responsible for safeguarding the password that you use to access the Services and you agree not to disclose your password to any third party. You are responsible for any activity using your account, whether or not you authorized that activity. You should immediately notify Dropbox of any unauthorized use of your account. You acknowledge that if you wish to protect your transmission of data or files to Dropbox, it is your responsibility to use a secure encrypted connection to communicate with the Services.

## Software and Updates

Some use of our Service requires you to download a client software package (“Software”). Dropbox hereby grants you a limited, nonexclusive, nontransferable, revocable license to use the Software, solely to access the Services. Your license to use the Software is automatically revoked if you violate these Terms in a manner that implicates our intellectual property rights. We hereby reserve all rights not expressly granted in these Terms. You must not reverse engineer or decompile the Software, nor attempt to do so, nor assist anyone else to do so. Our Services may update the Software on your device automatically when a new version is available. Our pause syncing feature pauses syncing of your files, but may not cease all data transfer, so you should exit the desktop client if you’d like to stop data transfer.

## Dropbox Property and Feedback

These terms do not grant you any right, title, or interest in the Services, Software, or the content in the Services. While we appreciate it when users send us feedback, please be aware that we may use any feedback, comments, or suggestions you send us or post in our forums without any obligation to you. The Software and other technology we use to provide the Services are protected by copyright, trademark, and other laws of both the United States and foreign countries. These Terms do not grant you any rights to use the Dropbox trademarks, logos, domain names, or other brand features.

## Acceptable Use Policy

You will not, and will not attempt to, misuse the Services, and will use the Services only in a manner consistent with the Dropbox Acceptable Use Policy.

## Copyright

Dropbox respects others’ intellectual property and asks that you do too. We will respond to notices of alleged copyright infringement if they comply with the law and are properly provided to us. Such notices should be reported using our DMCA Process. We reserve the right to delete or disable content alleged to be infringing and to terminate repeat infringers. Our designated agent for notice of alleged copyright infringement on the Services is:

### Copyright Agent

Dropbox, Inc.

185 Berry St. Ste. 400

San Francisco, CA 94107

[copyright@dropbox.com](mailto:copyright@dropbox.com)

## Other Content

The Services may contain links to third-party websites or resources. Dropbox does not endorse and is not responsible or liable for their availability, accuracy, the related content, products, or services. You are solely responsible for your use of any such websites or resources. Also, if we provide you with any software under an

open source license, there may be provisions in those licenses that expressly conflict with these Terms, in which case the open source provisions will apply.

#### Termination

Though we'd much rather you stay, you can stop using our Services any time. We reserve the right to suspend or end the Services at any time, with or without cause, and with or without notice. For example, we may suspend or terminate your use if you are not complying with these Terms, or use the Services in any way that would cause us legal liability or disrupt others' use of the Services. If we suspend or terminate your use, we will try to let you know in advance and help you retrieve data, though there may be some cases (for example, repeatedly or flagrantly violating these Terms, a court order, or danger to other users) where we may suspend immediately.

#### Dropbox is Available "AS-IS"

Though we want to provide a great service, there are certain things about the service we can't promise. For example, THE SERVICES AND SOFTWARE ARE PROVIDED "AS IS", AT YOUR OWN RISK, WITHOUT EXPRESS OR IMPLIED WARRANTY OR CONDITION OF ANY KIND. WE ALSO DISCLAIM ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. (We are not shouting- it's just that these disclaimers are really important, so we want to highlight them). Dropbox will have no responsibility for any harm to your computer system, loss or corruption of data, or other harm that results from your access to or use of the Services or Software. Some states do not allow the types of disclaimers in this paragraph, so they may not apply to you.

#### Limitation of Liability

TO THE FULLEST EXTENT PERMITTED BY LAW, IN NO EVENT WILL DROPBOX, ITS AFFILIATES, OFFICERS, EMPLOYEES, AGENTS, SUPPLIERS OR LICENSORS BE LIABLE FOR (A) ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, EXEMPLARY OR CONSEQUENTIAL (INCLUDING LOSS OF USE, DATA, BUSINESS, OR PROFITS) DAMAGES, REGARDLESS OF LEGAL THEORY, WHETHER OR NOT DROPBOX HAS BEEN WARNED OF THE POSSIBILITY OF SUCH DAMAGES, AND EVEN IF A REMEDY FAILS OF ITS ESSENTIAL PURPOSE; (B) AGGREGATE LIABILITY FOR ALL CLAIMS RELATING TO THE SERVICES MORE THAN THE GREATER OF \$20 OR THE AMOUNTS PAID BY YOU TO DROPBOX FOR THE PAST THREE MONTHS OF THE SERVICES IN QUESTION. Some states do not allow the types of limitations in this paragraph, so they may not apply to you.

#### Modifications

We may revise these Terms from time to time and the most current version will always be posted on our website. If a revision, in our sole discretion, is material we will notify you (for example via email to the email address associated with your account). Other changes may be posted to our blog or terms page, so please check those pages regularly. By continuing to access or use the Services after revisions

become effective, you agree to be bound by the revised Terms. If you do not agree to the new terms, please stop using the Services.

#### Miscellaneous Legal Terms

THESE TERMS AND THE USE OF THE SERVICES AND SOFTWARE WILL BE GOVERNED BY CALIFORNIA LAW EXCEPT FOR ITS CONFLICTS OF LAWS PRINCIPLES. ALL CLAIMS ARISING OUT OF OR RELATING TO THESE TERMS OR THE SERVICES OR SOFTWARE MUST BE LITIGATED EXCLUSIVELY IN THE FEDERAL OR STATE COURTS OF SAN FRANCISCO COUNTY, CALIFORNIA, AND BOTH PARTIES CONSENT TO VENUE AND PERSONAL JURISDICTION THERE. These Terms constitute the entire and exclusive agreement between you and Dropbox with respect to the Services, and supersede and replace any other agreements, terms and conditions applicable to the Services. These Terms create no third party beneficiary rights. Dropbox's failure to enforce a provision is not a waiver of its right to do so later. If a provision is found unenforceable the remaining provisions of the Agreement will remain in full effect and an enforceable term will be substituted reflecting our intent as closely as possible. You may not assign any of your rights in these Terms, and any such attempt is void, but Dropbox may assign its rights to any of its affiliates or subsidiaries, or to any successor in interest of any business associated with the Services. Dropbox and you are not legal partners or agents; instead, our relationship is that of independent contractors.

