



WEBINAR - MOLNTJÄNSTER I EN OROLIG OMVÄRLD - VAD BEHÖVER KOMMUNER TÄNKA PÅ

Sammanfattning från Webinar 11 april 2025.

Du kan se hela webinarret på digitalasamtal.se/akademi

När molnet blir en säkerhetsfråga – och offentlig sektor står i centrum

Vad innebär det att säkerställa digital suveränitet inom offentlig sektor – och varför är det plötsligt så brådskande? Frågan diskuterades nyligen vid ett webinarium anordnat av Akademi Digitala Samtal, där representanter från kommuner, myndigheter och leverantörer samlades för att ta del av insikter från en av Europas ledande experter på området: Johan Christensson, grundare av Cleura och medlem i ledningsgruppen för Iver.

Med ett förändrat säkerhetsläge, nya handelsbarriärer och ökade krav på dataskydd inom EU står kommuner och regioner inför ett skifte. Samtidigt flyttar allt fler välfärdstjänster till molnet – men vem kontrollerar egentligen infrastrukturen bakom? Vad är ett compliant cloud, och vilka risker löper verksamheter som förlitar sig på amerikanska tjänster som AWS, Google eller Microsoft?

I denna artikel sammanfattar vi det viktigaste från webinariet, med särskilt fokus på vad offentlig sektor behöver tänka på i ett digitalt landskap som snabbt håller på att ritas om.



Kapitel 1: "Vem äger ditt data?" – därför räcker det inte att servern står i Sverige

När offentlig sektor väljer molntjänst är det lätt att tro att lagring i Sverige eller inom EU är tillräckligt för att säkerställa kontroll och integritet. Men enligt Johan Christenson, grundare av Cleura och en av Europas ledande röster inom digital suveränitet, är detta en farlig förenkling. Det handlar inte bara om var datan lagras – utan **vem som har rätt att begära ut den**.

Bakom detta resonemang ligger den amerikanska lagen CLOUD Act (Clarifying Lawful Overseas Use of Data Act), som ger amerikanska myndigheter rätt att kräva ut data från företag med huvudkontor i USA – oavsett var i världen serverna står. Det innebär att en kommun som lagrar känslig information i en tjänst som drivs av amerikanska aktörer, som AWS, Microsoft eller Google, riskerar att den datan kan bli tillgänglig för utländska myndigheter – utan att svenska eller europeiska lagar väger tyngre.

"Det är inte en teknisk fråga – det är juridiskt och affärsmässigt. Den som har makt över bolaget har makt över datat, oavsett fysisk plats", förklarar Johan under samtalet.

Det är därför, menar han, som vi måste flytta fokus från **"location" till jurisdiction** – från var en server står till vilka lagar och intressen som styr den som har tillgång till datan.

För kommuner och regioner innebär det att en juridiskt säker molntjänst inte bara behöver följa **GDPR**, utan också vara **helt fri från utomeuropeiskt inflytande**. Och det räcker inte med fina ord i ett avtal – det måste vara tekniskt och organisatoriskt omöjligt för icke-EU-aktörer att komma åt informationen. Endast då kan man tala om verklig efterlevnad av offentlighetsprincipen, skydd av individens integritet – och demokratisk kontroll.

Den viktiga insikten, säger Johan, är alltså att **det är inte servern som avgör tilliten – det är leverantören**.

Kapitel 2: En ny geopolitisk verklighet – därför måste vi bygga europeiska alternativ

Molnteknik har länge betraktats som något globalt, gränslöst och värdeneutralt – men den bilden är snabbt på väg att förändras. Under seminariet lyfter Johan Christenson att vi idag befinner oss i en helt ny geopolitisk verklighet, där teknologisk infrastruktur blivit en del av storpolitikens kärna.

"Vi måste förstå att teknik inte längre är neutral. Den har blivit ett maktmedel. Och just därför måste offentlig sektor välja medvetet," menar Johan.

Det som tidigare handlade om effektivisering och kostnadsbesparing har idag blivit en fråga om **digital självständighet, beredskap och demokratisk suveränitet**. Med ett allt mer osäkert globalt läge – där USA:s och Kinas intressen dominerar den tekniska arenan – riskerar EU att hamna i ett digitalt beroendeförhållande till andra maktblock. Och just därför krävs nu strategiska satsningar för att säkra både **tillgång, kontroll och kontinuitet** i offentlig digitala tjänster.

