

Remissvar till Kammarkollegiet: ”Öppen källkod med tjänster” (Dnr 23.3-14464-2025)

Till Kammarkollegiet

Vi tackar för möjligheten att bidra med synpunkter på det viktiga arbetet med ramavtalet Öppen källkod med tjänster.

Vi delar ambitionen att modernisera den offentliga sektorns digitala infrastruktur , men vill samtidigt framhålla att avtalet, i sin nuvarande utformning, riskerar att bli omodernt redan från start.

Det saknar flera avgörande komponenter, särskilt krav som rör säker mjukvaruutveckling, kompetensnivå och suveränitet, vilka i dag är centrala för att uppfylla kraven i Cyber Resilience Act (CRA), NIS 2 och Cybersäkerhetslagen.

Vi vill bidra konstruktivt. Det här svaret belyser de luckor vi ser och ger förslag på hur ramavtalet kan bli både framtidssäkert och verkligen tryggt för svensk offentlig sektor.

1. Kompetenskrav: Avtalet måste tydligt skilja på ”makers” och ”takers”

Öppen källkod är inte gratis, den bygger på aktiva gemensamma insatser. Skillnaden mellan Makers och Takers är ytterst en fråga om ansvar.

En Maker förstår koden på djupet, bidrar med uppdateringar och delar sin kunskap.

En Taker paketerar andras arbete utan att återföra något.

Det är i grunden en fråga om hållbara ekosystem samt en säkerhetsfråga: kontinuerlig sårbarhetshantering och livscykelkontroll kan bara garanteras av aktörer som bidrar till och följer utvecklingen upstream.

Förslag:

- Ställ ska-krav på att leverantörer visar dokumenterade bidrag, till exempel patchar, pull requests eller registrerade CVE:er (Säkerhetsbrister) och värdera anbud utifrån detta.
- Väg in verkligt bidrag och aktiv SBOM-rutin (Software Bill of Materials) som kriterier i anbudsutvärderingen.

Det här är inte en teknisk detalj, det handlar om att myndigheter ska kunna vända sig till leverantörer som verkligen förstår den programvara de levererar och underhåller.

2. Teknikkrav: Säkerhetshärdning av applikationer är en nödvändighet

Att driftsätta publika container-images utan egna rutiner för säkerhetshärdning är fortfarande vanligt men utgör en allvarlig risk. Detta är en tickande bomb och avtalet behöver säkra upp att rätt krav ställs för alla tjänster.

Öppen källkod måste härdas, konfigureras och säkras för att kunna användas i samhällskritiska miljöer.

Produktionscontainers ska byggas på minimala basmiljöer, köras utan root-rättigheter och omfattas av kontinuerlig säkerhetsskanning.

Många IT organisationer och leverantörer saknar denna kompetens i dag, vilket har bidragit till flera säkerhetsincidenter i Sverige.

Förslag:

- Kräv att leverantörer kan uppvisa process för containerhärdning enligt etablerad standard och värdera anbudsgivare utifrån detta
- Säkerhetsskanning och patchnivå ska rapporteras och godkännas vid varje leverans.

Säkerhetshärdning är inte ett tillägg. Det är en förutsättning för en säker molntjänst.

3. Teknikkrav: Inför krav på 12-/15-faktor-metodik

Avtalet möjliggör molntjänster men anger inga krav på hur de ska byggas. Utan detta riskerar ni att upphandla föråldrade VPS-lösningar maskerade som molntjänster, något som leder till onödig inlåsning och ökade risker.

12-faktor-metodiken (<https://12factor.net/>) är en internationell standard för säker, skalbar och portabel molnutveckling.

Den säkerställer att applikationerna är stateless, automatiskt uppdaterbara och flyttbara mellan plattformar.

Förslag:

- Inför ska-krav på efterlevnad av 12-/15-faktor-principer och dokumenterad CI/CD-pipeline med SBOM.
- Koppla kravet till livscykelkraven på kontinuerlig förbättring och patchbarhet i CRA.

En applikation utan dessa grundprinciper är som en bil utan bromsar, den går framåt tills något går fel. Det är väldigt svårt att leverera framtidssäkra tjänster med gammal teknik helt enkelt. Det riskerar att bli väldigt svårt samt dyrt att följa lagar och regler.