#### **8.4.2 Google**

This Google Apps for Business (Online) Agreement (the "Agreement") is entered into by and between Google Inc., a Delaware corporation, with offices at 1600 Amphitheatre Parkway, Mountain View, California 94043 ("Google") and the entity agreeing to these terms ("Customer"). This Agreement is effective as of the date you click the "I Accept" button below (the "Effective Date"). If you are accepting on behalf of your employer or another entity, you represent and warrant that: (i) you have full legal authority to bind your employer, or the applicable entity, to these terms and conditions; (ii) you have read and understand this Agreement; and (iii) you agree, on behalf of the party that you represent, to this Agreement. If you don't have the legal authority to bind your employer or the applicable entity, please do not click the "I Accept" button below (or, if applicable, do not sign this Agreement). This Agreement governs Customer's access to and use of the Services.

#### 1. Services

##### 1.1 Facilities and Data Transfer.

All facilities used to store and process Customer Data will adhere to reasonable security standards no less protective than the security standards at facilities where Google stores and processes its own information of a similar type. Google has implemented at least industry standard systems and procedures to ensure the security and confidentiality of Customer Data, protect against anticipated threats or hazards to the security or integrity of Customer Data and protect against unauthorized access to or use of Customer Data. As part of providing the Services Google may transfer store and process Customer Data in the United States or any

other country in which Google or its agents maintain facilities. By using the Services Customer consents to this transfer, processing and storage of Customer Data.

## 1.2 Modifications

a.

### To the Services.

Google may make commercially reasonable changes to the Services from time to time. If Google makes a material change to the Services Google will inform Customer, provided that Customer has subscribed with Google to be informed about such change.

b. To URL Terms. Google may make commercially reasonable changes to the URL Terms from time to time. If Google makes a material change to the URL Terms, Google will inform Customer by either sending an email to the Notification Email Address or alerting Customer via the Admin Console. If the change has a material adverse impact on Customer, and Customer does not agree to the change, Customer must so notify Google via the Help Center within thirty days after receiving notice of the change. If Customer notifies Google as required, then Customer will remain governed by the terms in effect immediately prior to the change until the end of the then-current Services Term for the affected Services. If the affected Services are renewed, they will be renewed under Google's then current URL Terms.

## 1.3 Customer Domain Name Ownership.

Prior to providing the Services Google may verify that Customer owns or controls the Customer Domain Names. If Customer does not own or control the Customer Domain Names, then Google will have no obligation to provide Customer with the Services.

## 1.4 Ads.

The default setting for the Services is one that does not allow Google to serve Ads. Customer may change this setting in the Admin Console which constitutes Customer's authorization for Google to serve Ads. If Customer enables the serving of Ads it may revert to the default setting at any time and Google will cease serving Ads.

## 1.5 Google Apps Vault.

If Customer purchases Google Apps Vault, the following additional terms apply:

a.

### Retention.

Google will have no obligation to retain any archived Customer Data beyond the retention period specified by Customer (other than for any legal holds). If Customer does not renew Google Apps Vault, Google will have no obligation to retain any archived Customer Data.

b. Additional Purchases. Unless Google allows otherwise, with each additional purchase of End User Accounts for the Services after Customer has purchased Google Apps Vault, Customer will receive access to, and will be invoiced for, Google Apps Vault for that same number of End User Accounts.

## 2. Customer Obligations.

### 2.1 Compliance.

Customer will use the Services in accordance with the Acceptable Use Policy. Google may make new applications features or functionality for the Services available from time to time the use of which may be contingent upon Customer's agreement to additional terms. In addition, Google will make other Non-Google Apps Products (beyond the Services) available to Customer and its End Users in accordance with the Non-Google Apps Product Terms and the applicable product-specific Google terms of service. If Customer does not desire to enable any of the Non-Google Apps Products, Customer can enable or disable them at any time through the Admin Console.

### 2.2 Aliases.

Customer is solely responsible for monitoring responding to and otherwise processing emails sent to the "abuse" and "postmaster" aliases for Customer Domain Names but Google may monitor emails sent to these aliases for Customer Domain Names to allow Google to identify Services abuse.

### 2.3 Customer Administration of the Services.

Customer may specify one or more Administrators through the Admin Console who will have the rights to access Admin Account(s) and to administer the End User Accounts. Customer is responsible for: (a) maintaining the confidentiality of the password and Admin Account(s); (b) designating those individuals who are authorized to access the Admin Account(s); and (c) ensuring that all activities that occur in connection with the Admin Account(s) comply with the Agreement. Customer agrees that Google's responsibilities do not extend to the internal management or administration of the Services for Customer and that Google is merely a data-processor.

### 2.4 End User Consent.

Customer's Administrators may have the ability to access, monitor, use, or disclose data available to End Users within the End User Accounts. Customer will obtain and maintain all required consents from End Users to allow: (i) Customer's access, monitoring, use and disclosure of this data and Google providing Customer with the ability to do so and (ii) Google to provide the Services.

## 2.5 Unauthorized Use.

Customer will use commercially reasonable efforts to prevent unauthorized use of the Services' and to terminate any unauthorized use. Customer will promptly notify Google of any unauthorized use of, or access to, the Services of which it becomes aware.

## 2.6 Restrictions on Use.

Unless Google specifically agrees in writing' Customer will not, and will use commercially reasonable efforts to make sure a third party does not: (a) sell, resell, lease or the functional equivalent, the Services to a third party (unless expressly authorized in this Agreement); (b) attempt to reverse engineer the Services or any component; (c) attempt to create a substitute or similar service through use of, or access to, the Services; (d) use the Services for High Risk Activities; or (e) use the Services to store or transfer any Customer Data that is controlled for export under Export Control Laws. Customer is solely responsible for any applicable compliance with HIPAA.