Sverige står inte ensamt i detta. I flera EU-länder diskuteras nu nationella molnstrategier, krav på digital suveränitet och införande av "Trusted Cloud"-märkningar. Johan jämför med hur Europa byggt upp egen infrastruktur inom försvar, energi och livsmedel – och menar att samma tank behöver gälla för data och digitala tjänster.

"Vi behöver vårt eget digitala beredskapslager – för tryggheten, för framtiden och för friheten."



I praktiken betyder detta att svenska kommuner, regioner och myndigheter **måste börja prioritera leverantörer med europeisk hemvist, kontroll och jurisdiktion**. Först då kan vi bygga en digital infrastruktur som är robust nog att stå emot framtidens utmaningar – både politiskt, tekniskt och juridiskt.

Kapitel 3: Offentlig sektor som strategisk inköpare – dags att ställa rätt krav

En av de mest centrala punkterna i samtalet är att offentlig sektor inte bara är en stor användare av digitala tjänster – utan också en av de mest inflytelserika **inköparna**. Och med den rollen kommer ett ansvar. Ett ansvar att fatta medvetna beslut som inte bara gynnar den egna organisationen på kort sikt, utan som också formar den framtida digitala infrastrukturen för hela samhället.

”Det offentliga har en enormt stark förhandlingsposition – men den används alldeles för sällan,” konstaterar Johan.

I dag är det många kommuner och regioner som lutar sig mot standardiserade upphandlingar och generiska kravställningar. Men för att uppnå verklig **digital självständighet och datasuveränitet**, krävs att man som inköpare börjar ställa vassare, tydligare och mer informerade krav.

Det handlar inte bara om att ställa krav på **funktionalitet**, utan också på **ägarstruktur, dataplacering, jurisdiktion och kontroll**. Exempel på sådana krav kan vara:

- Att leverantören är etablerad i EU och omfattas av EU-lagstiftning.
- Att data lagras och hanteras inom EU:s gränser, utan åtkomst från tredjeland.
- Att tekniken är byggd på öppna standarder och kan granskas.

Johan lyfter också vikten av att **lyssna mindre på tekniska buzzwords – och mer på de faktiska riskerna**. Bara för att en tjänst sägs vara säker, behöver det inte betyda att den är rätt val ur ett samhällsperspektiv.

Som offentlig beställare bör man fråga sig:

- Vad händer om tjänsten försvinner i morgon?
- Vem har rätt att tvinga leverantören att lämna ut data?
- Hur säkerställer vi långsiktig tillgänglighet och kontroll?

”Om inte kommuner och myndigheter börjar agera strategiskt, så kommer vi snart stå i en situation där våra viktigaste system ligger i knät på utländska aktörer – utan att vi kan påverka.”

Det är nu det gäller. Den som upphandlar idag, lägger grunden för det digitala samhälle vi lever i om fem, tio eller femton år. Och där kan varje kommun göra skillnad.

Kapitel 4: Molnfrågan är inte teknisk – den är politisk

I många kommuner behandlas frågan om molntjänster fortfarande som en rent teknisk angelägenhet – något som IT-avdelningen eller leverantören ansvarar för. Men enligt Johan Christensson är detta en **fundamental missuppfattning**. Frågan om var våra data lagras, vem som har åtkomst till dem och vilka lagar som styr vår digitala infrastruktur är i allra högsta grad **politisk**.



"Det här handlar inte om vilken teknisk lösning som är snabbast eller billigast. Det handlar om vilket samhälle vi vill bygga."

Johan lyfter hur EU:s försök att skapa en digital suveränitet – bland annat genom initiativ som **GAIA-X** och arbetet med **EUCS-certifiering (European Cybersecurity Certification Scheme)** – syftar till att ge medlemsländerna kontroll över sina digitala resurser. Men dessa initiativ kräver att medlemsstaterna, och särskilt den offentliga sektorn, **tar ansvar för implementeringen**.

