Juridikgruppen

Rättsliga frågor vid flytten till molnet – en checklista

version 1.0

2011-05-11

Datum	[Med]författare	Version	Referenser
2011-02-07	Helena.Andersson@msb.se Jorgen.Axelsson@setterwalls.se anna.domander@bakermckenzie.com, Bjorn.Gustavsson@vinge.se Jens.Forzelius@hannessnellman.com Johan.Kahn@delphi.se cecilia.magnussonsjoberg@juridicum.su.se Oskar.Lothberg@vinge.se Mikael Moreira: mma@msa.se Lars.perhard@weplaw.se, **koordinator** anette.pettersson@skatteverket.se jim.runsten@twobirds.com Nicklas.Thorgerzon@vinge.se daniel.westman@juridicum.su.se	0.1	Bidrag inkomna från förf. med redovisning av bedömda tolv viktiga krav på molntjänster från juridisk synpunkt
2011-03-10	Lars Perhard	0.3	Första sammanställning och språklig genomgång
2011-03-17-23	Daniel Westman	0.4	Innehållsmässig och språklig genomgång + Fortsatt genomgång
2011-03-06 2011-04-18	Jim Runsten Lars Perhard	0.5 0.6	Revidering Innehållsmässig och språklig genomgång

Granskning

Namn	Version godkänd	Kvalitetssäkringen	Datum
Kvalitetsgranskare: Helena Andersson; Anna Domander, Jens Forselius, Björn Gustavsson, Erica Wiking Häger [ewh@msa.se], Conny.Larsson@gardepartners.se, Lars Perhard, Cecilia Magnusson Sjöberg, Jim Runsten och Nicklas Thorgerzon . Från övr. verksamhetsgrupper: Daniel.Akenine@microsoft.com; Martin.bergling@se.ibm.com; och John.lindstrom@ltu.se	Ver.0.6 godkänns till 1.0	Kvalitetsgranskarna har gått igenom v 0.6 och ställt sig bakom dokumentet; i vissa fall med förbehåll för vissa justeringar som i princip beaktats i v 1.0 nedan.	2011-05-04
Slutredigering Lars Perhard	Version 1.0	Bearbeting och integrering av resultaten från kvalitetsgranskningen	2011-05-06/11

Innehållsförteckning

I. OM CLOUD SWEDEN

Molnet är en abstraktion. Begreppet emanerar från Internets begynnelse då man ritade och abstraherade nätverket som ett moln. Begreppet fungerade som en benämning på de tekniska protokoll som användes. Senare blev molnet en beskrivning av de dokument och sidor man hämtade på Internet. Idag börjar molnet bli en benämning på de servrar, applikationer, data och tjänster som finns att tillgå via Internet.

Cloud Sweden, en verksamhetsgren och ett nätverk inom Dataföreningen, är den oberoende kontaktpunkten för kompetens om molnet. Cloud Sweden främjar ett säkert och ändamålsenligt utnyttjande av tjänster i molnet, och strävar efter att Sverige ska vara världsledande när det gäller molntjänster. Cloud Sweden vill också bidra till den internationella kompetensutvecklingen vad gäller molnet.

Cloud Sweden arbetar för att ta fram kriterier för en bra molntjänst. Det görs utifrån ett teknik-, juridik-, verksamhets- och säkerhetsperspektiv där användarens intressen sätts i fokus.

Organisationen arbetar brett för att skapa och tillgängliggöra kvalitativ information. Cloud Sweden är öppet för alla som vill engagera sig. Allt material inom organisationen tas fram under Creative Commons Licensen 3.0 Erkännande-Dela-Lika. Det innebär, enkelt uttryckt, att materialet kan användas så länge källan anges och så länge bearbetningar av materialet görs tillgängliga under samma licens.

Cloud Sweden utarbetar kontinuerligt dokument som behandlar olika aspekter på molnet. Besök gärna www.cloudsweden.se för att ta del av dessa och för att få mer information om nätverket.

II. OM DETTA DOKUMENT

Detta dokument är framtaget av Cloud Swedens arbetsgrupp för juridik (Juridikgruppen). Syftet är att dokumentet ska ge användare/kunder grundläggande insikter om de rättsliga frågeställningar som aktualiseras i samband med användning av molntjänster. Särskilt fokus riktas mot frågor som bör uppmärksammas i samband med granskningen av molntjänstleverantörernas avtalsvillkor och i samband med upprättandet av kundanpassade molntjänstavtal.