## 2.7 Third Party Requests.

Customer is responsible for responding to Third Party Requests. Google will, to the extent allowed by law and by the terms of the Third Party Request: (a) promptly notify Customer of its receipt of a Third Party Request; (b) comply with Customer's reasonable requests regarding its efforts to oppose a Third Party Request; and (c) provide Customer with the information or tools required for Customer to respond to the Third Party Request. Customer will first seek to obtain the information required to respond to the Third Party Request on its own, and will contact Google only if it cannot reasonably obtain such information.

## 3. Billing and Payment.

3.1 BillingCustomer may elect one of the following billing options when placing its order for the Services.

a.

### Flexible Plan.

If Customer selects this option, Customer will not be committed to purchase the Services for a pre-defined term, but will pay for the Services on a monthly basis.

Google will bill Customer: (i) Fees based upon Customer's daily usage of the Services during the preceding month; and (ii) monthly in arrears for its use of the Services. Google will provide Customer with the monthly rate for the Services when Customer orders the Services, and will use this rate to calculate the Fees, on a prorated basis, for Customer's daily usage during that month. Any partial day of Services usages will be rounded up to a full day of Services usage for the purposes of calculating Fees. Customer may pay for the Services using the payment options listed below.

b.

#### Annual Plan

If Customer selects this option, Customer will be committed to purchasing the Services from Google for an annual term, and in exchange will receive a discount on the Services which will be reflected in Customer's monthly payment. Google will still bill Customer monthly in arrears for its use of the Services when Customer has an annual commitment for the Services with Google. Customer may pay for the Services using the payment options listed below.

3.2 Payment. All payments due are in U.S. dollars unless otherwise indicated on the Order Page or invoice.

a.

#### Credit Card or Debit Card.

Fees for orders where Customer is paying with a credit card, debit card or other non-invoice form of payment, are due at the end of the month during which Customer received the Services. For credit cards, or debit cards, as applicable: (i) Google will charge Customer for all applicable Fees when due and (ii) these Fees are considered delinquent thirty days after the end of the month during which Customer received the Services.

b.

#### Invoices.

Payments for invoices are due thirty days after the invoice date, unless otherwise specified on the Order Page, and are considered delinquent after such date.

c.

#### Other Forms of Payment.

Customer may change its payment method to those available within the Admin Console. Google may enable other forms of payment by making them available in the Admin Console. These other forms of payment may be subject to additional terms which Customer may have to accept prior using the additional forms of payment.

#### 3.3 Delinquent Payments

Delinquent payments may bear interest at the rate of one-and-one-half percent per month (or the highest rate permitted by law, if less) from the payment due date until paid in full. Customer will be responsible for all reasonable expenses (including attorneys' fees) incurred by Google in collecting such delinquent amounts, except where such delinquent amounts are due to Google's billing inaccuracies.

#### 3.4 Suspension for Non-Payment.

a.

Automatic Suspension.

Customer will have thirty days to pay Google delinquent Fees. If Customer does not pay Google delinquent Fees within thirty days, Google will automatically suspend Customer's use of the Services. The duration of this suspension will be until Customer pays Google all outstanding Fees.

b.

During Suspension.

If Customer is on a monthly billing plan, and Customer is suspended for non-payment, Google will stop charging Customer monthly Fees during Customer's suspension for non-payment. If Customer has an annual commitment to Google for the Services, Google will continue to charge Customer monthly Fees during Customer's suspension for non-payment and Customer must pay all outstanding Fees in order to resume its use of the Services.

c.

Termination After Suspension.

If Customer remains suspended for non-payment for more than sixty days, Google may terminate Customer for breach pursuant to Section 11.

3.5 Taxes.

Customer is responsible for any Taxes, and Customer will pay Google for the Services without any reduction for Taxes. If Google is obligated to collect or pay Taxes, the Taxes will be invoiced to Customer, unless Customer provides Google with a valid tax exemption certificate authorized by the appropriate taxing authority. If Customer is required by law to withhold any Taxes from its payments to Google, Customer must provide Google with an official tax receipt or other appropriate documentation to support such payments.

3.6 Purchase Orders.

If Customer requires a purchase order number on its invoice, Customer will inform Google and Google will include such purchase order number on invoices following receipt. If Customer does not provide a purchase order number, Customer waives any purchase order requirement and (a) Google will invoice Customer without a purchase order number; and (b) Customer agrees to pay invoices without a purchase order number referenced. Any terms and conditions on a purchase order do not apply to this Agreement and are null and void.

4. Technical Support Services.

4.1 By Customer.

Customer will, at its own expense, respond to questions and complaints from End Users or third parties relating to Customer's or End Users' use of the Services. Customer will use commercially reasonable efforts to resolve support issues before escalating them to Google.

#### 4.2 By Google.

If Customer cannot resolve a support issue consistent with the above, then Customer may escalate the issue to Google in accordance with the TSS Guidelines. Google will provide TSS to Customer in accordance with the TSS Guidelines.

### 5. Suspension

#### 5.1 Of End User Accounts by Google.

If Google becomes aware of an End User's violation of the Agreement, then Google may specifically request that Customer Suspend the applicable End User Account. If Customer fails to comply with Google's request to Suspend an End User Account, then Google may do so. The duration of any Suspension by Google will be until the applicable End User has cured the breach which caused the Suspension.

#### 5.2 Emergency Security Issues.

Notwithstanding the foregoing, if there is an Emergency Security Issue, then Google may automatically Suspend the offending use. Suspension will be to the minimum extent and of the minimum duration required to prevent or terminate the Emergency Security Issue. If Google Suspends an End User Account for any reason without prior notice to Customer, at Customer's request, Google will provide Customer the reason for the Suspension as soon as is reasonably possible.

### 6. Confidential Information.

#### 6.1 Obligations.

Each party will: (a) protect the other party's Confidential Information with the same standard of care it uses to protect its own Confidential Information; and (b) not disclose the Confidential Information, except to Affiliates, employees and agents who need to know it and who have agreed in writing to keep it confidential. Each party (and any Affiliates' employees and agents to whom it has disclosed Confidential Information) may use Confidential Information only to exercise rights and fulfill its obligations under this Agreement, while using reasonable care to protect it. Each party is responsible for any actions of its Affiliates' employees and agents in violation of this Section.