Samtidigt utgör USA:s lagstiftning, såsom **Cloud Act** och tidigare **Patriot Act**, en direkt utmaning. Den gör det möjligt för amerikanska myndigheter att kräva ut data från amerikanska bolag – oavsett var i världen dessa data lagras. Detta gäller alltså även om kommunen i fråga använder en tjänst från ett amerikanskt bolag som drifas på svensk mark.

"Det är inte en fråga om att misstro USA – det är en fråga om att skydda våra egna medborgares rätt till integritet, och vår egen självständighet som nation."

Under samtalet lyfts också att **samma logik gäller på lokal nivå**. En kommun som outsourcar sin digitala kärninfrastruktur till aktörer vars kontroll ligger utanför EU förlorar i praktiken kontrollen över viktiga samhällsfunktioner. Detta kan få konsekvenser både ur ett säkerhets- och ett demokratiperspektiv.

Johan menar att **kommunerna måste sluta behandla molnfrågan som om det bara handlade om prestanda och kostnad**. Det handlar om tillit, kontroll och långsiktig hållbarhet.

Kapitel 5: Vad bör kommuner göra nu? – Tydliga råd för en säker väg framåt

Så vad bör egentligen kommuner göra – här och nu – för att hantera den snabbt förändrade situationen kring molntjänster och digital infrastruktur?

Johan Christensson lämnar inga vaga formuleringar. Tvärtom, han ger ett antal **konkreta, tydliga och handlingsbara rekommendationer** för kommuner som vill ta kontroll över sin digitala framtid.

1. Ta ett aktivt politiskt beslut

Frågan om var kommunens information ska lagras är inte bara en teknisk detalj. Det är en demokratisk och strategisk fråga som kräver beslut på högsta nivå. Johan menar att detta måste upp till kommunstyrelsen – och att det är dags att sluta ducka frågan.

"Antingen väljer man att lägga sin känsligaste information hos amerikanska techbolag, eller så väljer man att bygga upp en europeisk lösning. Men man måste välja."

2. Ställ rätt krav i upphandlingar

För att framtidssäkra kommunens digitala tjänster behöver kraven i upphandlingar förändras. Det räcker inte att säga att en lösning är "säker" – kommunen måste kräva att data hanteras inom EU, under EU-rätt, och att det finns ingen beroendeställning till amerikansk jurisdiktion.

Detta innebär att man i praktiken ofta måste välja bort de största molnaktörerna – även om de rent tekniskt uppfyller många andra kriterier.

3. Skaffa kontroll över leveranskedjan

Kommunen måste förstå inte bara vem som drifrar tjänsten, utan på vems plattform tjänsten är byggd. En europeisk leverantör som i sin tur bygger sin infrastruktur på exempelvis AWS eller Azure är fortfarande ett beroende av USA.



"Ställ frågan: Vem har nyckeln till våra system? Och vems lagar gäller när någon knackar på och vill ha ut data?"

4. Säkerställ förutsägbarhet och motståndskraft

Johan lyfter vikten av att kommuner bygger upp digital beredskap. Det handlar inte bara om att förebygga säkerhetsrisker – utan också om att skapa operativ resiliens. Om något händer i omvärlden – en konflikt, ett handelskrig, eller förändrade lagar – ska kommunen kunna fortsätta bedriva sin verksamhet **utan att vara beroende av aktörer utanför EU**.

5. Börja nu – vänta inte på "perfekta" lösningar

Slutligen skickar Johan med en viktig påminnelse: Det finns redan idag fullt fungerande alternativ. Cleura är ett exempel, men det finns flera. Att vänta på att EU ska tvinga fram en lösning eller att marknaden ska "lösa det själv" är att ta en onödig risk.

"Det här handlar inte om att vänta på att någon annan ska ta ansvar. Det handlar om att vi i offentlig sektor måste kliva fram – och visa ledarskap."

Avslutning: Från passivitet till handling – nu krävs digitalt ledarskap

Samtalet med Johan Christensson lämnar oss inte bara med ny kunskap – utan med ett uppdrag. I takt med att världen förändras, blir det allt tydligare att den svenska offentliga sektorn inte längre kan förlita sig på lösningar byggda på en annan kontinents lagar, prioriteringar och kommersiella intressen.

