Perspektiv på digital suveränitet

EU:s CSF (Cloud Sovereignty Framework), Sveriges första molnpolicy, EU:s CADA (Cloud and AI Development Act) & Skatteverkets RFI Molntjänster

Professor **Björn Lundell**, Ph.D.
Software Systems Research Group (SSRG)
Högskolan i Skövde
bjorn.lundell@his.se

@

Nätverk Digital suveränitet
Sambruk
28 oktober 2026

Introduktion – **Programvara** & **format** ...

- **Programvara** tillhandahålls under olika **villkor** och **licenser** som ***kan*** möjliggöra olika former av it-drift för att behandla och förvalta **digitala tillgångar** (data, dokument & andra typer av handlingar) som representeras i olika **format**
- **Format** tillhandahålls under olika **villkor** (den tekniska specifikationen av flera format har tekniska brister och många format är belastade med **standardessentiella patent**, SEP) och **licenser** som behöver anskaffas för att möjliggöra behandling och förvaltning av digitala tillgångar
- **Programvara som tjänst** (**SaaS-lösningar**) – '*Software as a Service (SaaS)*. The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure'

(NIST, 2011)

Introduktion – **Öppen programvara** (**OSS**)

- **Öppen programvara (OSS)** är en **delmängd** av all programvara
- **Öppen programvara** är programvara som tillhandahålls under **villkor** och en **licens** som uppfyller definitionen **Open Software Definition** (**OSD**) som etablerats av Open Source Initiative (https://opensource.org/)
- **All OSS utvecklas och tillhandahålls** under **eviga licenser**
- ‘For companies and their representatives **to fully appreciate the evolution of OSS projects**, it is **essential to participate in associated communities** to gain a deeper understanding of the code being developed. **Governance** and **work practices differ among OSS initiatives**, and **there is a need to engage with members of communities**, as important information may be discussed at various meetings’ (Lundell et al., 2022a)

Digital suveränitet & datasuveränitet ...

- ’Digital suveränitet definieras som förmågan hos en organisation, nation eller region att ha kontroll över och hantera sina digitala tillgångar, data och teknologiska infrastruktur på ett sätt som är skyddat från externa influenser och utländska jurisdiktionskrav.’ (FM, 2025)

- ’Datasuveränitet handlar om att säkerställa att information omfattas av det regelverk som gäller i den region där den genereras och används. Det är den mest mogna och reglerade dimensionen inom digital suveränitet, och utgör grunden för många organisationers strategier inom säkerhet, regulatorisk efterlevnad och riskhantering. I praktiken innebär datasuveränitet att organisationen har full teknisk och juridisk kontroll över var data lagras, behandlas och skyddas. Detta inkluderar inte bara primärdata, utan även metadata, loggar och faktureringsinformation – alla komponenter som kan avslöja känslig information om verksamheten.’

–’Försvarsmaktens hybrida multimolnstrategi’, Dnr. FM2024-3120:26 (FM, 2025)

Suveränitet, molnlösningar & OSS ...

- ’Operativ suveränitet innebär kontroll över drift, personal, åtkomst och support.’ (FM, 2025)
- ’Teknologisk suveränitet innebär oberoende från utländska teknologier och leverantörskedjor. Exempel på åtgärder för att skapa hög teknologisk suveränitet är att använda öppen källkod eller egenutvecklade lösningar, med portabilitet, baserade på öppna standarder och utan proprietära inlåsningseffekter. Detta innebär också att kritiska komponenter – såväl hårdvara som mjukvara – ska kunna granskas och valideras ur ett nationellt säkerhetsperspektiv.’ (FM, 2025)
- ’Suveräna moln innebär att molntjänster tillhandahålls inom en viss jurisdiktion och uppfyller krav på nationell eller platsbunden datalagring och oberoende drift. Syftet är att säkerställa att data, infrastruktur och verksamhet är fria från kontroll av externa jurisdiktioner samt skyddade från utländsk myndighetspåverkan och åtkomst.’ (FM, 2025)

Digital suveränitet & molntjänster ...