#### 6.2 Exceptions.

Confidential Information does not include information that: (a) the recipient of the Confidential Information already knew; (b) becomes public through no fault of the recipient; (c) was independently developed by the recipient; or (d) was rightfully given to the recipient by another party.

### 6.3 Required Disclosure.

Each party may disclose the other party's Confidential Information when required by law but only after it, if legally permissible: (a) uses commercially reasonable efforts to notify the other party; and (b) gives the other party the chance to challenge the disclosure.

## 7. Intellectual Property Rights; Brand Features.

### 7.1 Intellectual Property Rights.

Except as expressly set forth herein, this Agreement does not grant either party any rights, implied or otherwise, to the other's content or any of the other's intellectual property. As between the parties, Customer owns all Intellectual Property Rights in Customer Data, and Google owns all Intellectual Property Rights in the Services.

### 7.2 Display of Brand Features.

Google may display those Customer Brand Features authorized by Customer (such authorization is provided by Customer uploading its Brand Features into the Services) within designated areas of the Service Pages. Customer may specify the nature of this use using the Admin Console. Google may also display Google Brand Features on the Service Pages to indicate that the Services are provided by Google.

Neither party may display or use the other party's Brand Features beyond what is allowed in this Agreement without the other party's prior written consent.

### 7.3 Brand Features Limitation.

Any use of a party's Brand Features will inure to the benefit of the party holding Intellectual Property Rights in those Brand Features. A party may revoke the other party's right to use its Brand Features pursuant to this Agreement with written notice to the other and a reasonable period to stop the use.

## 8. Publicity.

Customer agrees that Google may include Customer's name or Brand Features in a list of Google customers, online or in promotional materials. Customer also agrees that Google may verbally reference Customer as a customer of the Google products or services that are the subject of this Agreement. This section is subject to Section 7.3 (Brand Features Limitation).

## 9. Representations, Warranties and Disclaimers.

### 9.1 Representations and Warranties.

Each party represents that it has full power and authority to enter into the Agreement. Each party warrants that it will comply with all laws and regulations applicable to its provision, or use, of the Services, as applicable (including applicable security breach notification law). Google warrants that it will provide the Services in accordance with the applicable SLA.

## 9.2 Disclaimers.

TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT AS EXPRESSLY PROVIDED FOR HEREIN, NEITHER PARTY MAKES ANY OTHER WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE AND NONINFRINGEMENT. GOOGLE MAKES NO REPRESENTATIONS ABOUT ANY CONTENT OR INFORMATION MADE ACCESSIBLE BY OR THROUGH THE SERVICES. CUSTOMER ACKNOWLEDGES THAT THE SERVICES ARE NOT A TELEPHONY SERVICE AND THAT THE SERVICES ARE NOT CAPABLE OF PLACING OR RECEIVING ANY CALLS, INCLUDING EMERGENCY SERVICES CALLS, OVER PUBLICLY SWITCHED TELEPHONE NETWORKS.

## 10. Term

### 10.1 Agreement Term.

This Agreement will remain in effect for the Term.

### 10.2 Services Term and Purchases During Services Term.

Google will provide the Services to Customer during the Services Term. Unless the parties agree otherwise in writing, End User Accounts purchased during any Services Term will have a prorated term ending on the last day of that Services Term.

### 10.3 Renewal.

a.

#### With a Flexible Plan.

With a flexible plan Customer is not committed to purchase the Services for a pre-defined term, but pays for the Services on a monthly basis. As a result, there is no renewal event for the flexible plan. Rather, Google will simply continuing billing Customer Fees based upon Customer's daily usage of the Services during the preceding month, and Customer can cancel their service at any time.

b.

#### With an Annual Plan.

At the end of each Services Term, the Services (and all End User Accounts previously purchased) will automatically renew for an additional monthly Services Term. In addition, after Customer's initial annual commitment has concluded, Customer's annual commitment will switch to the Flexible Plan. If Customer wants to renew the Annual Plan, then Customer must change the renewal settings in the Admin Console to reflect this change before their annual commitment has ended.

c.

## Generally.

Customer may alter the number of End User Accounts to be renewed by communicating the appropriate number of accounts to be renewed to Google via the Admin Console. Customer will continue to pay Google the then-current Fees for each renewed End User Account unless Customer and Google mutually agree otherwise. If Google does not want the Services to renew, then it will provide Customer written notice to this effect at least fifteen days prior to the end of the then current Services Term. This notice of non renewal will be effective upon the conclusion of the then current Services Term.

### 10.4 Requesting End User Accounts.

Customer may request End User Accounts by: (i) notifying its designated Google Account Manager; or (ii) ordering End User Accounts via the Admin Console.

### 10.5 Revising Rates.

Google may revise its rates for the following Services Term by providing Customer written notice (which may be by email) at least thirty days prior to the start of the following Services Term.

## 11. Termination.

### 11.1 Termination for Breach.

Either party may suspend performance or terminate this Agreement if: (i) the other party is in material breach of the Agreement and fails to cure that breach within thirty days after receipt of written notice; (ii) the other party ceases its business operations or becomes subject to insolvency proceedings and the proceedings are not dismissed within ninety days; or (iii) the other party is in material breach of this Agreement more than two times notwithstanding any cure of such breaches.

### 11.2 Effects of Termination.

If this Agreement terminates, then: (i) the rights granted by one party to the other will cease immediately (except as set forth in this Section); (ii) Google will provide Customer access to, and the ability to export, the Customer Data for a commercially reasonable period of time at Google's then-current rates for the applicable Services; (iii) after a commercially reasonable period of time, Google will delete Customer Data by removing pointers to it on Google's active servers and overwriting it over time; and (iv) upon request each party will promptly use commercially reasonable efforts to return or destroy all other Confidential Information of the other party. If a Customer on an annual plan terminates the Agreement prior to the conclusion of its annual plan, Google will bill Customer, and Customer is responsible for paying Google, for the remaining unpaid amount of Customer's annual commitment.

