Intraservice

Anna-Lena Widén-Fanto, projektledare

Göteborgs Stad

Rapport

Utredning av alternativ till tredjelands-baserade leverantörer av digitala produkter och tjänster/digital suveränitet

2026-11-12

Versionshantering

Datum	Version	Beskrivning	Ändrat av	Status
-	-	**Diarienummer:** INT-2026-00201	-	-
2026-11-06	1.0		Anna-Lena Fanto	Status
2026-11-10	2.0	Justeringar av slutord efter styrgruppsmöte mm	Anna-Lena Fanto	Status
Datum				Status

Innehåll

Utredning av alternativ till tredjelands-baserade leverantörer av digitala produkter och tjänster/digital suveränitet 1

1 Rapport 3

1.1.1 Inledning 3

1.1.2 Bakgrund och syfte 3

1.1.3 Några definitioner 3

1.2 Arbetssätt 5

1.2.1 Europeiskt perspektiv 5

1.2.2 Nya regelverk 6

1.3 Mål och effektmål 8

1.4 Vad gör andra länder 8

1.5 Nulägesanalys 9

1.5.1 Andra kommuner 10

1.6 Alternativa lösningar 11

1.6.1 Applikationer 11

1.7 Konsekvensanalys 15

1.7.2 Strategi 20

1.7.3 Rekommendation 22

1.8 Genomförande (PPS) 23

1 Rapport

Utredning av alternativ till tredjelands-baserade leverantörer av digitala produkter och tjänster/digital suveränitet

1.1.1 Inledning

Denna rapport analyserar organisationens behov av digital suveränitet och presenterar alternativa handlingsvägar samt tillhörande risker och konsekvenser. Syftet är att möjliggöra ett välgrundat beslut kring strategi och implementation.

1.1.2 Bakgrund och syfte

I och med ett mer osäkert världsläge där stora aktörer styr stora it-plattformar behöver vi som myndighet säkerställa att vi har säkra och motståndskraftiga IT-miljöer. Intraservice behöver ha en tydlig plan för hur vi formar och säkrar våra IT-miljöer på både kort och lång sikt.

På grund av ett ökat fokus på digitala beroenden, cybersäkerhet och förändrade geopolitiska förutsättningar, liksom nya och kommande regelverk inom EU, har även frågor om digital suveränitet, leveranskedjor och beroenden till internationella leverantörer under senare år aktualiserats i många organisationer och är även relevanta i kommunal verksamhet.

Frågor om Europas framtid med fokus på beroende av IT och påverkan på IT-utvecklingen har adresserats av beslutsfattare i EU.

Under maj–juni 2026 har två centrala styrdokument tillkommit – Sveriges nya molnpolicy och EU:s suveränitetspaket (EU:s "Tech Sovereignty Package") – vilka sammantaget förstärker behovet av att aktivt arbeta med frågor kopplade till digital suveränitet nu.

1.1.3 Några definitioner

1.1.3.1 Tredje land - definition

Enligt GDPR-definition för tredjeland handlar det om överföring av personuppgifter till ett land utanför EU/EES. Det kan till exempel vara när:

- dokument med personuppgifter skickas till ett tredjeland
- en leverantör har underleverantörer i ett tredjeland
- support ges från ett tredjeland och de har tillgång till dina data
- personuppgifter lagras i ett tredjeland.

1.1.3.2 Allmänna risker för tredje land

Några risker gällande tredjelandsbaserade leverantörer

- Juridisk osäkerhet (GDPR-efterlevnad): Personuppgifter är inte tillräckligt skyddade i USA, vilket gör överföring av data dit riskabel. Användningen kan i förlängningen bli olaglig.
- Amerikansk insyn (CLOUD Act): Amerikanska myndigheter kan kräva ut data från molnleverantörer utan att europeiska myndigheter eller användare informeras.
- Beroende och "lock-in": Stort beroende av ett fåtal amerikanska leverantörer gör det svårt att byta leverantör.
- Säkerhetsrisker: dataläckor, osäkra API: er och kontokapningar kan uppstå.
- Geopolitisk risk: Förändringar i USA:s politik eller agerande kan påverka driften för europeiska företag.

1.1.3.3 Digital suveränitet - definition

Digital suveränitet avser en myndighets förmåga att upprätthålla kontroll över sin data samt utöva självbestämmande över sin digitala infrastruktur. Detta utan att vara utsatt för okontrollerat inflytande från utländska myndigheter, domstolsbeslut eller privata plattformsaktörer.

Omfattning

Digital suveränitet handlar om att ha kontroll över hela det digitala ekosystemet, från tekniska system till kompetens och säkerhet. Den omfattar hela teknikstackens bredd och djup. På bredden finns informationssystem, digital arbetsplats, digitala tjänster och AI. På djupet finns applikationer, IT-plattformar, data/information, infrastruktur, nätverk och säkerhet samt resurser och personal.

I dagens globala och komplexa digitala miljö är det nästintill omöjligt att vara helt självförsörjande. Det man gör är att gradvis stärka kontrollen över prioriterade områden och göra medvetna avvägningar mellan säkerhet, kostnad och samarbeten.

