WHITEPAPER

Regulatoriska aspekter att tänka på vid en jämförelse av olika molntjänsteleverantörer

cleura

Introduktion

Molntjänster för digital infrastruktur är själva basen för den digital transformationen. Precis som annan samhällskritisk infrastruktur är molntjänsterna omgärdade av olika regelverk. Ofta innebär användningen av molntjänster att flera länders lagar och regelverk behöver appliceras och det är då komplexiteten börjar. Detta whitepaper syftar till att hjälpa dig som upphandlar molntjänster med olika frågeställningar och processer att ta ställning till för att hamna rätt regulatoriskt.

Att jämföra äpplen med äpplen

När ni jämför olika molnleverantörer, var noga med att ni utvärderar samma kvalifikationer hos era potentiella leverantörer avseende tekniska, juridiska och efterlevnadsmässiga aspekter samt servicenivåavtal och priser.

Ett standardavtal, även kallat allmänna villkor i ett publikt moln, är den enklaste typen av avtal mellan en användare och en leverantör av molntjänsten. De allmänna villkoren anger det grundläggande syftet med och förväntningarna på tjänsten och klargör relationen mellan slutanvändaren och leverantören.

De allmänna villkoren har en direkt koppling till den offentliga prislistan från leverantören av den publika molntjänsten. Den här är den mest grundläggande avtalstypen med en standardnivå för regelefterlevnad, skyldigheter och servicenivåavtal.

Organisationer som lagrar särskilt känslig och skyddsvärd information lyder nästan uteslutande under mer strikta regulatoriska krav än vad allmänna villkor kan uppfylla. Allmänna villkor är just vad namnet antyder, allmänna, och kan i regel inte uppfylla den skyddsnivå eller de regler som bolag inom bank- och finansbranschen samt sjukvården, myndigheter och övriga offentliga sektorn har för både dem själva och deras samarbetspartners, underentreprenörer och tjänsteleverantörer. De här organisationerna måste ha direktavtal med moln-tjänstleverantörerna, som specifierar högre krav på regelefterlevnad, servicenivåavtal och förmågan att genomföra revisioner på plats varje år.

Nästan alla leverantörer av publika molntjänster kan upprätta ett direktavtal sådana krav, på ett eller annat sätt. En av de viktigaste aspekterna för er som kund är dock att vara uppmärksam på priset. I takt med att ni ökar kraven stiger också priset. Utmaningen är att hitta rätt nivå för den egna organisationen samtidigt som ni säkerställer att lagar och förordningar följs.

Riskbedömning

Alla aktörer i tjänsteleverantörskedjan måste göra sin egen riskbedömning utifrån verksamhetens krav på säkerhet, regelefterlevnad och ansvar i samband med den aktuella tjänsten.

En riskbedömning bör omfatta:

- Geografisk lagringsplats för data
- Dataöverföringspunkter
- Administrationsåtkomst
- Konkurrerande datalagar i olika länder och regioner
- Molntjänstleverantörens rättsliga hemvist
- Vilket lands lag som tillämpas på avtalet
- Underentreprenörer och samarbetspartners

Hur man får klarhet i Internationella datalagar

Det finns ett flertal dataskyddslagar och -regler i världen idag som påverkar en organisations förmåga att använda internationella molntjänster och IT-tjänster i allmänhet. Ett av problemen ligger i det faktum att både leverantörer och användare av molntjänster vill att datan ska finnas tillgänglig från alla världens hörn dygnet runt. Samtidigt tillhandahålls de här tjänsterna i en värld där dataöverförings- och dataskyddslagarna fortfarande i hög grad varierar mellan olika länder och kontinenter, och vissa är direkt motstridiga.

En enkel utgångspunkt är att det är molntjänsteföretagets hemvistlands datalagar som gäller. För att illustrera med ett exempel, en amerikansk molntjänst med datacenter i Sverige lyder under amerikansk dataskyddslag så länge ägaren inte är skriven i Europa.

Allmänna punkter gällande datalagring och dataöverföringar utifrån ett EU- och GDPR-perspektiv

- Var datan lagras rent geografiskt är viktigt, men minst lika viktigt är vilka som har tillgång till datan. Amerikanska Foreign Intelligence Surveillance Act (FISA 702) reglerar insamling av data för ändamål som är relaterade till nationell säkerhet. FISA 702 har av flera rättsinstanser visat vara extraterritoriell. Det innebär att även om data lagras i Sverige hos ett Svenskt bolag så om detta bolaget är ägt av ett Amerikanskt bolag så bör man betrakta FISA 702.