- ‘**Digital sovereignty** refers to the ability of a nation to **control** its own digital infrastructure, data, and technology, **independent of foreign influence or control**.’ (Katsikas, 2025)
- ‘It is possible to draw a distinction between “data sovereignty” and “digital sovereignty,” where “**data sovereignty**” refers to **control over data**, including through **data protection law**, **competition law**, and **national security law**. This definition would make data sovereignty a subset of digital sovereignty.’ (Chander & Sun, 2022)
- ‘The Cloud Sovereignty Framework [**CSF**] defines the European Commission’s criteria, assurance levels (SEAL), and scoring methodology for assessing the sovereignty of cloud services across strategic, legal, operational, and technological dimensions.’ (EC, 2025)

EU:s **CSF** (**Cloud Sovereignty Framework**) ...

- ‘This document defines **Sovereignty Objectives** relevant for the provision of Cloud services requested in this procedure. They draw on European initiatives such as CIGREF’s Trusted Cloud Referential v2, Gaia-X policy rules and architecture, and the European Cybersecurity Certification Framework (ENISA, NIS2, DORA). In addition, they echo lessons from national cloud sovereignty strategies (e.g., France’s “Cloud de Confiiance”, Germany’s “Souveräner Cloud”), as well as international practices in export controls, supply chain resilience, and security auditability. The result is a set of objectives that supplement security assurance requirements with sovereignty specific safeguards defining clearly what sovereignty means.’ (EC, 2025)

- Den 1 juni 2026 förtydligas CSF med en ’Implementation guidance’ (EC, 2026a)

Sveriges första molnpolicy – innehåll (1/3) ...

Syfte: ökad **säkerhet**, **effektivitet** & **innovation** *...*

- ’Syftet med denna policy för användning av molntjänster är att bidra till ökad säkerhet, effektivitet och innovation i den offentliga förvaltningen. innovation.’ *–En molnpolicy för Sverige, 28 maj 2026* (Regeringskansliet, 2026, s. 1)

Självständig bedömning & **varje myndighet är själv ansvarig** ...

- ’Varje [offentlig] aktör måste göra en självständig bedömning och är själv ansvarig för sin användning av molntjänster.’ (s. 1)

Oönskade beroenden av leverantörer utanför EU ...

- ’Amerikanska företag är marknadsledande inom molntjänster i EU. Detta medför utmaningar, såsom beroenden, risk för inlåsningseffekter och höga priser vid bristande konkurrens, men även behov av datasäkerhet och rådighet över data.’ (s. 3)

Sveriges första molnpolicy – innehåll (2/3) ...

Upphandling behöver beakta varje lands regelverk ...

- 'I samband med upphandlingar är det viktigt att offentliga aktörer beaktar att företag i vissa länder enligt respektive lands regelverk under vissa förutsättningar måste lämna ut data till sina berörda nationella myndigheter, även om dessa data hanteras och lagras utanför dessa länder.' (s. 5)

Undvik inlåsningseffekter & säkerställ dataportabilitet ...

- '[Det är] viktigt att offentliga aktörer säkerställer att det finns möjlighet att, vid behov, skyndsamt överföra data till och hantera system hos någon annan leverantör eller i egen regi. Regeringen välkomnar därför molntjänster med standarder och lösningar som främjar portabilitet, dvs. förmågan att t.ex. flytta data, funktioner eller tjänster från ett system till ett annat system, och minskar inlåsningseffekter.' (s. 7)

Sveriges första molnpolicy – innehåll (3/3) ...

Vilseledande vägledning angående OSL ...

- 'I 10 kap. 2 a § offentlighets- och sekretesslagen (2009:400) har en sekretessbrytande bestämmelse införts som möjliggör för myndigheter att lämna uppgifter som omfattas av sekretess till en enskild eller till en annan myndighet som har i uppdrag att tekniskt bearbeta eller tekniskt lagra uppgifterna för den uppgiftslämnande myndighetens räkning.' (s. 10)

Olämplig vägledning angående krav på molntjänster ...