Fyra kärnperspektiv inom digital suveränitet

- Kontroll: vem som äger, lagrar och behandlar data.
- Autonomi: förmågan att fatta självständiga beslut om teknik
- Motståndskraft: samhällsviktig verksamhet störs inte av externa beroenden

- Regelefterlevnad: nationell och europeisk lagstiftning kan upprätthållas i praktiken.

1.2 Arbetssätt

Ett utredningsarbete görs under perioden 2026-03-01 – 2026-12-31. Arbetet har skett i några steg.

- Steg 1 maj: **Få kunskap** om ämnet, begrepp, hur gör andra, hur ser det ut hos oss
- Steg 2 augusti: Fördjupa oss i **alternativ och konsekvenser**
- Steg 3 november: Förslag hur vi kan jobba framåt **strategiskt**, och **steg** vi kan ta.

En utredningsgrupp med olika kompentenser har arbetat med svar på dessa frågor:

1 Vad innebär tredje land och digital suveränitet

2 Vilka regelverk omfattas gällande digital suveränitet

3 Vilka risker omfattas gällande digital suveränitet

4 Hur ska vi bedöma leverantörer

5 Vilka typer av alternativa lösningar finns

6 Vilka konsekvenser kan inträffa vid införande av alternativ

7 Hur kan vi tänka strategiskt

8 Vilka steg kan vi ta?

9 Rekommendationer hur vi kan jobba vidare med frågan

Projektgruppen har deltagit på olika möten och seminarium med externa aktörer som Gartner, Sambruk, eSam, Högskola i Skövde, RISE, och även andra myndigheter och kommuner som Försäkringskassan, Skatteverket, VGR och Alingsås kommun.

Projektgruppen har också deltagit i konferenser och seminarium där andra myndigheter och kommuner har deltagit, och olika svenska och europeiska experter och myndigheter har talat.

1.2.1 Europeiskt perspektiv

En rapport om Europas framtid visar att flera europeiska länder ligger i framkant när det gäller digitalisering och tillhör världens mest digitaliserade länder. Sverige är ett av dessa länder, och stora delar av t ex jordbruk och industri är digitaliserat. Samtidigt medför detta ett omfattande beroende av externa aktörer, både vad gäller:

- IT-leverantörer (t.ex. molntjänster, mjukvara och hårdvara)
- Andra länders lagstiftning (exempelvis dataskyddsregler eller exportkontroller)
- Politiska och ekonomiska beslut som fattas utanför EU:s kontroll.

I dag sker den globala IT-utvecklingen till stor del i USA, medan Europa står för en relativt liten andel. Flera framtidsscenarier lyfter fram vikten av att Europa ökar sitt teknologiska självbestämmande genom att:

- Stärka den egna utvecklingen av ny teknik och digitala lösningar.
- Minska beroendet av utomstående aktörer för kritisk infrastruktur.
- Ta en ledande roll i att forma teknikens framtid på egna villkor.

Det krävs alltså ett strategiskt skifte för att Europa ska kunna påverka digitaliseringen i stället för att följa andras beslut.

Utifrån bland annat denna bakgrund arbetar EU-kommissionen nu fram ramverk och strategier för att stärka EU:s digitala suveränitet och säkerställa en oberoende hantering av unionens teknikstack. De ekonomiska satsningarna fokuserar på öppen källkod och tillhörande konsulttjänster, samt på kritisk infrastruktur som datahallar, AI och halvledare.

1.2.2 Nya regelverk

Nya regelverk inom området digital suveränitet har kommit under våren 2026. De tar avstamp från GDPR och NIS2 cybersäkerhetslagen.
Den nya regelverken bygger på vidare på:

- GDPR:s fokus på dataskydd och individens rättigheter, men utvidgar detta till att omfatta statens och organisationers skyldigheter att skydda digitala tillgångar.
- NIS2:s krav på cybersäkerhet för kritisk infrastruktur, men skärper kraven för offentliga aktörer och lägger större vikt vid självständig teknikförsörjning.

1.2.2.1 Svensk molnpolicy (28 maj 2026)

Bakgrund: Sveriges geopolitiska situation är allvarlig och kännetecknas av stor osäkerhet. Den snabba utvecklingen i omvärlden påverkar vår säkerhet. Som framgår av regeringens utrikesdeklaration den 18 februari 2026 måste Europa stärkas.

Några viktiga punkter i molnpolicyn är:

- Myndigheter, kommuner och regioner bör i sina projekt prioritera lösningar som möjliggör hög grad av portabilitet, det vill säga att data

och tjänster kan flyttas mellan plattformar utan onödiga tekniska eller avtalsmässiga begränsningar.