## 12. Indemnification.

### 12.1 By Customer.

Customer will indemnify, defend, and hold harmless Google from and against all liabilities, damages, and costs (including settlement costs and reasonable attorneys' fees) arising out of a third party claim: (i) regarding Customer Data or Customer Domain Names; (ii) that Customer Brand Features infringe or misappropriate any patent, copyright, trade secret or trademark of a third party; or (iii) regarding Customer's use of the Services in violation of the Acceptable Use Policy.

#### 12.2 By Google.

Google will indemnify, defend, and hold harmless Customer from and against all liabilities, damages, and costs (including settlement costs and reasonable attorneys' fees) arising out of a third party claim that Google's technology used to provide the Services or any Google Brand Feature infringe or misappropriate any patent, copyright, trade secret or trademark of such third party. Notwithstanding the foregoing, in no event shall Google have any obligations or liability under this Section arising from: (i) use of any Services or Google Brand Features in a modified form or in combination with materials not furnished by Google, and (ii) any content, information or data provided by Customer, End Users or other third parties.

#### 12.3 Possible Infringement.

a.

##### Repair, Replace, or Modify.

If Google reasonably believes the Services infringe a third party's Intellectual Property Rights, then Google will: (a) obtain the right for Customer, at Google's expense, to continue using the Services; (b) provide a non-infringing functionally equivalent replacement; or (c) modify the Services so that they no longer infringe.

b.

##### Suspension or Termination.

If Google does not believe the foregoing options are commercially reasonable, then Google may suspend or terminate Customer's use of the impacted Services. If Google terminates the impacted Services, then Google will provide a pro-rata refund of the unearned Fees actually paid by Customer applicable to the period following termination of such Services.

#### 12.4 General.

The party seeking indemnification will promptly notify the other party of the claim and cooperate with the other party in defending the claim. The indemnifying party has full control and authority over the defense, except that: (a) any settlement requiring the party seeking indemnification to admit liability or to pay any money will require that party's prior written consent, such consent not to be unreasonably withheld or delayed; and (b) the other party may join in the defense with its own counsel at its own expense. THE INDEMNITIES ABOVE ARE A PARTY'S ONLY

REMEDY UNDER THIS AGREEMENT FOR VIOLATION BY THE OTHER PARTY OF A THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS.

### 13. Limitation of Liability.

#### 13.1 Limitation on Indirect Liability.

NEITHER PARTY WILL BE LIABLE UNDER THIS AGREEMENT FOR LOST REVENUES OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES, EVEN IF THE PARTY KNEW OR SHOULD HAVE KNOWN THAT SUCH DAMAGES WERE POSSIBLE AND EVEN IF DIRECT DAMAGES DO NOT SATISFY A REMEDY.

#### 13.2 Limitation on Amount of Liability.

NEITHER PARTY MAY BE HELD LIABLE UNDER THIS AGREEMENT FOR MORE THAN THE AMOUNT PAID BY CUSTOMER TO GOOGLE HEREUNDER DURING THE TWELVE MONTHS PRIOR TO THE EVENT GIVING RISE TO LIABILITY.

#### 13.3 Exceptions to Limitations.

These limitations of liability apply to the fullest extent permitted by applicable law but do not apply to breaches of confidentiality obligations, violations of a party's Intellectual Property Rights by the other party, or indemnification obligations.

### 14. Miscellaneous.

#### 14.1 Notices.

Unless specified otherwise herein, (a) all notices must be in writing and addressed to the attention of the other party's legal department and primary point of contact and (b) notice will be deemed given: (i) when verified by written receipt if sent by personal courier, overnight courier, or when received if sent by mail without verification of receipt; or (ii) when verified by automated receipt or electronic logs if sent by facsimile or email.

#### 14.2 Assignment.

Neither party may assign or transfer any part of this Agreement without the written consent of the other party, except to an Affiliate, but only if: (a) the assignee agrees in writing to be bound by the terms of this Agreement; and (b) the assigning party remains liable for obligations incurred under the Agreement prior to the assignment. Any other attempt to transfer or assign is void.

#### 14.3 Change of Control.

Upon a change of control (for example, through a stock purchase or sale, merger, or other form of corporate transaction): (a) the party experiencing the change of control will provide written notice to the other party within thirty days after the change of control; and (b) the other party may immediately terminate this Agreement any time

between the change of control and thirty days after it receives the written notice in subsection (a).

#### 14.4 Force Majeure.

Neither party will be liable for inadequate performance to the extent caused by a condition (for example, natural disaster, act of war or terrorism, riot, labor condition, governmental action, and Internet disturbance) that was beyond the party's reasonable control.

#### 14.5 No Waiver.

Failure to enforce any provision of this Agreement will not constitute a waiver.

#### 14.6 Severability.

If any provision of this Agreement is found unenforceable, the balance of the Agreement will remain in full force and effect.

#### 14.7 No Agency.

The parties are independent contractors, and this Agreement does not create an agency, partnership or joint venture.

#### 14.8 No Third-Party Beneficiaries.

There are no third-party beneficiaries to this Agreement.

#### 14.9 Equitable Relief.

Nothing in this Agreement will limit either party's ability to seek equitable relief.

#### 14.10 Governing Law.

This Agreement is governed by California law, excluding that state's choice of law rules. FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS AGREEMENT, THE PARTIES CONSENT TO PERSONAL JURISDICTION IN, AND THE EXCLUSIVE VENUE OF, THE COURTS IN SANTA CLARA COUNTY, CALIFORNIA.

#### 14.11 Amendments.

Any amendment must be in writing and expressly state that it is amending this Agreement.

#### 14.12 Survival.

The following sections will survive expiration or termination of this Agreement: Section 3, 6, 7.1, 11.2, 12, 13, 14, and 15.

#### 14.13 Entire Agreement.

This Agreement, and all documents referenced herein, is the parties' entire agreement relating to its subject and supersedes any prior or contemporaneous

agreements on that subject. The terms located at a URL and referenced in this Agreement are hereby incorporated by this reference.

