EU:s Tech Sovereignty Package

En analys av potentiella konsekvenser för svenska kommuner och myndigheter

Agenda

01. Vad innehåller EU:s suveränitetspaket — och vad är bindande?

02. Hur påverkar CADA:s fyra nivåer kommunal IT-upphandling?

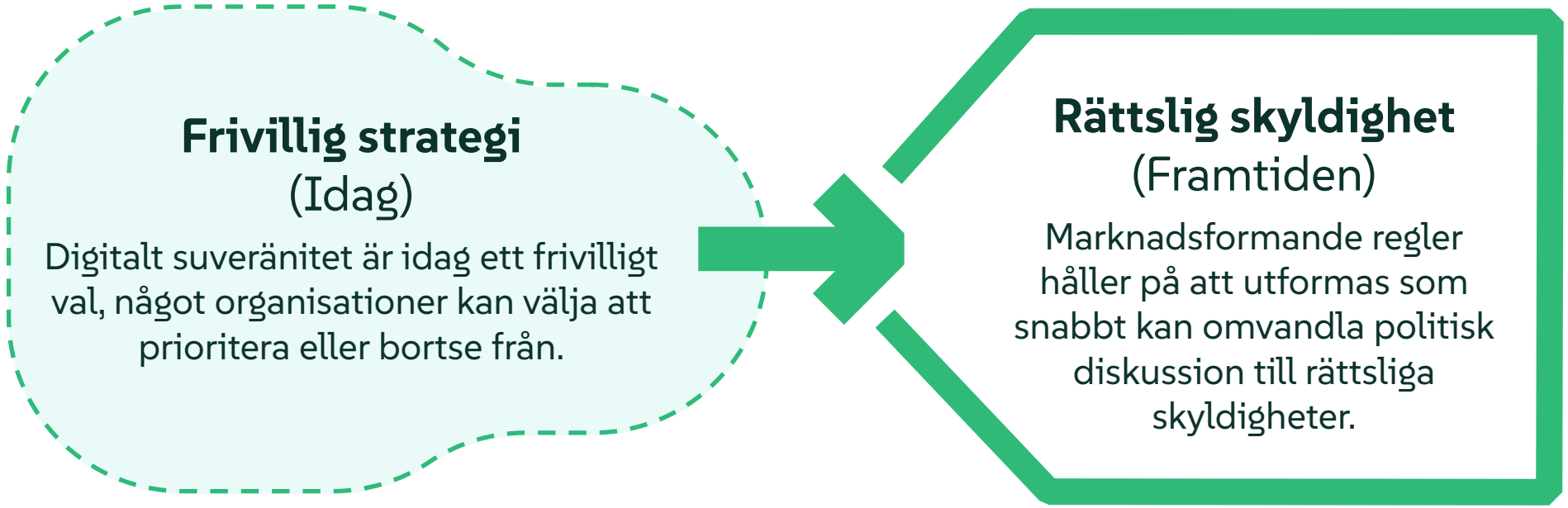
03. Vad kräver EU:s Open Source-strategi av offentlig sektor?

04. Vilka konkreta steg behöver kommuner ta nu?

I AM NOT A LAWYER

Från frivillig strategi till rättslig skyldighet

Europa har ett molnproblem, och det försöker lösa det genom att investera pengar, ändra reglerna och göra öppen källkod till standard. Branschen har verkat i ett lätt reglerat fält och det förändras nu.



EU tar kontroll över sina digitala leveranskedjor och framtid

EU:s Tech Sovereignty Package markerar en genomgripande förändring i unionens syn på teknik och är ett avgörande steg mot stärkt europeisk teknologisk suveränitet.

Vad paketet syftar till

- Mer avancerade chip för innovation och investeringar i nyckelssektorer
- Förbättrad motståndskraft och autonomi inom moln och AI
- Starkare ekosystem för öppen källkod i kritiska sektorer
- Hållbar integrering av datacenter i energisystem

De fyra instrumenten

- Chips Act 2.0
- Cloud and AI Development Act
- EU Open Source Strategy
- Strategisk färdplan för digitalisering och AI i energisektorn

Europas utländska beroenden enligt CADA

70%+

Överberoende som strategisk risk

Marknaden domineras av 3 icke-europeiska leverantörer

29%→15%

Fel riktning

EU-leverantörers molnmarknadsandel 2017–2022

CADA:s förklarande memorandum klargör beroendet: **EU-leverantörernas marknadsandel föll från 29% till 15%** mellan 2017 och 2022.

Missbruk

Kommissionens egna hotbegrepp

sabotage, vapenisering, spionage, tvång

För en ledare inom försvar, offentlig sektor eller samhällskritisk verksamhet skapar den listan en annan sorts brådska än ett marknadsandelsdiagram.

Kill Switch

Risken för ett digitalt nödstop är verklig

Ensidiga beslut av tredjelandsaktörer kan avbryta tjänsteleveransen

Den amerikanska CLOUD Act, kinesiska nationella säkerhetslagar och liknande extraterritoriella instrument innebär att en utländsk regering kan tvinga en leverantör att agera på sätt som strider mot europeisk lag, eller helt enkelt stänga av åtkomsten.

Paketets fyra åtgärdsaxlar

Från “preferens för öppen källkod” till rättslig skyldighet

Investering

EU investerar kraftigt i moln- och AI-infrastruktur med målet att tredubbla kapaciteten

Infrastruktur

Snabbspår för tillstånd, accelerationszoner för datacenter

Suveränitetsnivåer

Fyranivåcertifiering; högre nivåer är en upphandlingsregel, inte en preferens

Öppen källkod-krav

Explicit prioritering av öppen källkod i offentlig upphandling

CADA är ett kommissionsförslag (COM(2026) 502) som ännu inte trätt i kraft. EU:s Open Source-strategi (COM(2026) 503) är ett meddelande, inte en bindande förordning.