Framställningen är inte heltäckande och inte heller anpassad till enskilda kunders verksamhet och behov. En annan begränsning är att dokumentet utgår från svensk rätt trots att molntjänsterna till sin natur ofta aktualiserar även andra länders lagar. I många fall måste en kund som avser att använda sig av molntjänster anlita juridisk expertis.

Arbetet med dokumentet har bedrivits i enlighet med de principer för kvalitetssäkring som Cloud Sweden tillämpar. I ett första steg har flera av Juridikgruppens medlemmar oberoende av varandra genomfört en inventering av de mest centrala rättsliga frågeställningarna som användningen av molntjänster aktualiserar. Detta underlag har bearbetats och strukturerats av en mindre arbetsgrupp. Arbetsgruppens resultat har slutligen granskats av en vidare krets av Juridikgruppens medlemmar. Ett utkast har remitterats till andra arbetsgrupper inom Cloud Sweden för synpunkter innan det slutliga dokumentet fastställts.

Juridikgruppen avser att återkomma med fler och mer djupgående rapporter på utvalda områden. Synpunkter på detta dokument kan lämnas till lars.perhard@weplaw.se och anna.domander@bakermckenzie.com som är koordinator resp vice koordinator för juridikgruppen.

III. ALLMÄNNA RÄTTSLIGA ÖVERVÄGANDE INFÖR ANVÄNDANDET AV MOLNTJÄNSTER

Denna rapport behandlar i huvudsak rättsliga aspekter på molntjänstavtal. Innan ett avtal över huvud taget blir aktuellt är det emellertid nödvändigt att göra en riskanalys inklusive en noggrann rättslig analys och praktiska undersökningar kring lämpligheten av nyttjandet av en molntjänst. För nyttjandet av publika molntjänster är användaren beroende av access via

Internet. Driftsstopp i nätet kan snabbt bli en s.k. *single point of failure*[1] för många företag och organisationer.

Rättsliga hinder. Vid den rättsliga analysen är det inledningsvis nödvändigt att överväga om det finns några rättsliga hinder mot användning av molntjänster. I praktiken finns det få direkta rättsliga hinder, men ibland kan krav som uppställs i lagstiftningen vara svåra att uppfylla med hjälp av traditionella molntjänster. Det handlar typiskt sett om särskilda säkerhetskrav som uppställs för en viss verksamhet eller för en viss typ av information. Vanligare är emellertid att generella rättsliga krav på säkerhet, t.ex. sekretess, säkerhet vid behandling av personuppgifter, börskrav, behöver omvandlas till krav som ställs i samband med val av molntjänstleverantör eller till krav på säkerhet i molntjänstavtalet. Med ett ökat flöde av företagshemligheter som skickas och placeras utanför företagens brandväggar måste även kryptering av information övervägas.

Informationssäkerhet. En migrering av tjänster till molnet ställer särskilda krav på ett systematiskt informationssäkerhetsarbete, inte bara hos leverantören utan även hos kunden. De brister avseende informationssäkerhet som redan finns hos kunden innan beslut fattas att använda molntjänster kommer inte att automatiskt åtgärdas genom migreringen. I de flesta fall kommer det istället bli mer komplext att åtgärda bristerna när tjänsterna läggs i en molnmiljö. Utnyttjade på rätt sätt kan dock molntjänster i de flesta fall erbjuda en fullgod säkerhetsnivå.

Due diligence. En kund bör inte helt förlita sig på ett välutformat avtal utan bör även undersöka leverantörens ställning och historik. Det kan t.ex. handla om att inhämta referenser eller om att genomföra en mer eller mindre omfattande undersökning av leverantörens verksamhet och ställning utifrån såväl ett legalt, finansiellt som tekniskt perspektiv (due diligence), där kunden t.ex. får ta del av leverantörens underlag, rutiner och processer för att kunna bedöma leverantörens förmåga att leva upp till kundens krav.