- Införande av krav på öppna standarder, tydliga och väl definierade avtal samt etablerade exit-strategier är centralt för att minska risken för leverantörsinlåsning. Förmågan att genomföra snabba och kontrollerade byten av lösningar är särskilt kritisk i krissituationer, såsom vid allvarliga geopolitiska händelser eller cybersäkerhetsincidenter, där kontinuitet och handlingsförmåga behöver säkerställas.
- Arbeta riskbaserat inför molnanvändning
  viktigt med digital suveränitet där risker är som störst
- Lösningar som innefattar molntjänster bör tillämpa ett riskbaserat arbetssätt, där beslut om arkitektur, leverantörsval och datalagring grundas på en systematisk analys av verksamhetskritiska risker.
- Särskild vikt bör läggas vid digital suveränitet i de delar av verksamheten där riskexponeringen bedöms som högst, för att säkerställa kontroll över data, efterlevnad av regelverk samt operativ kontinuitet.

1.2.2.2 EU:s "Tech Sovereignty Package" (3 juni 2026)

EU:s suveränitetspaket anger en tydlig strategisk inriktning, där ny lagstiftning förväntas träda i kraft inom cirka 18 månader. Initiativet bedöms få betydande konsekvenser för offentlig sektor, särskilt inom upphandling och IT-styrning.

- Regelverksutvecklingen kommer att få en genomgripande påverkan på offentlig upphandling, med ökade krav på efterlevnad.
- En förskjutning sker från tidigare handlingsfrihet till mer bindande rättsliga skyldigheter.
- Öppen källkod/Open source-lösningar kan komma att bli ett krav vid hantering av känslig information, i syfte att stärka kontroll och transparens.
- Krav på testbarhet och förmåga till snabba byten av leverantör eller lösning kan införas.
- Ökad tyngd läggs vid robust arkitektur, interoperabilitet och användning av öppna standarder.
- Offentliga myndigheter förväntas spela en central roll som ankarkunder i etableringen av europeiska digitala lösningar.

Dessutom innehåller paketet satsning på

- AI och europeiska moln - datahallar
- Energi för datahallar

- Halvledare

1.3 Mål och effektmål

- Projektmål:
  - Ta fram beslutsunderlag

  Effektmål:

- Ökad kontroll över data och informationsflöden
- Minskade beroenden av tredjelandslösningar
- Förmåga att snabbt byta eller ersätta lösningar (interoperabilitet)
- Ökad användning av europeiska alternativ och leverantörer
- Stärkt regelefterlevnad och juridisk kontroll

1.4 Vad gör andra länder

Länder som Frankrike, Tyskland, Österrike, Schweiz, och Nederländerna och Danmark har gjort har arbetat intensivt med frågan sedan ca 2020, några före.

Många arbetar med öppen källkod, och gör successiva förflyttningar. Danmark bygger även upp ett eget system för skolan med bland annat applikationer i öppen källkod för elever och lärare utifrån deras pedagogik, språk och behov.

Länder som Ukraina, Finland, de baltiska staterna, Polen m fl arbetar också intensivt med frågan.

Sverige har till 2026 inte gjort så mycket gällande digital suveränitet, men har nu agerat i riktning med övriga Europa. En skillnad mellan Sverige och många andra Europeiska länder är att Sverige har självständiga myndigheter, medan andra har en mer central styrning.

Ledarna i länderna, som Dirk Schröder, digitaliseringsminister i den tyska delstaten Schleswig-Holstein, anger följande argument:

- Utan kontroll har vi ingen suveränitet
- Vi vill komma bort från
  - Inlåsningseffekter
  - Lösningar som faller under lagstiftning som inte utgår från EU
  - Komplexa och dyra lösningar
- Lösningar med open source/öppen källkod är nyckeln för digital suveränitet

- Idag exporterar vi medborgarnas pengar och importerar beroende till leverantörer och andra länder
- Vi vill
  - Få tillbaka kunskap och en högre grad av innovation
  - Öppenhet ökar innovation
- Politiska beslut behövs.
- Teknikfrågan är inte nog - vi behöver skapa en kultur med öppna lösningar
  - Vi börjar ersätta till LibreOffice, nästa är Nextcloud o s v
  - Vi har sparat 15 mkr euro
- Vi måste bygga suveränitet - det är inte lätt, men det går att uppnå!

1.5 Nulägesanalys

Idag har vi, liksom de flesta kommuner i Sverige, ett stort beroende till amerikanska molnleverantörer och hårdvara från Kina och USA.

Utifrån problembilden

- Hårdvara tillverkas i USA och Kina.
- Data lagras i många system i molntjänster.
- Många plattformar och system har beroende till tredjeland.
- Förvaltningen använder huvudsakligen operativsystem, plattform och applikationer från Microsoft på förvaltningens klientdatorer.
- Förvaltningen använder även operativsystem från andra leverantörer såsom Apple och Google för sina mobila enheter.
  Förvaltningen använder även ett stort antal verksamhetsapplikationer och applikationer inom Gemensamma Tjänster där leverantörerna av dessa endast har stöd för Microsofts, Apples och Googles operativsystem.
  Datacenter och nätverksinfrastruktur levereras av VMWare och Cisco
- AI molnbaserat (t ex Co pilot utreds) och lokalt (Svea GBG tas fram).