#### 14.14 Interpretation of Conflicting Terms.

If there is a conflict between the documents that make up this Agreement, the documents will control in the following order: the Order Page, the Agreement, and the terms located at any URL. If Customer signs a physical agreement with Google to receive the Services, the physical agreement will override this online Agreement.

#### 14.15 Counterparts.

The parties may enter into this Agreement in counterparts, including facsimile, PDF or other electronic copies, which taken together will constitute one instrument.

### **8.4.3 Microsoft**

Standardtermer som gäller alla serviceavtal som beskrivs i det här dokumentet:

#### Definitioner

”Krav” avser ett krav som en Kund lämnar till Microsoft i samband med det här serviceavtalet om att en viss Servicenivå inte har uppfyllts och att Kunden kan ha rätt till Servicekrediter.

”Kund” avser den organisation som har undertecknat ett volymlicensavtal (”Avtal”) enligt vilket denne har köpt Windows Azure Compute-tjänster från Microsoft.

”Kundtjänst” avser de tjänster genom vilka Microsoft kan hjälpa Kunden att lösa problem med tjänsterna.

”Incident” avser alla slags omständigheter som leder till att en viss Servicenivå inte uppfylls.

”Microsoft” avser den Microsoft-enhet som undertecknade ditt avtal för Microsofts onlineprenumeration.

”Tjänst” eller ”Tjänster” avser den Windows Azure Compute-tjänst som Kunden tillhandahålls i enlighet med Avtalet.

”Servicekredit” avser den andel av månadsavgiften för Tjänsten som Kunden krediteras vid ett godkänt Krav.

”Servicenivå” avser de standarder som Microsoft väljer att följa och genom vilka Microsoft mäter den Servicenivå som tillhandahålls enligt beskrivningen nedan.

”Innehavare” avser en eller flera roller som var och en består av en eller flera rollinstanser som driftsätts i ett enda paket.

”Uppdateringsdomän” avser en uppsättning Windows Azure-datornoder där plattformsuppdateringar tillämpas samtidigt.

## Krav och Servicekrediter

Microsoft tillhandahåller det här serviceavtalet med förbehåll för följande villkor. Villkoren kan inte ändras under den första prenumerationsperioden. Om en prenumeration förlängs gäller den version av serviceavtalet som är aktuell då förlängningen inleds under hela förlängningsperioden. Kunden kan när som helst läsa den senaste versionen av serviceavtalet och relaterade villkor genom att gå till <http://go.microsoft.com/fwlink/?LinkId=159704>.

Innan ett Krav gällande en Incident kan lämnas måste Kunden underrätta Kundtjänst om Incidenten, via de procedurer som fastställts av Microsoft, inom fem arbetsdagar från Incidenten.

Innan ett Krav kan lämnas måste Kunden kontakta Kundtjänst och meddela att Kunden avser att lämna ett Krav. Kunden måste ge Kundtjänst alla relevanta uppgifter avseende Kravet, inklusive men inte begränsat till en detaljerad beskrivning av Incidenten/ Incidenterna, Incidenternas varaktighet, traceroute-nätverksloggar, berörda webbadresser samt eventuella försök av Kunden att åtgärda Incidenten.

För att Microsoft ska ta ett Krav under beaktande måste Kunden lämna Kravet, inklusive tillräckligt med stödande uppgifter, senast i slutet av faktureringsmånaden efter den faktureringsmånad då den Incident som Kravet gäller inträffade.

Microsoft använder all i rimlig utsträckning tillgänglig information för att godkänna Krav och i god tro bedöma om serviceavtalet och Servicenivåerna är tillämpliga på Kravet.

Om fler än en Servicenivå inte uppfylls på grund av samma Incident måste Kunden välja endast en Servicenivå enligt vilken ett Krav kan göras i samband med Incidenten. Inget annat Krav under någon annan Servicenivå accepteras för Incidenten i fråga.

### Undantag för serviceavtalet

Det här serviceavtalet och eventuella tillämpliga Servicenivåer gäller inte prestanda- eller tillgänglighetsproblem:

som beror på faktorer som rimligen ligger utanför Microsofts kontroll,

som beror på Kundens eller tredje parts maskinvara eller programvara,

som uppstår på grund av åtgärder eller uteblivna åtgärder från Kundens eller tredje parts sida,

som beror på att Kunden använder Tjänsten efter det att Microsoft har uppmanat Kunden att ändra sin användning av Tjänsten, såvida Kunden inte har ändrat sin användning enligt anvisningarna,

som uppstår under beta- eller utvärderingstjänster (enligt vad som fastställs av Microsoft)

eller

som beror på handlingar eller uteblivna handlingar av Kunden eller Kundens anställda, representanter, leverantörer eller underleverantörer, eller någon annan som har åtkomst till Microsofts tjänst via Kundens lösenord eller utrustning.

Servicekrediter

Antal Servicekrediter och hur de beräknas beskrivs nedan i anslutning till varje Servicenivåbeskrivning.

Servicekrediter är Kundens enda kompensation vid eventuella brott mot det här serviceavtalet.

Det antal Servicekrediter som betalas ut under en viss faktureringsmånad ska under inga omständigheter överstiga Kundens månadsavgifter för Tjänsten.

För Tjänster som köpts som en del av ett paket beräknas Servicekrediterna proportionellt, enligt vad som fastställs av Microsoft efter eget gottfinnande. Om Kunden har köpt tjänster från en återförsäljare baseras Servicekrediterna på cirkapriset för Tjänsten, enligt vad som fastställs av Microsoft efter eget gottfinnande.

Servicekrediter för det här serviceavtalet beräknas endast utifrån månadsavgifter för Windows Azure Compute. Här ingår avgifter i samband med dataöverföring till datornoder.

Servicenivåer

Servicenivå för anslutningstid per månad

Definitioner:

”Högsta antal anslutningsminuter” avser sammanlagt antal minuter under en faktureringsmånad för alla roller mot Internet med två eller fler driftsatta instanser i olika uppdateringsdomäner. Högsta antal anslutningsminuter mäts från den tidpunkt då innehavaren har driftsatts och dess associerade roller har startats till följd av en åtgärd som vidtagits av Kunden till den tidpunkt då Kunden har vidtagit en åtgärd som leder till att innehavaren avbryts eller tas bort.