 # Internationella aspekter. Molntjänster utförs ofta över landsgränser och i olika världsdelar samtidigt. Det är således inte tillräckligt att endast ta reda på var information lagras utan även var den bearbetas för det fall molntjänster används för bearbetning av data, eftersom leverantörer ofta försöker optimera sin datorkraft vid bearbetning av data. Detta innebär att information kan överföras för bearbetning för att sedan återföras och lagras i bearbetad form på överenskommen lagringsplats. Konsekvensen blir att en kund – oavsett vad avtalet anger – kan vara exponerad mot andra länders rättssystem. Dessa tekniska aspekter har

[1] Definition: En ”*Single point of failure*” är en komponent i ett system som måste fungera för att hela systemet ska fungera pga att redundans saknas.

betydelse vid bedömningen av hur t.ex. persondataskyddsfrågor (PUL) ska lösas, jfr nedan. Vidare kan exempelvis data som lagras i ett visst land bli föremål för s.k. edition eller motsvarande eller tvångsvis tillgängliggörande för [lokala] myndigheter såsom polis- eller underrättelsemyndigheter. Även sådana förhållanden bör beaktas innan molntjänster tas i bruk.

 # Riskanalys. Innan beslut om övergång till molnet fattas måste därför kunden analysera vilka risker och krav som är särskilt förknippade härmed. Det är centralt att kunden omvandlar analysens resultat till behov av säkerhetsåtgärder och förankrar dessa hos leverantören.

Upphandling. Privata företag kan i de flesta fall avtala om molntjänster utan formella krav på avtalet. Offentliga organ som är s.k. upphandlande enheter måste däremot i de flesta fall beakta reglerna om offentlig upphandling. Vidare måste stat och kommun beakta den rättsliga reglering som är förknippad med offentlighetsprincipen, arkivregler m.m., vilka inte behandlas i detta dokument.

IV. CHECKLISTA FÖR MOLNTJÄNSTAVTAL

A. ALLMÄNNA SYNPUNKTER PÅ MOLNTJÄNSTAVTAL

- Leverantörer presenterar vanligen egna standardvillkor eller allmänna villkor som underlag för avtal om molntjänster. De avtalsvillkor som föreslås är ofta förmånliga för leverantören. En blivande kund bör därför noggrant sätta sig in i de erbjudna villkoren.
- Det förhållandet att molntjänster i hög grad är standardiserade gör att utrymmet för individuella avtalsförhandlingar många gånger är kraftigt begränsat. I sådana situationer är det viktigt att kunden noggrant granskar olika leverantörers standardvillkor innan en leverantör väljs. Affärens omfattning eller parternas inbördes förhållande kan dock innebära att kunden har bättre möjligheter att individuellt förhandla om villkoren i molntjänstavtalet, t.ex. om avtal ingås med en lokal återförsäljare av molntjänster och denne tillhandahåller vissa kundspecifika anpassningar.
- Tjänstespecifikationen är helt avgörande för vilka krav som en kund kan ställa på molntjänsten. Det är viktigt att kunden försäkrar sig om att specifikationen motsvarar behoven i den egna verksamheten. Kunden bör försäkra sig om att specifikationen är så tydlig att det enkelt kan fastställas om den levererade tjänsten är avtalsenlig eller inte. Det bör därutöver tydligt framgå vad användningen av molntjänster ställer för krav på kundens driftmiljö.
- En kund bör undvika att acceptera att vissa avtalsfrågor ska bestämmas och lösas efter avtalets undertecknande, utan att i så fall i avtalet införa regler om hur detta ska gå till och vad som ska hända om parterna inte kommer överens.

- Kunden bör vara särskilt uppmärksam på avtalsvillkor som ger leverantören rätt att ensidigt ändra i tjänstespecifikationen.
- Det bör övervägas om kunden ska ges rätt att på förhand godkänna alla leverantörens underleverantörer som ska behandla eller på annat sätt komma i kontakt med kundens data.
- Avtalet bör tydligt ange vilka krav som leverantören ska uppfylla om och när det upphör.

B. ANSVAR FÖR HANTERING AV PERSONUPPGIFTER

Exempel på ett regelverk som aktualiseras vid varje användning av molntjänster är personuppgiftslagstiftningen. Den som använder sig av molntjänster måste vara observant på det ansvar som följer av personuppgiftslagens bestämmelser. Det innebär bl.a. att lagens regler om när behandling av personuppgifter är tillåten måste beaktas, att lagens säkerhetskrav måste uppfyllas och att det måste finnas ett avtal som reglerar molntjänstleverantörens behandling av personuppgifterna. För att personuppgifter ska få föras in i en molntjänst som innebär att data kan komma att lagras utanför EES-området (dvs. EU- och EFTA-länderna) gäller särskilda rättsliga krav. Den som vill använda en molntjänst för lagring av personuppgifter måste alltså antingen försäkra sig om att lagring endast sker inom EES eller aktivt se till att uppfylla kraven för överföring till tredje land.