Mindre beroende

- Vissa kritiska system har vi inte i molnlösningar.
- Vi har ett datalakehouse där vi äger vårt data (lagring hos oss).
- Vi har ett fåtal öppen källkod-lösningar med Linux som operativsystem

En genomlysning av kritiska tjänster har genomförts i syfte att kartlägga beroenden till tredje land på tjänstenivå.

Vidare pågår ett fördjupat analysarbete där beroenden till tredje land identifieras och bedöms på en mer detaljerad nivå, omfattande förmågor, tjänster, applikationer, funktioner och komponenter.
EU-kommissionen har utvecklat ett ramverk som möjliggör bedömning av digital suveränitet för specifika produkter och leverantörer.

1.5.1 Andra kommuner

Branschrapporter och statistik visar att den absoluta merparten, **över 90 procent**, använder någon form av proprietär molnsvit från Microsoft eller Google.

Några kommuner som använder öppen källkod för kontorsapplikationer helt är Alingsås, Sundsvall, Motala, Eksjö, och delvis användning av Luleå, Jönköping och Filipstad våra efterforskningar. I arbetet har vi haft samtal med Alingsås kommun, som har varit mycket tillmötesgående i att svara på våra frågor.

Leverantörer och leverantörsbedömningar

För att bedöma om en leverantör och deras lösningar ger oss tillräckligt stor digital suveränitet har EU-kommissionen tagit fram ett ramverk för kartläggning och analys (DSAF). DSAF står för Digital Sovereignty Assessment Framework (på svenska: Ramverk för bedömning av digital suveränitet)

Ramverket bygger på frågor från olika perspektiv.

Det här bedöms i ramverket DSAF:

1. Självständighet och strategisk påverkan
    1.1. Vem har kontroll över beslut och pengar?
    1.2. Är företaget anpassat efter EU:s gemensamma mål?
2. Lagar och risker med utländsk påverkan
    2.1. Följer leverantören svenska eller EU-lagar?
    2.2. Kan utländska regler och lagar påverka säkerheten?
3. Skydd och kontroll av data
    3.1. Hur säkert skyddas data och AI-tjänster?
    3.2. Används kryptering och säker lagring?
    3.3. Kan EU kontrollera tekniken själv?
4. Oberoende teknikutveckling

    4.1. Kan EU självt köra och utveckla tekniken utan hjälp från länder utanför EU?

5. Leverantörskedjan (varifrån kommer tekniken?)
    5.1. Var utvecklas och hanteras molntjänsten?
    5.2. Är leverantörskedjan öppen och motståndskraftig mot störningar?
6. Teknisk öppenhet
    6.1. Används öppna standarder, API:er och öppen källkod?
    6.2. Är tekniken transparent och oberoende?
7. Säkerhet under EU-kontroll
    7.1. Hanteras säkerheten inom EU?
    7.2. Har leverantören oberoende säkerhetscertifikat?
8. Miljö och hållbarhet
    8.1. Hur energisnål och klimatsmart är lösningen?
    8.2. Jobbar leverantören med cirkulär ekonomi och hållbarhet?

Enligt ramverket DSAF genomförs bedömningar utifrån åtta perspektiv, vilkas resultat sammanställs till en totalpoäng. En leverantör och dess IT-lösning kan erhålla mellan 0 och 4 poäng, där 4 poäng indikerar god digital suveränitet.

Idag är det tidskrävande och svårt att få svar på alla frågor, men mycket pekar mot en förenklad hantering längre fram. Några myndigheter har fått i uppdrag att underlätta arbetet för digital suveränitet av regeringen, till exempel Post- och telestyrelsen tillsammans med DIGG. AI kan också vara en möjliggörare inom detta område.

1.6 Alternativa lösningar

Alternativ 1: Nuvarande lösning
Alternativ 2: Full digital suveränitet

En kombination av dessa kommer att förekomma både kort- och långvarigt, beroende på målsättningar.

1.6.1 Applikationer

För att möta behovet av digital suveränitet, flexibilitet och kostnadseffektivitet rekommenderas en strategi baserad på färdigutvecklade komponenter i öppen källkod. Genom att kombinera mindre, specialiserade lösningar kan organisationer även skapa skräddarsydda system

Förutom att använda externa leverantörer skulle organisationen även kunna utveckla egna lösningar. Exempel på detta är:

- Mikrotjänster med anpassade gränssnitt och dedikerade databaser.
- Processbaserade lösningar kopplade till egna databaser.
- AI-drivna lösningar som skapas och tränas internt för att säkerställa kontroll över data och funktionalitet.

Datahantering

För att säkerställa digital suveränitet och säkerhet kan data lagras på flera sätt:

- I egna datahallar – full kontroll men högre kostnader.
- Hos en gemensam myndighetsdatahall i Sverige – nationell insyn och skalbarhet.
- Via företagslagring inom EU – kostnadseffektivt men kräver granskning av leverantör.
- I privat eller hybridmoln – bättre kontroll än publika moln, men privatmoln är dyrare.
- Med egen krypteringsnyckel – ökad säkerhet, men medför extra kostnader.