”Anslutningsavbrott” avser sammanlagt antal minuter som driftsatta roller mot Internet som inte har avbrutits av en åtgärd av Kunden inte har någon extern anslutning under en femminutersperiod, enligt vad som mäts och sammanräknas i femminutersintervall.

”Anslutningstid per månad i procent” för en viss Kund avser högsta antal anslutningsminuter sammanlagt minus anslutningsavbrott delat med högsta antal

anslutningsminuter för en faktureringsmånad för en viss prenumeration på Windows Azure. Anslutningstid per månad i procent beräknas med följande formel:

$$\frac{\text{Högsta antal anslutningsminuter} - \text{anslutningsavbrott}}{\text{Högsta antal anslutningsminuter}} = \text{Anslutningstid per månad i procent}$$

Servicenivåer för anslutningstid per månad

Drifttidsandel per månad	Servicekredit*
<99,95 %	10 %
<99 %	25 %

\*Servicekredit gäller bara Windows Azure Compute-tjänster (dvs. inte Windows Azure Storage eller andra tjänster inom Windows Azure-plattformen)

Servicenivå för rollinstanstid per månad

Definitioner

”Högsta antal rollinstansminuter” avser sammanlagt antal minuter under en faktureringsmånad för alla rollinstanser från den tidpunkt då den associerade innehavaren har driftsatts och dess associerade roller har startats till följd av en åtgärd som vidtagits av Kunden till den tidpunkt då Kunden har vidtagit en åtgärd som leder till att innehavaren avbryts eller tas bort.

”Rollinstansavbrott” avser sammanlagt antal minuter för alla rollinstanser under en faktureringsmånad som driftsatts och startats genom en åtgärd av Kunden och som inte körts längre än två minuter utan upptäckt och att korrigerande åtgärder inletts.

”Rollinstanstid per månad i procent” för en viss Kund avser högsta antal rollinstansminuter sammanlagt minus rollinstansavbrott delat med högsta antal rollinstansminuter för en faktureringsmånad för en viss prenumeration på Windows Azure. Rollinstanstid beräknas med följande formel:

$$\frac{\text{Högsta antal rollinstansminuter} - \text{rollinstansavbrott}}{\text{Högsta antal rollinstansminuter}} = \text{Rollinstanstid per månad i procent}$$

Ytterligare undantag från serviceavtalet

Utöver de undantag från serviceavtalet som noteras i avsnitt 1.c. omfattar inte serviceavtalet och eventuella tillämpliga Servicenivåer i samband med den

månatliga rollinstanstiden problem med prestanda eller tillgänglighet i samband med regelbundna uppgraderingar och korrigeringar av plattformen.

Servicenivåer för rollinstanstid per månad

Drifttidsandel per månad	Servicekredit*
<99,9 %	10 %
<99 %	25 %

\*Servicekredit gäller bara Windows Azure Compute-avgifter (dvs. inte Windows Azure Storage eller andra tjänster inom Windows Azure-plattformen).

#### **8.4.4 Amazon**

Amazon S3 is intentionally built with a minimal feature set.

Write, read, and delete objects containing from 1 byte to 5 terabytes of data each. The number of objects you can store is unlimited.

Each object is stored in a bucket and retrieved via a unique, developer-assigned key.

A bucket can be stored in one of several Regions. You can choose a Region to optimize for latency, minimize costs, or address regulatory requirements. Amazon S3 is currently available in the US Standard, US West (Oregon), US West (Northern California), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Tokyo), South America (Sao Paulo), and GovCloud (US) Regions. The US Standard Region automatically routes requests to facilities in Northern Virginia or the Pacific Northwest using network maps.

Objects stored in a Region never leave the Region unless you transfer them out. For example, objects stored in the EU (Ireland) Region never leave the EU.

Authentication mechanisms are provided to ensure that data is kept secure from unauthorized access. Objects can be made private or public, and rights can be granted to specific users.

Options for secure data upload/download and encryption of data at rest are provided for additional data protection.

Uses standards-based REST and SOAP interfaces designed to work with any Internet-development toolkit.

Built to be flexible so that protocol or functional layers can easily be added. The default download protocol is HTTP. A BitTorrent™ protocol interface is provided to lower costs for high-scale distribution.

Includes options for performing recurring and high volume deletions. For recurring deletions, rules can be defined to remove sets of objects after a pre-defined time

period. For efficient one-time deletions, up to 1,000 objects can be deleted with a single request.

## Protecting Your Data

Data stored in Amazon S3 is secure by default; only bucket and object owners have access to the Amazon S3 resources they create. Amazon S3 supports multiple access control mechanisms, as well as encryption for both secure transit and secure storage on disk. With Amazon S3's data protection features, you can protect your data from both logical and physical failures, guarding against data loss from unintended user actions, application errors, and infrastructure failures. For customers who must comply with regulatory standards such as PCI and HIPAA, Amazon S3's data protection features can be used as part of an overall strategy to achieve compliance. The various data security and reliability features offered by Amazon S3 are described in detail below.

## Data Security Details

Amazon S3 supports several mechanisms that give you flexibility to control who can access your data as well as how, when, and where they can access it. Amazon S3 provides four different access control mechanisms: Identity and Access Management (IAM) policies, Access Control Lists (ACLs), bucket policies, and query string authentication. IAM enables organizations with multiple employees to create and manage multiple users under a single AWS account. With IAM policies, you can grant IAM users fine-grained control to your Amazon S3 bucket or objects. You can use ACLs to selectively add (grant) certain permissions on individual objects. Amazon S3 Bucket Policies can be used to add or deny permissions across some or all of the objects within a single bucket. With Query string authentication, you have the ability to share Amazon S3 objects through URLs that are valid for a predefined expiration time.