Notera även vad som nämnts i avsnitt III ovan om att Molntjänster utförs ofta över landsgränser och i olika världsdelar samtidigt m.m. Ur personuppgiftslagstiftningens perspektiv är emellertid även överföringen för bearbetningen, själva bearbetningen liksom återföringen av bearbetad data en behandling av personuppgifter. Avtalet bör tydligt ange var kundens data får behandlas (t.ex. bestämt till region, land/länder eller datacenter) samt att detta görs spårbart. Det bör även regleras i avtalet var systemadministrativt arbete får utföras.

- Avtalet bör som ett minimum innehålla de bestämmelser som enligt personuppgiftslagen ska finnas i avtal med part som behandlar uppgifter för kundens räkning. Säkerställ även kontroll över var och av vem personuppgifter behandlas. Exempelvis bör kunden överväga att införa bestämmelser om att leverantören ska assistera kunden i frågor rörande skyldigheter enligt personuppgiftslagen, att godkännande alltid ska inhämtas av kunden om underleverantör ska användas eller om personuppgifter ska överföras till tredje land (dvs. land utanför EES), att leverantören ska stå för kostnader och risker hänförliga till avtal med underleverantörer samt att leverantören ska ersätta kunden för eventuella skador som kunden orsakas p.g.a. att leverantören eller underleverantör inte uppfyller de åtaganden som följer av avtalet.

- Om avtalet tillåter att molntjänstleverantören rent faktiskt, direkt eller indirekt genom underleverantör, behandlar kundens personuppgifter i ett land utanför EES måste avtalet innehålla en reglering av den rättsliga grunden för detta (jfr avsnitt ovan). Det finns ett flertal sätt på vilka kunden kan säkerställa att kraven för överföring av personuppgifter till tredje land uppfylls. Kunden kan t.ex. ingå ett särskilt standardavtal (ett s.k. modellklausulavtal) med leverantören som reglerar överföringen av personuppgifter. Här är det även viktigt att beakta vilket slags uppgifter det rör sig om i det enskilda fallet, hur länge behandlingen ska pågå och vad för slags dataskyddsregler som finns i det land där man vill utföra behandlingen[2].

C. KONFIDENTIALITET OCH KRYPTERING (SEKRETESS)

Konfidentialitet uppnås genom att skapa en förmåga att hindra obehöriga att få tillgång till den egna informationen. Rättsliga krav ställer i vissa sammanhang uttryckliga krav på att viss information ska ges ett konfidentialitetsskydd på detta sätt, ett bland de främsta exemplen är offentlighets- och sekretesslagens (2009:400) regelverk. Kraven på konfidentialitet behöver hanteras i avtalet med leverantören av molntjänsterna.

- Det bör i avtalet regleras att kundens information inte får lämnas ut till tredje man eller användas av leverantören för andra ändamål än att leverera tjänsten. Leverantören bör tillse att tillgången till kundens information begränsas till de personer inom organisationen som behöver access till data för att kunna utföra sina arbetsuppgifter.

- Det bör även regleras hur och på vilket sätt leverantören får övervaka samt samla in information om på vilket sätt och i vilken omfattning kunden använder sin tjänst (såsom exempelvis frekvens, ändringar i volym samt bandbredds användning etc.). Om leverantören ges sådan möjlighet, ska med noggrannhet regleras om och till vilka parter (företag, myndigheter etc.) leverantör ska kunna delge sådan information.

- Särskilt känslig information ska skyddas genom kryptering vid överföring till och från tjänsteleverantören. Det bör även övervägas om informationen ska skyddas genom kryptering när de är i ”vila”. Vidare ska säkerställas att tjänsten uppfyller gällande exportkontrollregler, särskilt i fall då tjänsten levereras från USA.

- Avtalet ska även innehålla en reglering om att leverantören ska förvara kundens information avskild från övriga kunders information.

[2] Leverantören kan bli personuppgiftsanvarig om denne behandlar kundens data utanför ändamålet med tjänsten, jfr punkt L nedan.

D. SERVICENIVÅER OCH PÅFÖLJDER

- Beroende på om tjänsten är helt eller delvis standardiserad kan det vara aktuellt att avtala om specialanpassade servicenivåer.

- Checklista för förhandling av servicenivåer:

  - Utgå från kundens verkliga behov och överväg vad som utgör lämpliga krav och vad som ska och kan mätas beträffande den aktuella tjänsten.

  – Servicenivåer bör alltid vara väl anpassade till verksamhetens behov då de annars kan leda till onödiga kostnader.