1.6.1.1 Riskanalys nuläge

Identifiera risker, sannolikhet, konsekvens och åtgärder.

Risker med alternativ 1: Nuvarande lösning

Nr	Nuläge	Risker med nuläge	Alternativ
1	**Hårdvara** tillverkas i USA och Kina.	Geopolitisk risk Beroende	Inga i nuläget EU-kommissionen jobbar med europeiska alternativ i EU´s tech soveriegnty package.
2	**Data** lagras i många system i molntjänster.	Juridisk osäkerhet Amerikanska insyn Beroenden och lock-in Säkerhetsrisk Geopolitisk risk	Europeiska moln Egen lagring Privat lagring Egen krypteringsnyckel
3	Förvaltningen använder huvudsakligen **operativsystem**, plattform och applikationer från Microsoft på	Juridisk osäkerhet Amerikanska insyn Beroenden och lock-in Säkerhetsrisk Geopolitisk risk	Linux

	förvaltningens klientdatorer.		
4	Förvaltningen använder även **operativsystem** från andra leverantörer såsom Apple och Google för sina mobila enheter.	Juridisk osäkerhet Amerikanska insyn Beroenden och lock-in Säkerhetsrisk Geopolitisk risk	Opendesk, ungefär som O365 (Tyskland, Frankrike, Schweiz mfl, vissa svenska kommuner) Libre Office, Colabora Online (Word, Excel, Power-point, jobba i samma fil) Nextcloud (fillagring) Open Xchange/Thunderbird (e-post, kalender) Open projekt (projekt, uppföljning) Open Talk, Element /Matrix, Jitsi (chatt, videosamtal) Frankrike: Visio (videosamtal) Icewarp Compliant Office (eSam, svenska myndigheter) Hanteras i svenska datahallar -ordbehandling -e-post, kalender -videokonferenser
5	**AI** molnbaserat (t ex Copilot utreds) och lokalt (Svea GBG tas fram).	Främmande lagstiftning och jurisdiktion Bristande kontroll över träningsdata och modeller Inlåsningseffekter leverantör	Europeiska moln - beroende av Europa Egen lagring - kapacitet i längden Öppna dataformat Textformat med Schema markup, som AI kan läsa och använda (ej docx, xlsx, vissa pdf mm)

En skillnad från att köpa färdiga lösningar av leverantörer och hur man arbetar med öppen källkod (open source) är att man ofta använder en iterativ metod där man testar och utvärderar olika verktyg för att hitta den mest optimala, kostnadseffektiva och skalbara lösningen för sina kunder.

1.6.1.2 Riskanalys alternativ

Risker med alternativ 2: Full digital suveränitet

Nr	Alternativ	Risk med alternativ	Konsekvenser med alternativ
1	Hårdvara Inga i nuläget	-	-

	EU-kommissionen jobbar med detta.		
2	Datalagring Europeiska moln Egen lagring Egen nyckel Privat lagring	Europeiska moln - beroende av Europa Egen lagring - kapacitetbrist i längden Egen nyckel - troligen fortsatt amerikansk insyn Privat lagring - troligen fortsatt amerikansk insyn	Europeiska moln - Bygga upp nätverk, avtal Eget, svenskt moln - Bygga upp nätverk, avtal Egen lagring - Se över kapacitet och skalning Egen nyckel - kostnad Privat lagring – betalar för hårdvara, mjukvara, säkerhet, underhåll mm
3	**Operativsystem** Linux	Open source produkter kan komma från USA, Kina, underleverantörer kan komma från Indien osv Ägare för open source produkter kan ha affärsintressen	
4	**Applikationer** Opendesk, ungefär som O365 (Tyskland, Frankrike, Schweiz mfl, vissa svenska kommuner) Libre Office, Colabora Online (Word, Excel, Power-point, jobba i samma fil) Nextcloud (fillagring) Open Xchange (e-post, kalender) Open projekt (projekt, uppföljning) Open Talk, Element /Matrix, Jitsi (chatt, videosamtal) Frankrike: Visio (videosamtal) Icewarp Compliant Office (eSam, svenska	Open source produkter kan komma från USA, Kina, underleverantörer kan komma från Indien osv (ca 40% är europeiskt) Ägare för open source produkter kan ha affärsintressen Community är/blir oaktivt Olika typer av licenser, olika typer av kostnader finns Kräver mera utvecklare och olika kom-petenser	Troligen ca 350 verksamhetsapplikationer och applikationer med som endast har stöd för Microsofts, Apples och Googles operativsystem.

	myndigheter) Hanteras i svenska datahallar -ordbehandling -e-post, kalender -videokonferenser		
5	**AI** Europeiska moln - beroende av Europa Egen lagring - kapacitet i längden Öppna dataformat Textformat med Schema markup, som AI kan läsa och förstå (ej docx, xlsx, vissa pdf mm) AI bygger app (Med hjälp av AI kan man som utvecklare mycket snabbt bygga enkla appar) AI istället för app (Man använder data och ber AI att göra saker) AI stöd i app (AI kan stödja applikationen att t ex snabbare hitta info, med hjälp av regelverk föreslå värden att fylla I mm)		Kan användas för information med sekretess.