Upphandling som suveränitetsverktyg: vad förändras för kommuner?

Digitalt suveränitet börjar inte i driftsättningen och det börjar i upphandlingsfasen. CADA förflyttar bedömningspunkten från teknisk kapacitet till strukturell äganderätt och operationell jurisdiktion.

Vad upphandlare ställt hittills

Funktionella krav: vad kan tjänsten göra?

Prestandakrav: SLA, tillgänglighet, svarstider

Kostnadsjämförelse: TCO-analys

Säkerhetskrav: ISO 27001, SOC 2

Vad CADA kräver nu

Strukturell: var är moderbolaget registrerat?

Operationell: support endast av EU-medborgare?

Supply chain: finns SBOM och migrationsplan?

Certifiering: vilken suveränitetsnivå (1–4)?

Konsekvenser vid uteblivna frågor

- Risk för kostsam omupphandling vid lagkraft.
- Granskning av revisorer *innan* kontraktsskrivning.
- Personligt ansvar för kommunledning via SFS 2025:1506 vid incident.

"Det räcker inte att välja en europeisk leverantör.
Ni behöver kunna dokumentera varför den specifika strukturen uppfyller den nivå era kritiska system kräver."

CADA är nästa lager i ett nationellt säkerhetsramverk som redan är i rörelse.

CADA:s fyra suveränitetsnivåer

De fyra suveränitetsnivåerna. I AM NOT A LAWYER!

Nivå	Centralt tekniskt krav	Konsekvens för upphandling	Tredjelandsexponering	Relevans för kommunal verksamhet
Nivå 1	Egenkontroll och konformitetsförklaring	Infrastruktur och kunddata lokaliserade inom EU	Ej begränsad	Alla kommunala molntjänster — miniminivå utan undantag
Nivå 2	Oberoende tredjepartsrevision, årlig förnyelse	Fullständig transparens i leveranskedjan; SBOM dokumenterat; cybersäkerhetscertifikat på nivån "substantial"	Möjlig med dokumenterade skyddsåtgärder	HR-system, lönehantering, e-tjänsteplattformar, ärendehantering
Nivå 3	Tredjepartsrevision + strukturell ägarskapsvalidering	Leverantören och dess underleverantörer får inte vara rättsligt underställda utomeuropeisk lagstiftning; all support utförs av EU-medborgare inom unionen	Förbjuden	Samhällsviktig infrastruktur, krisberedskap, miljö- och vattenövervakning, socialregister
Nivå 4	Strängaste revision + effektiv kontroll över komponentutveckling	Leverantören måste påvisa att ingen tredjelandsentitet utövar effektiv kontroll över design, underhåll, säkerhetshantering eller långsiktig kontinuitet hos ingående programvarukomponenter (Annex II, Art. 4.1(i)(ii))	Förbjuden	Klassificerad kommunikation, säkerhetspolisiära funktioner, försvarsrelaterade uppdrag

Två arkitekturinriktningar

CADA ställer inte krav på ett specifikt verktyg utan på arkitekturella egenskaper. Har din stack dessa?

Typisk befintlig kommunal IT-stack

Karaktäristika som skapar CADA-exponering:

- **Proprietära kontrollplan** — Inlåsta i leverantörsspecifika gränssnitt utan insyn.
- **Hyperscaler-beroende** — Designade för specifika API:er, omöjliggör portabilitet.
- **Rättslig exponering** — Utländsk lagstiftning kan kräva tillgång till EU-data.
- **Avsaknad av SBOM** — Ingen dokumenterad inventering av komponenter.
- **Support utanför EU** — Operativ support i strid med suveränitetskrav.

CADA-kompatibel arkitekturinriktning

Arkitekturella egenskaper som möjliggör certifiering:

- **Granskningsbara plattformar** — Öppen källkod som primärt verktyg för revision.
- **Öppna standarder** — Byggt på standardiserade API:er och containerformat.
- **EU-kontrollerad gräns** — Moderbolag och support helt under EU-jurisdiktion.
- **SBOM-dokumentation** — Fullständig kontroll över hela leveranskedjan.
- **Verifierbar kontroll** — Ingen tredjelandsentitet kontrollerar teknisk utveckling.

Det handlar inte bara om leverantörsbyte utan det handlar om att förstå vilka krav nästa upphandling måste ställa.

Öppen källkod: ett strukturellt suveränitetskrav

EU:s Open Source-strategi fastslår öppen källkod som det primära verktyget för att uppfylla CADA:s högre suveränitetsnivåer. Det handlar om inspekterbarhet och kontroll.

Absolut granskningsbarhet (Art. 20)

Stängd proprietär källkod kan inte genomgå den fullständiga kodgranskning som CADA:s revision kräver. Öppen källkod är den enda ansatsen som möjliggör detta.

Interoperabilitet i EuroCloud

Öppna standarder möjliggör direkt, säker interoperabilitet utan bilaterala avtal eller leverantörsberoenden som begränsar suveräniteten.

Suveränitet genom design

CADA etablerar öppen källkod som standardverktyget för teknologiskt oberoende genom sin utformning av revisionskrav.

Ni är "anchor users"

Offentlig sektor ska driva efterfrågan. Programvara utvecklad med offentliga medel ska som huvudregel publiceras som öppen källkod.