- 'Det är viktigt att offentliga aktörer fortsatt ställer tydliga krav på leverantörer av molntjänster, bl.a. för att få klarhet kring hur data hanteras, lagras, överförs och skyddas i hela leverantörskedjan.' (s. 10)
- *Alt.:* **Inför** tilltänkt **anskaffning** av en molnlösning behöver varje offentlig aktör ställa **ändamålsenliga krav** så att de organisationer (och alla dess partners och underleverantörer, i alla led) som tillhandahåller lösningen möjliggör en lämplig behandling och förvaltning av digitala tillgångar

Förordning om utveckling av moln och AI (1/3)

Faktapromemoria avseende **CADA** (Regeringskansliet, 2026)

- ’Den 3 juni 2026 presenterade Europeiska kommissionen ett förslag till förordning om utveckling av moln och artificiell intelligens (AI).’ (s. 1)
- ’Förordningen syftar till att stärka unionens konkurrenskraft och rådighet genom att utveckla dess s.k. moln- och AI-ekosystem’ (s. 1)
- ’Moln- och AI-ekosystemet ska stärkas genom att minska EU:s strategiska beroenden inom digital infrastruktur, öka den teknologiska suveräniteten, stimulera investeringar samt stärka hela leveranskedjans kapacitet, säkerhet, anpassningsförmåga och motståndskraft.’ (s. 1)
- ’Målsättningen med den föreslagna förordningen är att stärka EU:s kapacitet, konkurrenskraft och digitala suveränitet inom moln- och AI-området. […] ett stort beroende av molntjänstleverantörer utanför EU [innebär] risker för Europas digitala suveränitet.’ (s. 3)

Förordning om utveckling av moln och AI (2/3)

- Medlemsstaterna ska ’eftersträva att minst 25 procent av upphandlingar av molntjänster och AI-system tilldelas innovativa små och medelstora företag, samt vidta åtgärder för att underlätta deras deltagande.’ (s. 7)
- ’Kommissionen föreslår åtgärder för att främja användningen av öppen källkod och öppna standarder inom EU:s moln- och AI-ekosystem. Bland annat ska offentliga aktörer uppmuntras att använda och återanvända lösningar som utvecklas och tillhandahålls som öppen källkod, dvs. programvara vars källkod är fritt tillgänglig för användning, granskning, ändring och vidaredistribution.’ (s. 9)
- ’Regeringen är positiv till ambitionen att stärka EU:s kapacitet, konkurrenskraft och digitala suveränitet inom moln- och AI-området.’ (s. 10)
- ’Regeringen delar bedömningen att Europas digitala konkurrenskraft och suveränitet behöver stärkas.’ (s. 11)

Förordning om utveckling av moln och AI (3/3)

- ’Sverige ska ha rådighet över data och system och kunna agera självständigt och i linje med europeiska värderingar och intressen, samtidigt som fördelarna med globalt samarbete med internationella partners tillvaratas utan att öka beroenden som begränsar handlingsutrymmet i framtiden.’ (s. 11)
- ’Regeringen är preliminärt positiv till ett EU-ramverk för molntjänst-leverantörer med gemensamma kriterier för olika tillitsnivåer avseende säkerhet och suveränitet.’ (s. 12)

Finansdepartementet har **remitterat CADA** den 7 juli 2027

- Svar har inkommit från 63 av de (totalt 100) utpekade remissinstanserna
- Svar har inkommit från ytterligare 10 intressenter (utanför listan)
- Totalt 73 svar finns (27 oktober 2027) publicerade på regeringens webb
  https://www.regeringen.se/remisser/2026/07/remiss-av-europeiska-kommissionens-forslag-till-forordning-om-utveckling-av-moln-och-ai-kom2026502/

Perspektiv på betydelsen av **CADA** ...