1.7 Konsekvensanalys

Analysen belyser konsekvenser ur verksamhetsmässigt, ekonomiskt, tekniskt och juridiskt perspektiv.

Konsekvenserna kopplade till förflyttningen från nuläge till framtida målbild är inte av stoppande karaktär, men kräver analys, prioritering och åtgärder i det fortsatta arbetet.

1.7.1.1 Verksamhetsmässiga konsekvenser

Det föreligger en betydande risk för negativ påverkan på verksamheten vid omfattande förändringar, såsom byte av kontorsplattform (t.ex. Officeprogram) eller andra centrala verksamhetssystem. Risken ökar särskilt vid snabba genomföranden och när förändringens syfte, nyttor och arbetssätt inte är tillräckligt förankrade hos användarna.

Genomföranderisken är ofta underskattad. Plattformsskiften och större systemförändringar kräver omfattande insatser inom migrering, förändringsledning, utbildning samt anpassning av processer och arbetssätt. Konsekvenserna kan bli:

- Långa införandetider
- Störningar i den dagliga verksamheten
- Produktivitetsbortfall under övergångsperioden
- Ökad risk att målbilden inte uppnås inom beslutad tid eller budget
- Ett särskilt fokus behöver därför läggas på förändringsledning och användarstöd.

1.7.1.2 Ekonomiska konsekvenser

Initial etablering (open source-kontorssvit)

För en kommun med cirka 10 000 användare bedöms behovet för förvaltning och drift av en open source-baserad kontorssvit (t.ex. LibreOffice eller Collabora Online) uppgå till cirka 3–5 heltidstjänster (FTE).

Utöver detta tillkommer:

- Kostnader för integrationer
- Anpassningar och utveckling
- Införandestöd och utbildning

Fullskalig implementation (open source-kontorssvit)

Vid en större organisation, exempelvis cirka 55 000 användare, övergår lösningen till att bli en kritisk infrastrukturkomponent. Förvaltning och drift kräver då uppskattningsvis 8–12 heltidstjänster (FTE).

I denna skala domineras kostnadsbilden inte av programvaran i sig, utan av:

- Hög integrationskomplexitet
- Krav på robust nätverkskapacitet

- Omfattande förändringsledning och användarstöd
- Även här tillkommer betydande kostnader för integrationer, anpassningar och löpande vidareutveckling.

Minskade kostnader

Om man i samband med införande (tidigt eller senare) kan minska antalet licenser för nuvarande IT_lösningar kan man tjäna in dessa kostnader.

Idag går över 45% av kommunernas licenskostnader till bigtech-bolag som Microsoft och Google m fl.

1.7.1.3 Tekniska konsekvenser

Ur ett arkitekturperspektiv krävs en ökad kontroll över beroenden till leverantörer och komponenter utanför EU (tredje land), avseende tjänster, applikationer, funktioner och tekniska komponenter.

Detta innebär bland annat:

- Behov av att använda EU-kommissionens verktyg för bedömning av digital suveränitet
- Bedömning av befintliga och nya förmågor i IT-stacken gällande digital suveränitet
- Kartläggning och hantering av beroenden till proprietära operativsystem (uppskattningsvis ca 350 leverantörer/tillverkare)
- Hantering av ett stort antal integrationer och tillägg (add-ins)

Vidare behöver krav ställas på:

- Öppna API:er
- Möjlighet till datalagring inom egen kontroll eller inom EU
- Standardisering och interoperabilitet

1.7.1.4 AI och digital suveränitet

AI-suveränitet är en del av vår digitala suveränitet. När omvärlden förändras snabbt, tekniskt, geopolitiskt och ekonomiskt, behöver vi kunna behålla kontrollen över vår information, vårt språk och vår kunskap, så att vi kan fullgöra vårt samhällsuppdrag även när förutsättningarna ändras. Därför förordar vi lokal AI där det är möjligt och lämpligt. Det betyder inte att vi ska göra allt själva, utan att vi ska kunna välja, kombinera och byta lösningar utan att bli inlåsta hos enskilda leverantörer.

En förutsättning är att vi beskriver vår information, våra begrepp och hur de hänger ihop, så att både människor och AI kan förstå och använda dem. Kunskapen ska kunna bevaras, återanvändas och flyttas mellan system. Den får inte låsas till specifika format, verktyg eller plattformar.

AI är en möjliggörare. Den kan hjälpa oss att granska kod, utveckla applikationer och effektivisera både de verktyg vi har i dag och de vi skaffar framöver. När vi kombinerar vår egen information med AI kan vi också pröva nya arbetssätt och i vissa fall minska behovet av separata applikationer. Utgångspunkten är alltid nyttan för invånarna och verksamheten, med hänsyn till säkerhet, kvalitet och kostnader.