  – I en molntjänst är anslutningen av relativt enkel karaktär, varför andra parametrar än försenad leverans bör mätas, såsom t.ex. åtgärdstider vid fel, tillgänglighet och svarstider.

  – Mot bakgrund av att leverantören själv kontrollerar tjänstens utformning och utförande, bör leverantörens undantag från ansvar vara relativt begränsade.

  – Om leverantören anger en procentsats för tillgänglighet ska denna räknas om i absoluta tal för att få en exakt uppskattning av exempelvis hur många minuter per månad en tjänst kan ligga nere utan att detta medför ansvar för leverantören.

  – Överväg om hela tjänsten behöver samma servicenivå eller om differentierade nivåer är en möjlighet, t.ex. höjd servicenivå för specifika kundkritiska applikationer och olika nivåer vardag/helg och dag/natt.

  – Beskriv hur servicenivåerna ska kunna justeras över tiden samt hur de ska mätas och rapporteras.

- Viten anges ofta som påföljd när servicenivåer inte uppfylls. Vid eventuell försening av kundens anslutning, eller vid störningar i tjänsten, bör kunden kompenseras för detta.

- Vite bör beräknas på allt kunden inte kan använda till följd av störningen och kunden bör som utgångspunkt få ersättning fullt ut för sin eventuella skada. Det innebär att skadestånd ska kunna utgå utöver vitesbeloppet om kunden kan visa att hans skada inte täcks av vitet.

- Vitessatserna behöver inte vara gemensamma för hela tjänsten, utan kan differentieras, t.ex. genom:

  – Olika viten beroende på om en specifik tjänst är kundkritisk eller inte.

  – Kumulativa viten vid upprepade tillfällen eller om flera störningar på samma gång.

– Användning av kraftigt höjda viten när det exempelvis gäller de mest verksamhetskritiska systemen eller störningar av väsentlig betydelse.

- Kunden bör alltid överväga om det är lämpligt att införa alternativ eller komplement till viten som t.ex. olika incitament för att ”belöna” en leverantör för bra leveranser särskilt i de fall en sådan leverans bidrar till ett bättre resultat för kunden.

E. KRAV PÅ SÄKERHET (BACK-UP, FÖRLUST AV DATA ETC.)

- Ett grundläggande krav från kundens sida på leverantören bör vara att arbetet med informationssäkerhet bedrivs enligt etablerade standarder på området. Lämpliga säkerhetsåtgärder ska åtminstone finnas t.ex. i form **a**v säkerhetspolicy, behörighetskontroll inklusive administrativa rutiner för denna, loggning och spårbarhet, rutiner för incidenthantering och rapportering, skydd mot skadlig kod, säkerhetskopiering med återkommande kontroll av återläsbarhet och kontinuitetsplanering samt möjligheter till säkerhetsrevision både av kunden själv samt av tredje part bör regleras i avtalet. Utformningen och nivån på respektive säkerhetsåtgärd bör styras av resultatet från kundens analys av risker och krav (se ovan).

- Kunden bör klargöra och stämma av leverantörens roll i kundens kontinuitetsplanering med leverantören. Exempelvis bör kunden överväga om hela eller delar av tjänsten ska omfattas av alternativa infrastrukturer som skapar en redundans.

- Beakta vem som ska ansvara för *förlust av data* (t.ex. pga tekniska fel, stöld av data eller intrång) och hur detta begrepp definieras i det enskilda fallet. Det är viktigt att i avtalet noga klargöra vad som ska anses innefattas i sådan förlust, samt vilken av parterna som ska bära ansvar för förebyggande åtgärder såsom återställningar och backup. Kunden bör således kritiskt granska vissa leverantörers skrivningar om att förlust av data är att anse som indirekt skada, och som sådan, undantagen från leverantörens ansvar (jfr G. om ansvarsbegränsningar nedan).

F. AVVECKLING, MIGRERING OCH EXIT

- Avtalet bör innehålla bestämmelser som klargör vilka skyldigheter leverantören har att biträda kunden vid flytt till annan leverantör eller tillbaka till kund. Avtalet bör i detalj ange leverantörens skyldighet att bistå kunden och samarbeta med ny leverantör – hur och när detta ska ske och om leverantören förutom att återlämna information, även ska förstöra eller anonymisera annan information som inte återgår till kunden.

- Det bör även framgå när dessa skyldigheter aktualiseras – t ex. vid upphörande av (i) hela avtalet, (ii) del av avtalet och/eller (iii) viss specifik tjänst.