4. Lag- och regelkrav: Avtalet måste reflektera tvingande EU-lag

Ramavtalet behöver spegla de lagar som nu styr hela den europeiska IT-sektorn. Särskilt måste det säkerställa att levererad mjukvara uppfyller CRA:s krav på säker utveckling och livscykelkontroll, att myndighetsnära system har den tillgänglighet och incidentledning som krävs enligt NIS 2 samt att molnbaserade tjänster följer EU:s kommande suveränitetsstandard EUCS.

Förslag:

- Inför kontraktssäkrade bilagor för SBOM och vulnerability management och värdera anbud utifrån detta
- Uppdatera SLA till 24/7 övervakning för system av hög kritisk nivå.

5. Kritisk brist: Avsnitt 1.24 Behandling av personuppgifter (s. 23-24)

Detta avsnitt är kritiskt och innehåller utkastets allvarligaste brist.

Avseende: 1.24.2 Särskilt om... Publik molntjänst och proprietär programvara (s. 23)

Problem: Denna klausul är en trojansk häst för icke-suveräna tjänster. Den anger att "Standardvillkor gälla för behandling av personuppgifter".

Detta är den enskilt största risken i hela avtalet. Klausulen, som den är skriven, tillåter en leverantör att sälja en "Publik molntjänst" (t.ex. en Open Source-applikation på AWS/Azure) och hävda att AWS/Azures Standardvillkor gäller för databehandlingen. Dessa standardvillkor inkluderar medgivanden till och efterlevnad av US CLOUD Act, vilket direkt bryter mot GDPR (enligt Schrems II) och hela suveränitetsprincipen.

Förslag:

Vi avråder å det starkaste från denna text. Den urholkar alla andra säkerhets- och suveränitetsambitioner i avtalet. Klausulen bör antingen strykas helt (så att avsnitt 1.24 och ett tecknat Personuppgiftsbiträdesavtal gäller för alla tjänstetyper), eller helt skrivas om för att tydliggöra att Standardvillkor aldrig kan ha företräde.

6. Suveränitetskrav: Juridiskt ägande och EES-jurisdiktion

De nuvarande definitionerna av Privat molntjänst i upphandlingsdokumentet är enbart tekniska och saknar beskrivningar av juridisk suveränitet.

De ställer inga krav på vem som äger och driftar miljön eller vilken lagstiftning personal omfattas av.

Detta riskerar att göra tjänster underkastade utländsk lag (CLOUD Act m.fl.), trots att de marknadsförs som "privata".

EUCS (EU Cloud Services Scheme) och Schrems II-praxis kräver att känsliga data hanteras inom EES och av EES-baserad personal.

Förslag:

- Utöka definitionen av "Privat molntjänst" med villkor om EES-jurisdiktion för data och personal.
- Krav på suverän drift och revision av säker lagerplats inom Sverige/EU.

7. Verifieringskrav: reviderade ledningssystem

Många leverantörer hänvisar till "processer enligt ISO" utan att vara certifierade eller granskade. Det är väldigt lätt att med generativ AI ta fram processer som matchar krav i en upphandling. För att garantera verklig säkerhet behöver processer och certifieringar grunda sig på oberoende revision.

Förslag:

- Inför ska-krav på återkommande extern revision av ledningssystem för informationssäkerhet av ackrediterad revisor. (certifikat ej äldre än 12 månader).
- Ge poängfördel åt AI-leverantörer med reviderade ledningssystem enligt ISO 42001.

Det är skillnaden mellan att "ha en policy" och att visa att den följs i praktiken.

Sammanfattande rekommendationer

Kammarkollegiet har tagit ett viktigt initiativ, men för att ramavtalet ska ge samhället det skydd och den effektivitet som EU nu kräver, behöver fokus ligga på verifierbarhet och kompetens.

Det betyder att:

1. Ska-krav enligt CRA och NIS 2 införs.
2. Leverantörer måste visa verkliga open-source-bidrag och säkerhetsförmåga.
3. ISO-certifiering med revision vägs tydligt in.
4. Molntjänster ska följa EUCS och säker EES-jurisdiktion.

Genom dessa förändringar kan Kammarkollegiet säkerställa att Sverige blir ett föregångsland för säkra, öppna och suveräna digitala tjänster.

Vänliga hälsningar

Tomas Persson / Fabian von Tiedemann

Digitalist Open Cloud AB / Digitalist Open Tech AB

Kontaktperson

Tomas Persson, tomas.persson@digitalist.com +46706000383