citynetwork

REGULATORISKA ASPEKTER ATT TÄNKA PÅ VID EN JÄMFÖRELSE AV OLIKA MOLNTJÄNSTLEVERANTÖRER

ATT JÄMFÖRA ÄPPLEN MED ÄPPLEN

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 bedriver verksamhet inom vissa områden eller lagrar känslig information för sina kunders räkning lyder nästan alltid under striktare regulatoriska krav. Bolag inom bank- och finansbranschen samt sjukvården, myndigheter och övriga offentliga sektorn har också särskilda regler och bestämmelser som gäller både dem själva och deras samarbetspartners, underentreprenörer och tjänsteleverantörer. För de här organisationerna räcker inte allmänna villkor för att uppfylla kraven på hur information enligt lag får behandlas och lagras. De här organisationerna måste ha direktavtal med molntjänstleverantörerna, som specifierar högre krav på efterlevnad, servicenivåavtal och förmågan att genomföra revisioner på plats varje år.

Nästan alla leverantörer av publika molntjänster kan uppfylla 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.

Sammanfattningsvis, 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.

RISKBEDÖMNING

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

EN RISKBEDÖMNING BÖR OMFATTA:

- **GEOGRAFISK LAGRINGSPLATS FÖR DATA**
- **DATAÖVERFÖRINGSPUNKTER**
- **ADMINISTRATÖRSÅTKOMST**
- **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.[1]

[1] Europeiska dataskyddsstyrelsens regler avseende CLOUD Act: restriktiv hållning i fråga om legitimiteten i dataöverföringar till USA:s undersökande myndigheter https://www.cms-lawnow.com/ealerts/2019/07/edpb-rules-on-the-cloud-act-restrictive-position-on-the-legitimacy-of-data-transfers

ALLMÄNNA PUNKTER GÄLLANDE DATALAGRING OCH DATAÖVERFÖRINGAR UTIFRÅN ETT EU- OCH GDPR-PERSPEKTIV

- **Var datan lagras rent geografiskt är inte lika viktigt som vem som har tillgång till den.**
- **Internationell administrativ åtkomst till data som lagras exempelvis i Sverige betraktas som en internationell dataöverföring.[2]**
- **Leverantörens juridiska hemvist avgör vilket lands lagar som leverantören måste följa.**
- **Företag inom EU har inget annat val än att följa EU:s regler och den allmänna dataskyddsförordningen, GDPR.**
- **Amerikanska leverantörer måste följa amerikanska lagar, bland annat CLOUD Act, även om de har kontor och datacenter i Europa.[3]**

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 lagtexten[3] 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

[2] Art. 49 GDPR. Undantag i särskilda situationer – https://gdpr-info.eu/art-49-gdpr/
[3] GDPR böter och avgifter – https://www.gdpreu.org/compliance/fines-and-penalties/

FRÅGOR ATT STÄLLA VID UTVÄRDERINGEN AV EN MOLNTJÄNSTLEVERANTÖR OCH VID UPPRÄTTANDET AV ETT AVTALSUTKAST

Har ni tillåtelse att besöka deras 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 informationssäkerhetskedjan förblir intakt. Kort sagt har er organisation det fulla ansvaret för att göra en riskbedömning 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 sekretessavtal 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 molntjänstleverantörer. Avtalet måste göra det möjligt för er att kontrollera all relevant personal hos molntjänstleverantören, eller att ni kan verifiera att leverantören har genomfört kontrollerna. Det måste göras för varje enskild 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 bestämmelser 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 sekretessbelagda 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.

NÅGRA SISTA RÅD

Vi kanske får uppleva en tid då brott mot datasekretessen är något som hör historien till, men det är osannolikt. Eftersom varje mänskligt fel, kriminella handlingar, och ringar på vattnet till följd av obetydliga misstag kan innebära en katastrof, är den enda egentliga frågan i vilken mån vi kan förbereda oss för och skydda oss mot det oundvikliga. I den informationsera vi lever är svaret att springa fortare än konkurrenterna genom att ständigt höja medvetandet om möjliga risker och avvärja dem.

- **Se till att dataskyddskedjan aldrig bryts.**

- **Kartlägg och skriv avtal om era datarelationer med alla som har direkt eller indirekt tillgång till den data som er organisation ansvarar för.**

- **Er organisations möjligheter att vidta rättsliga åtgärder mot en underentreprenör kan aldrig sudda bort fläckarna på ert anseende om det väl händer något.**

OM CITY NETWORK

City Network är en ledande leverantör av tjänster för IT-infrastruktur.

Bolaget erbjuder publika och privata molnlösningar samt hybrid-lösningar baserade på OpenStack från fler än 20 datacenter i hela världen. Genom sitt branschspecifika IaaS City Cloud kan bolaget säkerställa att kunderna uppfyller de krav som följer med särskilda lagar och regler gällande revision, anseende, databearbetning och datasäkerhet såsom Basel och Solvency och GDPR. City Network är certifierade enligt ISO 9001, 14001, 22301, 27001, 27010, 27013, 27017 och 27018 samt följer PCI-CPP C5, SOC 2, PCI-DSS och HIPAA – internationellt erkända standarder för kvalitetsledningssystem, miljö och informationssäkerhet.

SALES@CITYNETWORK.SE WWW.CITYNETWORK.SE


WWW.FACEBOOK.COM/CITYNETWORK


WWW.TWITTER.COM/CITYNETWORK

WWW.YOUTUBE.COM/CITYNETWORKHOSTING

citynetwork