- Även om öppna standarder används är det inte okomplicerat att migrera data. Därför är det viktigt att reglera på vilket sätt och i vilket format kundens data ska återlämnas för att undvika inlåsningseffekter. Leverantören får i princip aldrig ha rätt att hålla inne kundens data. Även detta bör framgå tydligt av avtalet.

G. ANSVARSBEGRÄNSNING SÄRSKILT VID FÖRLUST AV DATA

- Vanligtvis innehåller avtal från leverantör olika former av ansvarsbegränsningar. Kunden bör i varje enskilt fall noga överväga om och på vilket sätt leverantören ska kunna begränsa sitt ansvar.

- Finn balans mellan, å ena, en skälig ansvarsbegränsning, och, å andra sidan, vikten av att leverantörens grundläggande ansvar inte urholkas. En sådan urholkning riskerar att minska leverantörens incitament att agera i enlighet med avtalets bestämmelser. Krav på ett obegränsat eller mycket långtgående ansvar för leverantören riskerar att drabba kunden i form av en prishöjning.

- Många gånger är det bättre att tydligt ange vilka typer av skador som ska omfattas respektive inte omfattas av en ansvarsbegränsning istället för att förlita sig på den traditionella uppdelningen i direkta och indirekta skador. Betänk att en stor del av den skada en kund kan komma att lida är just indirekt skada, såsom exempelvis förlorad intäkt. Ett obegränsat åtagande härvidlag skapar en stor riskexponering och oförutsebarhet för leverantören.

  Även om det ofta är rimligt att leverantören på något sätt begränsar sitt ansvar bör som nämnts olika tänkbara scenarion övervägas med beaktande av vilka risker kunden ser framför sig i det aktuella fallet. Om det är rimligt att kräva att leverantören tar ett visst ansvar även för indirekt skada, kan exponeringen t ex. begränsas genom ett angivet tak för ersättningar.

- *Force Majeure* – anpassa Force Majeure skrivningens utformning efter det specifika fallet. Väljer leverantören ett offshore alternativ, där delar av leverantörens verksamhet, exempelvis lagring, läggs ut i ett land med en helt annan infrastruktur, klimatmässiga förutsättningar el dyl. bör en *Force Majeure* skrivning, och vad som kan anses som en ”oförutsedd händelse”, tolkas i ljuset av detta.

- Vid molntjänster, då kunden enbart via exempelvis Internet ansluter sig till en av leverantören tillhandahållen tjänst, har leverantören full kontroll över hela sitt åtagande. Samtligt material från kunden hamnar hos leverantören, där kundens inblandning och kontaktytor är mycket mindre än vad de traditionellt sett har varit vid IT-leveranser. Leverantören avgör själv vilken kvalitet som servrar och annan utrustning ska ha samt vilka rutiner som ska existera i form av backuptagning, redundans osv. Detta torde innebära att leverantören för dessa nya

molntjänster bör kunna ta ett större och mer definierat ansvar vad gäller förlust av data, än tidigare.

- Undvik att kunden åläggs bevisbördan för att bevisa felets art och uppkomst.

H. IMMATERIELLA RÄTTIGHETER ETC.

- Leverantören bör garantera att för tjänsten erforderliga immateriella rättigheter finns samt åta sig ett ansvar för att nyttjande av tjänsten inte utgör intrång i tredje mans rätt. Det är inte ovanligt att licensvillkor är landsspecifika så kunden bör se till att användandet av tjänsten garanteras i samtliga länder där kunden bedriver verksamhet. Samtidigt är en av fördelarna med molntjänster att de är tillgängliga ”överallt”, varför en global garanti givetvis är att föredra. Om avtalet t ex. omfattar infrastruktur eller plattform bör kunden säkerställa att kundens licensavtal tillåter användning i sådan miljö.
- Klargör att kunden oinskränkt äger och ska behålla alla rättigheter till sina data samt att kundens rättigheter inte kan övergå till leverantören. Definitionen av ”kundens data” i avtalet bör innefatta data som kunden laddar upp till leverantören, samt resultatet av leverantörens behandling av data.