Trygg välfärd i en digital tidsålder kräver mer än tekniska system. Det kräver digital suveränitet – att kommuner själva har kontroll över sin data, sin infrastruktur och sin beredskap.

Det handlar inte om teknik för teknikens skull. Det handlar om att säkra medborgarnas rättigheter, att bygga robusta samhällsfunktioner och att långsiktigt skydda det som är vårt gemensamma. Precis som vi inte outsourcar dricksvattnet eller detaljplaneringen av våra städer, ska vi heller inte outsourca våra mest centrala informationssystem till andra jurisdiktioner.

Johan är tydlig: Alternativen finns. Väntar vi för länge blir det dyrt – inte bara i pengar, utan i förtroende, säkerhet och kontroll.

Nu är det upp till kommunerna att kliva fram.

Nu är det dags att **leda digitaliseringen – inte bara förvalta den**.

Om Johan Christensson

Johan Christensson är en av Europas mest erfarna experter inom digital suveränitet, molninfrastruktur och efterlevnad. Han är grundare av Cleura, ett svenskt molnföretag som erbjuder Compliant Cloud – en EU-baserad molntjänst utvecklad för att möta offentlig sektors behov av säkerhet, kontroll och integritet. Cleura är idag en del av Iver-koncernen där Johan har en ledande roll som ansvarig för Technology Strategy and Platforms.

Johan har i över 20 år varit en tongivande röst i debatten om Europas behov av oberoende IT-infrastruktur och behovet av att bygga robusta alternativ till amerikanska molnjättar. Han är en återkommande debattör i Dagens Industri och andra medier, där han bland annat föreslagit ett europeiskt "digitalt Airbusprojekt" för att värna vår teknologiska suveränitet.



Med både strategiskt helhetsperspektiv och djup teknisk kompetens är Johan en efterfrågad rådgivare i frågor som rör digital infrastruktur, cybersäkerhet, dataskydd och geopolitisk påverkan på molnmarknaden. Han är en central röst i omställningen mot ett mer motståndskraftigt och självständigt digitalt Europa.

Om Digitala Samtal

Digitala Samtal är en svensk leverantör av säker välfärdsteknik och digitala kommunikationstjänster för kommunal omsorg och socialtjänst. Genom ett komplett ekosystem av tjänster – såsom Digitalt Hemtjänst, Digitalt Boendestöd, Digital Socialtjänst samt Digital Hemvård – möjliggör vi digitala insatser i vardagen för brukare i hela landet.

Våra lösningar är utvecklade för offentlig sektor, med fokus på hög användbarhet, robust säkerhet och nära integration med kommunens befintliga system. Tjänsterna levereras som helhetslösningar och är helt molnbaserade, med förinstallerade enheter, mobil datatrafik och full support inkluderad.

Digitala Samtal används idag av ett växande antal kommuner och kommunalförbund i Sverige, och är upphandlingsbar via Adda, Atea och Kammarkollegiet. Vi arbetar för att digital omsorg ska vara trygg, enkel att införa – och göra verklig skillnad för både brukare och personal.

Om Akademi Digitala Samtal

Akademi Digitala Samtal är vår kunskapsplattform där kommuner och andra aktörer inom offentlig sektor kan ta del av fördjupande webinarier och samtal kring digitalisering i välfärden. Akademin bjuder in experter, forskare och praktiker inom juridik, dataskydd, ledarskap, digital transformation och socialt arbete – med fokus på det som är viktigt i vardagen för kommuner och verksamheter.

Genom Akademin vill vi bidra till kunskapsspridning, inspiration och gemensamt lärande – med ett tydligt verksamhetsperspektiv.

Vill du veta mer

Vill du veta mer om hur Digitala Samtal uppfyller och arbetar med dessa krav i sina lösningar? Hur Digitala Samtal fungerar, eller kanske hur du integrerar Digital Hemtjänst i ert verksamhetssystem?

Boka ett möte på digitalasamtal.se/kontakt.

Vi hjälper dig även att komma i kontakt med Johan Christensson för mer diskussioner om hur ni kan tänka kring molntjänster.