- Internationell administrativ åtkomst till data som lagras exempelvis i Sverige betraktas som en internationell dataöverföring.

- Leverantörens juridiska hemvist kan vara problematiskt, om landets lagar står i direkt konflikt med de lagar vi har inom EU. Företag med juridisk hemvist inom EU har inget annat val än att följa EU:s regler och den allmänna dataskyddsförordningen, GDPR.

- Amerikanska leverantörer måste också följa EU:s regler för att kunna tillhandahålla sina tjänster inom Europa, men har också amerikanska lagar att förhålla sig till. Däribland lagar som står i direkt konflikt med GDPR.

Böter

De böter som utdöms för att inkräkta på eller göra intrång i medarbetarnas eller kundernas personuppgifter är relativt hårda i den allmänna dataskyddsförordningen.
Enligt beskrivningen i lagtexten3 är straffsatserna följande:

Mindre överträdelse: 2% av årsomsättningen eller 10 miljoner euro (det högsta)

Allvarlig överträdelse: 4% av årsomsättningen eller 20 miljoner euro (det högsta)

Böterna utdöms från fall till fall och inkluderar både samarbetspartners och underentreprenörer till moderbolaget. Exempel på verkställande finns på www.enforcementtracker.com.

Utöver böter riskerar givetvis även trovärdigheten till verksamheten från både medarbetar, kunder och andra intressenter vilket kan ge än större ekonomisk skada.

Frågor att ställa vid utvärderingen av en molntjänst-leverantör och vid upprättande av ett avtalsutkast

Har ni tillåtelse att besöka er molntjänsteleverantörs lokaler och utföra era egna revisioner?

Till följd av möjliga skillnader i ett uttalande om tillämplighet (SOA) för ISO 27001 mellan er och er leverantör måste ni försäkra er om att informations-säkerhetskedjan förblir intakt. Kort sagt har er organisation det fulla ansvaret för att göra en risk-bedömning av er molntjänstleverantör. Det i sin tur kräver att ni har ett direktavtal för att tillåta sådana revisioner, och det gäller alla molntjänstleverantörer.

Omfattas hela kedjan av administratörer av sekretess-avtal och har de gått igenom lämpliga bakgrunds- och screeningkontroller?

Alla länder har en uppsättning krav för alla personer med tillgång till sekretessbelagda uppgifter. Som en organisation som genomför databehandling måste ni säkerställa att kraven också följs av era molntjänst-leverantörer. Avtalet måste göra det möjligt för er att kontrollera all relevant personal hos molntjänstlever-antören, eller att ni kan verifiera att leverantören har genomfört kontrollerna. Det måste göras för varje en-skild person och kan inte täckas in av ett allmänt avtal.

Har ni verifierat en lämplig riskbedömning av de leverantörer som er molntjänstleverantör använder sig av?

Ni måste säkerställa och utvärdera relevanta avtal som er molntjänstleverantör i sin tur har med sina leverantörer och som är av betydelse för er säkerhet och datasekretess. Avtalet bör innehålla bestäm-melser om att ni kan göra lämpliga revisioner av er molntjänsteleverantörs leverantörer.

Var i världen finns administratörerna som har tillgång till informationen?

Ni måste göra en riskbedömning som inte bara grundar sig på var ni lagrar er data rent fysiskt, utan också vem som har åtkomst till uppgifterna och varifrån det sker. Om ni lagrar data som är sekretess-belagda i ett visst land kan den exponeras för ytterligare risker om molntjänstleverantören har administratörer som finns i ett annat land. Regler för datasuveränitet gäller även för den plats där administratörerna finns.

Om Cleura

Cleura är en ledande global leverantör av moln-tjänster för it-infrastruktur. Företagets molntjänster är alla byggda på den öppna plattformen OpenStack och erbjuds som publikt, privat eller ett compliant moln.

Cleura är certifierade enligt ISO 9001, 14001, 22301, 27001, 27010, 27013, 27017 och 27018 – internationellt erkända standarder för kvalitetsledningssystem, miljö och informationssäkerhet. Företagets tjänster finns tillgängliga från fler än 20 datacenter i hela världen. Cleura är en del av Iver.

20220520

sales@cleura.com / cleura.com

cleura