I. AVSTÄNGNING AV TJÄNST

- En kund är helt beroende av att en molntjänst levereras kontinuerligt och leverantörens eventuella möjligheter att stänga av tjänsten bör därför regleras i detalj.
- Det är viktigt att avtalet i detalj anger när sådan stängningsmöjlighet ska finnas. Leverantören bör inte ha rätt att efter eget skön stänga av tjänsten.
- För en kund är det ofta rimligt att kräva att tjänsten inte får stängas av annat än efter beslut av domstol eller skiljenämnd eller om det föreligger allvarlig och konkret risk för leverantörens säkerhet eller för att tjänsten används för att begå brott. Varje påstående om att kunden brutit mot avtalet bör t.ex. inte kunna läggas till grund för en avstängning av tjänsten.
- I avtalet bör även tas in bestämmelser om skyldighet för leverantören att bevara kundens data en viss tid även om det visar sig att leverantören äger rätt att stänga av tjänsten. Tidrymden ska vara tillräcklig för att kunden ska hinna återfå sin information.

J. FLEXIBILITET, ÄNDRING AV TJÄNSTEN OCH RAPPORTERING

- Vid nya samarbetsformer, som är under utveckling, kan det vara svårt att initialt förutse vilka situationer som kan uppkomma och hur dessa ska lösas. Eftersom molntjänster innebär en ny form av samarbete för både kund och leverantör, bör avtalet vara flexibelt och innehålla regleringar om hur förändringshanteringen går till.

- Vid molntjänster, där leverantören har kontroll över kundens data och där kunden saknar möjlighet till insyn i hur leverantören utför sin tjänst, bör samverkan och rapportering få framträdande roller.

- Det är viktigt att i avtalet föreskriva att kundens och leverantörens respektive IT-incidenthanteringsorganisationer ska upprätta ett nära samarbete med varandra.

- Ange i detalj hur samarbete och rapportering ska ske
  - Kunden bör erhålla regelbundna statusuppdateringar, information om inträffade incidenter etc.
  - Viktiga frågor bör hanteras i en kontinuerlig och öppen dialog (exempelvis rörande säkerhet).
  - Ange på vilka samverkansnivåer beslut får fattas.
  - Möjlighet att kunna eskalera viktiga uppkomna frågor i ett tidigt skede.
  - För att undvika framtida diskussioner, bör sammanträden alltid protokollföras och godkännas av båda parter.

K. AVROP

- En karaktäristisk egenskap hos molntjänster är flexibilitet och enkelhet att beställa. Det finns därmed en risk/möjlighet att kundens organisation anammar ett decentraliserat och okontrollerat IT-inköp. Om kunden upplever sådan decentralisering som negativ bör behörigheten att göra beställningar och även befogenheter vad avser belopp och tjänstetyper regleras i avtalet. På så sätt bibehåller kundens IT- eller sourcing-avdelning kontrollen.

L. LEVERANTÖRENS RÄTT ATT ANVÄNDA KUNDENS DATA FÖR ANDRA ÄNDAMÅL ÄN TJÄNSTEPRODUKTION

- Det förekommer att molnleverantörer vill använda kundens data för egen räkning, dvs. utöver tillhandahållande av tjänsten till kunden. Det kan givetvis röra sig om legitima skäl till sådan användning som att leverantören använder aggregerad data för att lära sig mer om kundernas behov och därmed skaffa sig kunskap för att kunna förbättra tjänsten. Ett rimligt grundantagande är dock att kunden inte vill att

någon annan använder kundens data. Kunden bör därför säkerställa att avtalet verkligen motsvarar kundens uppfattning i denna fråga.

- I den utsträckning som leverantören behandlar kundens personuppgifter för andra ändamål än tjänsteproduktion tillbaka till kunden blir leverantören personuppgiftsansvarig för denna behandling. Om kunden tillåter att leverantören behandlar kundens data för annat ändamål än tjänsteproduktion tillbaka till kunden måste detta utrymme noga preciseras i avtalet.

M. JURISDIKTION, LAGVAL, FORM FÖR TVISTELÖSNING M.M.

Tillämplig lag

Typ av händelse

- Frågan om tillämplig lag hänger samman med vad det är för typ av situation som är för handen. T ex. avgörs straffrättsliga frågeställningar oftast enligt det lands lag där det misstänkta brottet begåtts; persondataskyddsfrågor bedöms enligt rätten i det land där den personuppgiftsansvarige har sitt hemvist, men där även andra rättsordningar kan komma in i bilden beroende på var personuppgifterna behandlas. Det finns således en rad situationer där avtalsparterna inte disponerar över valet av tillämplig lag.