You can securely upload/download your data to Amazon S3 via the SSL encrypted endpoints using the HTTPS protocol. Amazon S3 also provides multiple options for encryption of data at rest. If you prefer to manage your own encryption keys, you can use a client encryption library like the Amazon S3 Encryption Client to encrypt your data before uploading to Amazon S3. Alternatively, you can use Amazon S3 Server Side Encryption (SSE) if you prefer to have Amazon S3 manage encryption keys for you. With Amazon S3 SSE, you can encrypt data on upload simply by adding an additional request header when writing the object. Decryption happens automatically when data is retrieved.

Amazon S3 also supports logging of requests made against your Amazon S3 resources. You can configure your Amazon S3 bucket to create access log records for the requests made against it. These server access logs capture all requests made against a bucket or the objects in it and can be used for auditing purposes.

For more information on the security features available in Amazon S3, please refer to Access Control and Using Data Encryption topics in the Amazon S3 Developer

Guide. For an overview on security on AWS, including Amazon S3, please refer to Amazon Web Services: Overview of Security Processes document.

### Data Durability and Reliability

Amazon S3 provides a highly durable storage infrastructure designed for mission-critical and primary data storage. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 Region. To help ensure durability, Amazon S3 PUT and COPY operations synchronously store your data across multiple facilities before returning SUCCESS. Once stored, Amazon S3 maintains the durability of your objects by quickly detecting and repairing any lost redundancy. Amazon S3 also regularly verifies the integrity of data stored using checksums. If corruption is detected, it is repaired using redundant data. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

Amazon S3's standard storage is:

Designed to provide 99.999999999% durability and 99.99% availability of objects over a given year.

Designed to sustain the concurrent loss of data in two facilities.

Amazon S3 provides further protection via Versioning. You can use Versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. This allows you to easily recover from both unintended user actions and application failures. By default, requests will retrieve the most recently written version. Older versions of an object can be retrieved by specifying a version in the request. Storage rates apply for every version stored.

### Reduced Redundancy Storage (RRS)

Reduced Redundancy Storage (RRS) is a storage option within Amazon S3 that enables customers to reduce their costs by storing non-critical, reproducible data at lower levels of redundancy than Amazon S3's standard storage. It provides a cost-effective, highly available solution for distributing or sharing content that is durably stored elsewhere, or for storing thumbnails, transcoded media, or other processed data that can be easily reproduced. The RRS option stores objects on multiple devices across multiple facilities, providing 400 times the durability of a typical disk drive, but does not replicate objects as many times as standard Amazon S3 storage, and thus is even more cost effective. Reduced Redundancy Storage is:

Designed to provide 99.99% durability and 99.99% availability of objects over a given year. This durability level corresponds to an average annual expected loss of 0.01% of objects.

Designed to sustain the loss of data in a single facility.

Effective Date: October 1, 2007

This Amazon S3 Service Level Agreement (“SLA”) is a policy governing the use of the Amazon Simple Storage Service (“Amazon S3”) under the terms of the Amazon Web Services Customer Agreement (the “AWS Agreement”) between Amazon Web Services, LLC (“AWS”, “us” or “we”) and users of AWS’ services (“you”). This SLA applies separately to each account using Amazon S3. Unless otherwise provided herein, this SLA is subject to the terms of the AWS Agreement and capitalized terms will have the meaning specified in the AWS Agreement. We reserve the right to change the terms of this SLA in accordance with the AWS Agreement.

**Service Commitment**

AWS will use commercially reasonable efforts to make Amazon S3 available with a Monthly Uptime Percentage (defined below) of at least 99.9% during any monthly billing cycle (the “Service Commitment”). In the event Amazon S3 does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

**Definitions**

“Error Rate” means: (i) the total number of internal server errors returned by Amazon S3 as error status “InternalError” or “ServiceUnavailable” divided by (ii) the total number of requests during that five minute period. We will calculate the Error Rate for each Amazon S3 account as a percentage for each five minute period in the monthly billing cycle. The calculation of the number of internal server errors will not include errors that arise directly or indirectly as a result of any of the Amazon S3 SLA Exclusions (as defined below).

“Monthly Uptime Percentage” is calculated by subtracting from 100% the average of the Error Rates from each five minute period in the monthly billing cycle.

A “Service Credit” is a dollar credit, calculated as set forth below, that we may credit back to an eligible Amazon S3 account.

**Service Credits**

Service Credits are calculated as a percentage of the total charges paid by you for Amazon S3 for the billing cycle in which the error occurred in accordance with the schedule below.

<b>Monthly Uptime Percentage</b>	<b>Service Credit Percentage</b>
Equal to or greater than 99% but less than 99.9%	10%
less than 99%	25%

We will apply any Service Credits only against future Amazon S3 payments otherwise due from you; provided that, we may issue the Service Credit to the credit card that you used to pay for Amazon S3 for the billing cycle in which the error occurred. Service Credits shall not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the

applicable monthly billing cycle is greater than one dollar (\$1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement, your sole and exclusive remedy for any unavailability or non-performance of Amazon S3 or other failure by us to provide Amazon S3 is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA or termination of your use of Amazon S3.

#### Credit Request and Payment Procedures

To receive a Service Credit, you must submit a request by sending an e-mail message to [aws-sla-request @ amazon.com](mailto:aws-sla-request@amazon.com). To be eligible, the credit request must (i) include your account number in the subject of the e-mail message (the account number can be found at the top of the AWS Account Activity page); (ii) include, in the body of the e-mail, the dates and times of each incident of non-zero Error Rates that you claim to have experienced; (iii) include your server request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks); and (iv) be received by us within ten (10) business days after the end of the billing cycle in which the errors occurred. If the Monthly Uptime Percentage applicable to the month of such request is confirmed by us and is less than 99.9%, then we will issue the Service Credit to you within one billing cycle following the month in which the error occurred. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

#### Amazon S3 SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension or termination of Amazon S3, or any other Amazon S3 performance issues: (i) that result from a suspension described in Section 6.1 of the AWS Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon S3; (iii) that result from any actions or inactions of you or any third party; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); or (v) arising from our suspension and termination of your right to use Amazon S3 in accordance with the AWS Agreement (collectively, the “Amazon S3 SLA Exclusions”). If availability is impacted by factors other than those used in our calculation of the Error Rate, we may issue a Service Credit considering such factors in our sole discretion.