1.7.1.5 Juridiska konsekvenser

Förändringen medför ett ökat behov av juridisk analys och kontroller av efterlevnad, bland annat inom följande områden:

- Löpande bevakning av lagstiftning och policyutveckling inom Sverige och EU, särskilt kopplat till digital suveränitet
- Anpassning och eventuell nyteckning av ramavtal, exempelvis inom kommunkluster
- Granskning av licensvillkor för open source-programvara och communities
- Genomförande av juridiska riskbedömningar
- Uppdatering av interna regelverk och policys
- Upprättande av exitstrategier för att säkerställa handlingsfrihet vid leverantörsbyte

1.7.1.6 Informationssäkerhet konsekvenser

Informationssäkerhetsarbetet påverkas i hög grad och behöver vidareutvecklas för att möta nya krav:

- Integrering av digital suveränitet i informationsklassning
- Genomförande av olämplighetsbedömningar
- Riskanalyser kopplade till datalagring i olika molnmodeller, inklusive:
- Publika moln
- Europeiska moln
- Nationella (svenska) moln
- Privata moln
- Särskilt fokus bör läggas på:
- Åtkomstkontroll
- Kryptering och hantering av krypteringsnycklar
- Juridisk jurisdiktion och datalokalisation

1.7.1.7 Inköp och upphandling konsekvenser

Ett nytt statligt inköpssystem tas nu, där att stärka EU och den digital suveräniteten är en stor anledning till arbetet, på initiativ av den svenska regeringen. Man säger bland annat att det måste bli enklare och effektivare för kommuner, regioner och myndigheter att köpa in digitala lösningar. Samtidigt behöver det bli lättare att hitta små och medelstora europeiska företag som erbjuder dessa tjänster.

Förändringen innebär skärpta krav i upphandlingar, särskilt inom datasäkerhet, leverantörskedjor och europeisk kontroll (rådighet).

Centrala aspekter inkluderar

- Molntjänster och AI (Cloud and AI Development Act – CADA)
  Krav på att uppfylla olika suveränitetsnivåer (Union Assurance Levels) för hantering av känslig och kritisk data.
- Mervärdeskriterier
  Upphandlande myndigheter behöver i högre grad beakta ”EU Added Value” i tilldelningskriterier
- Principen om ”Open Source First” behöver tolkas och appliceras
  Ökad prioritering av lösningar baserade på öppen källkod där det är lämpligt
- Avtal med andra typer av leverantörer och andra typer av produkter och tjänster
- Eventuellt kortare avtalstider och mera fokus på exitstrategier

Sammanfattningsvis innebär detta en mer komplex upphandlingsprocess, med ökade krav på analys, dokumentation och uppföljning.

1.7.1.8 Suveränitetsnivåer

De olika suveränitetsnivåerna är enligt förslaget i CADA enligt nedan, efter remisser i respektive land och gemensam fastställs de till ca 2028.

- Nivå 1: Om uppgifter behandlas och lagras i infrastruktur som är belägen i unionen.
  Föreslagen berörd information: Ingen känslig eller kritisk information
- Nivå 2: Leverantörerna måste visa att de är oberoende av tredjeländer och att de har insyn i sin leveranskedja för programvara.
  Föreslagen berörd information: Personuppgifter, hälsouppgifter, inköp, avtal
- Nivå 3: Där leverantörerna måste ägas och kontrolleras från EU och uppfylla ytterligare kriterier, såsom personalmedborgarskap. Kommissionen kan erkänna leverantörer från tredjeländer.
  Föreslagen berörd information: Känslig sektorkritisk information

- Nivå 4: Om leverantörerna har full insyn i och kontroll över sin leveranskedja för programvara och ingen inblandning från ett tredjeland.
  Föreslagen berörd information: Försvar, mycket känslig infrastruktur, underrättelseformation

1.7.2 Strategi

Några tankar kring hur förvaltningen kan hantera frågorna på strategisk nivå.

- Leverantörer kommer att bedömas utifrån digital suveränitetsnivå och portabilitet mm.
- Förmågor/funktioner analyseras utifrån informationens känslighet (t ex konfidentialitet och tillgänglighet) och kritikaliteter (samhällskritisk, sektorkritisk, verksamhetskritisk).
- Förmågor/funktioner med känslig/kritisk information hos en leverantör med låg suveränitetsnivå övervägs utifrån olika strategier utifrån olika typer av säkerhetshot, regelefterlevnad mm.
- De olika strategierna kan vara någon av följande val:
  1. Trygg som det är - fortsätter som vanligt
  2. Bevaka - Följa dialogen och utvecklingen inom området, alternativlösningar och strategier.
  3. Plan B - Reservplan som kan implementeras på kort tid.
  4. Komplementlösning - Flera lösningar för samma funktion, där den ena lösningen är mer digitalt suverän.
  5. Exit - Befintlig lösning ersätts av annan lösning.

Förmågor kan ha flera dimensioner och kräver olika strategier beroende på tidsperspektiv
En förmåga är sällan enkelspårig – den kan bestå av flera delar, där varje del kan kräva sin egen strategi. Exempelvis kan en och samma förmåga behöva en strategi för kortsiktig hantering och en helt annan för mer långsiktig utveckling.