Avtalsförhållandet

- När det gäller kontraktuella relationer mellan parterna, t ex. i situationer där en part vill göra rättsliga påföljder gällande visavi motparten, kommer ofta det lands lag in i bilden till vilket avtalet har mest anknytning. Inom EU gäller bl. a den s.k. Rom I-förordningen om avtalsförpliktelser. Grunden för lagvalsreglerna i nämnda förordning är att avtalsparterna själva kan komma överens om vilket lands lag som är tillämplig på avtalet. Om parterna inte enats om detta så är huvudregeln att lagarna i det land som avtalet har närmast anknytning till är tillämpliga. Detta anknytningsland är normalt det land där den som enligt avtalet ska utföra en prestation har sin vistelseort. I ett gränsöverskridande molntjänstavtal torde detta i allmänhet vara leverantörens land. Om den ena parten befinner sig utanför EU blir det mer komplicerat. Vad gäller gränsöverskridande molntjänstavtal är det därför alltid att rekommendera att parterna redan i avtalet bestämmer om tillämplig lag. I det fall en svensk part nödgas acceptera en utländsk rättsordning kan det finnas anledning att konsultera en jurist i det landet för att få konsekvenserna av avtalets olika bestämmelser klarlagda.

- I leverantörernas standardvillkor anges typiskt sett att en tvist ska prövas enligt lagen i det land där leverantören är etablerad. Kunden bör inte utan vidare analys acceptera en sådan skrivning. Ett molntjänstavtal bör med hänsyn till vad som nämnts ovan innehålla en reglering av vilket lands lag som ska tillämpas om en tvist uppstår mellan parterna.

Forum - domstol

- Vid avtal rörande gränsöverskridande förhållanden kan det vidare vara av vikt att i avtalet klara ut var och i vilket land en tvist ska lösas. Inom EU (Bryssel I-förordningen) äger parterna i princip rätt att välja vilken domstol som ska avgöra tvisten. Annars är huvudregeln att en talan ska väckas i svarandens hemland; ett undantag är till exempel att vid avtalsbrott ska målet prövas vid ”uppfyllelseorten”, det vill säga den ort där molntjänsterna skulle ha utförts. En nackdel med domstolsprocessen är att den kan ta förhållandevis lång tid – vid en jämförelse med skiljeförfarande – bl. a eftersom det finns vissa överklagandemöjligheter. Vid gränsöverskridande tvister som sträcker sig utanför EU är domstol mindre lämpligt av flera skäl. Bl. a är det ofta svårt att få en domstolsdom verkställd i ett sådant land.

Skiljeförfarande

- Skiljeförfarande som tvistelösningsmodell är särskilt intressant vad gäller molntjänster då en vunnen skiljedom i princip är verkställbar i de allra flesta länder enligt New York-konventionen (från 1958).

- Avtalsparterna kan genom att ta in en skiljeklausul i avtalet välja att lösa eventuella tvister utanför domstol. Förfarandet bygger på frivillighet, men är reglerat i lag. Parterna kan även bestämma att skiljeförfarandet ska vara hemligt, och förfarandet kan anpassas till parternas behov i en rad hänseenden. Dels får parterna möjlighet att själv utse sina skiljemän, som i sin tur tillsammans utser en ordförande, dels får de en möjlighet att välja skiljemän med *rätt* kompetens. En skiljedom går i princip inte att överklaga. Vid skiljeförfarande får visserligen parterna ersätta skiljenämnden eller skiljemannen, men ombudskostnaderna är ofta den tunga posten. Ett rättegångsförfarande som kan leda till prövning i fler än en instans riskerar att generera väsentligen högre ombudskostnader. För kostnadsansvaret gäller i princip samma huvudregel som vid domstol, dvs. tappande part får ersätta sina egna och motpartens kostnader för förfarandet.

- Stockholms Handelskammares Skiljedomsinstitut (SCC) lämnar fyllig information om skiljeförfarande och dess regler på hemsidan www.sccinstitute.se där olika klausuler för olika nivåer kan väljas. Vid mindre omfattande projekt kan parterna

välja ett s.k. förenklat skiljeförfarande som kan genomföras relativt snabbt till en begränsad kostnad. I det fallet utses endast en ensam skiljeman.

- Ett skiljeförfarande enligt SCC:s regler kan dessutom vara att föredra då de skiljedomsregler som tagits fram ger en mer utförlig vägledning än vad som följer av lag för hur hanteringen ska gå till.
- Det kan finnas goda skäl att ta hjälp av en kunnig jurist för att informera sig om för- och nackdelar med olika tvistelösningmodeller.

// 2011-05-11