Kunskap som grund för beslut – men i krislägen gäller andra prioriteringar
Att fatta välgrundade beslut i normala situationer kräver att man har tillräcklig kunskap, både genom teoretisk förståelse och praktisk insikt. I krislägen, däremot, är det ofta avgörande med snabba beslut baserade på prioriteringar som kan skilja sig från det vanliga. Här handlar det mer om att agera effektivt under tidspress än att vänta på fullständig information.

1.7.2.1 Steg att ta framåt

Förslag på steg att vid ett fortsatt arbetet

- Projekt som hanterar kommunikation, omvärldsbevakning, strategi och åtgärder enligt nedan
- Dialog inom Intraservice och med Stadsledningskontoret och verksamheter i Göteborgs stad för att fatta beslut om inriktning på digital suveränitet.
- Åtgärder enligt exempel på åtgärdslista nedan
- Ta fram alternativa lösningar och testa enligt prioriterad lista enligt nedan enligt beslut.
    - I nästa steg - produktionssätta lösningar enligt beslut

1.7.2.2 Exempel på åtgärder

För att hantera digital suveränitet behöver ett antal åtgärder vidtas, såsom:

- Kontinuerlig omvärldsbevakning
  Säkerställa aktiv uppföljning av utveckling, regelverk och initiativ inom området.
- Utveckling av strategi och färdplan
  Ta fram en tydlig strategi och roadmap för införande och utveckling av digital suveränitet.
- Anpassning av styrning och kravställning
  Revidera kriterier enligt molnpolicy och EU:s suveränitetsinitiativ inom arkitektur, informationssäkerhet, juridik och inköp.
- Samverkan och erfarenhetsutbyte
  Samarbeta med Sambruk samt andra kommuner och myndigheter.
- Stärkta krav på leverantörer och datahantering
  Säkerställa API-tillgång där relevant samt möjliggöra lokal lagring av kritisk data.
- Hantering av känslig information
  Säkerställa att känslig information hanteras i digitalt suveräna lösningar, med ökad revision och tydlig spårbarhet i beslut.
- Etablering av organisation
  Säkerställa ansvar för frågan på strategisk, taktisk och operativ nivå i organisationen. Säkerställa att nödvändiga resurser allokeras i rätt tid.
- Budgetering och prioritering
  Se över prioritering i förhållande till andra initiativ samt analysera kostnadseffekter på både kort och lång sikt, inklusive potentiella besparingar och ökade investeringar.
- Ökad flexibilitet och flyttbarhet
  Bygga förmåga att snabbt kunna byta leverantör eller lösning vid behov.

- Bygg upp open source kompetens
  Kompetens att granska kod, vidareutveckla, dela, ta hand om säkerhetsfrågor, test, publicering av lösning och support, samt att använda AI som verktyg för detta.
  Öppenhet och att samarbeta med andra myndigheter innebär ett annat sätt att arbeta.

1.7.2.3 Arbete med lösningar

För att stärka den digitala självständigheten i våra IT-system föreslås följande:

- Underlag och prioritering
    - Utredningsgruppen tar fram en initial lista över IT-lösningar som ska utvärderas, baserat på befintlig kunskap om kritiska system och känslig information och leverantörens suveränitetsnivå.
- Riskanalys och strategi
    - För varje identifierad lösning genomförs en riskbedömning. Därefter fastställs en strategi med åtgärder för kort och lång sikt.
- Alternativutveckling
    - För lösningar med identifierade risker tas ersättningsförslag fram, med hänsyn till verksamhetens behov, säkerhet, suveränitet och funktionalitet.
- Prioritering och handlingsplan
    - En prioriterad lista skapas över lösningar som kräver omedelbara byten, baserat på risknivå och verksamhetsbehov.

1.7.3 Rekommendation

Vi har utrett frågan om tredjelandsberoende och digital suveränitet översiktligt och ser följande:

- Göteborgs Stad behöver en gemensam inriktning för digital suveränitet, med tydliga principer, ansvar och mandat för strategiska vägval.
- Digital suveränitet är en stadsövergripande strategisk fråga som inte kan hanteras av enskilda förvaltningar eller bolag var för sig.
- Det finns behov av ett politiskt förankrat uppdrag med tydligt utpekat ansvar för att utreda stadens samlade juridiska, tekniska, ekonomiska och verksamhetsmässiga förutsättningar samt föreslå gemensam styrning, strategiska vägval och en långsiktig färdplan.
    - Normalläge – krisläge - krigsläge
- Intraservice föreslås få ett fortsatt uppdrag att stärka stadens digitala suveränitet genom ökad rådighet över stadens informationsmängder.

1.8 Genomförande (PPS)

Nästa steg:
Förstudie, Planering, Genomförande, Avslut

Beslutspunkter

BP1 – Förstudie
BP2 – Strategibeslut
BP3 – Genomförande
BP4 – Leverans