- ‘**Open source software** represents **a strategic policy response** to **vendor lock-in** and the **excessive dependence on vertically integrated non-EU providers**.’ (SWD(2026) 502 final, Part 2/2) (EC, 2026b)
- ’**Stora amerikanska aktörer**, såsom Microsoft och Google, har i sina villkor långtgående möjligheter att helt stänga av en tillhandahållen tjänst om så krävs enligt ospecificerade lagar eller för att skydda någon annan kunds intressen. Enligt Microsofts standardvillkor kan bolaget stänga av en kunds tillgång till tjänsterna om kundens användning är ”*in a way prohibited by law, regulation, governmental order or decree*”. Även AWS har långtgående möjligheter att stänga av tjänsterna vid risk för AWS eller någon tredje part.’ (Sahibli & Olsson, 2025)
- ’Vad gäller leverantörer som omfattas av amerikansk lagstiftning såsom Cloud Act och FISA 702 behöver även beaktas att de har en långtgående skyldighet att överlämna information till amerikanska myndigheter’ (FM, 2025)

Perspektiv på betydelsen av **CADA – säkerhetshot**

- ‘det största **säkerhetshotet** är Ryssland, Kina och Iran’ (Säpo, 2023)
- Enligt Säpo ’bedriver ett femtontal länder **spioneri mot [Sverige]**’ (Kristiansson, 2022)
- ‘USA bedrev **spionage** mot de nordiska länderna’ (SVK, 2021)
- ‘**92% of data** from the West is **hosted in the US**’ (WEF, 2021)
- Forskning visar att många myndigheter **underlåter att identifiera och anskaffa** alla tillämpliga **avtalsvillkor** och alla nödvändiga licenser inför tilltänkt anskaffning och användning av Microsoft 365 *och ännu färre genomför någon seriös analys av under vilka villkor den egna myndighetens uppgifter kan komma att behandlas och förvaltas vid tilltänkt användning av Microsoft 365*

Av alla undersökta myndigheter som anskaffat & använder …
… **M365 har ingen myndighet** identifierat och …

- … anskaffat alla tillämpliga **avtalsvillkor** för M365 och alla format som används
- … anskaffat alla tillämpliga **licenser** för M365 som krävs för användning
- … anskaffat alla tillämpliga **licenser** för format som krävs vid användning av M365
- … anskaffat alla tillämpliga **licenser** för format som möjliggör behandling och förvaltning av digitala tillgångar oberoende av M365
- … identifierat tillämpliga **säkerhetsrisker** (**NIL**)
- … analyserat risker avseende **patent** (**SEPs**)
- … analyserat risker avseende **upphovsrätt**
- … analyserat användning av underleverantörer (och alla dess potentiella underleverantörer, i alla nivåer) för behandling av uppgifter i alla länder utanför EU, däribland **Kina**, **Serbien** & **Förenade Arabemiraten**
- … anskaffat en tillämplig **exitstrategi** som möjliggör att användningen av M365 kan avslutas med en god förvaltning

(Lundell et al., 2021, 2022b, 2022c, 2023a, 2023b, 2025)

M365 & olämplig behandling av digitala tillgångar

- ‘In sworn testimony before a French Senate inquiry into the role of public procurement in promoting digital sovereignty, Anton Carniaux, Microsoft France’s director of public and legal affairs, was asked whether he could guarantee that French citizen data would never be transmitted to U.S. authorities without explicit French authorization. And, he replied, “No, I cannot guarantee it.”’ (Woollacott, 2025)
- Den 13 juni 2024 genomförde ‘the House Committee on Homeland Security’ en **hearing** (‘A Cascade of Security Failures: Assessing Microsoft Corporation’s Cybersecurity Shortfalls and the Implications for Homeland Security’) med ‘Microsoft President Brad Smith’ då det bl.a. ställdes frågor om **NIL**: ‘Rep. Carlos Gimenez (R-FL): Are you aware of the 2017 National Intelligence Law in China? Brad Smith: Yes, I am. [...] Rep. Carlos Gimenez (R-FL): Do you comply with this law? Brad Smith: No, we do not.’ (Miller, 2024)

Skatteverkets RFI MoIntjänster ...

- Skatteverket genomför en RFI MoIntjänster i samverkan med följande 26 myndigheter (Dnr. 8-186234-2026):
  - Arbetsmiljöverket, Centrala Studiestödsnämnden, Domstolsverket, Finansinspektionen, Folkhälsomyndigheten, Försäkringskassan, Jordbruksverket, Kronofogden, Kustbevakningen, Lantmäteriet, Livsmedelsverket, Läkemedelsverket, Länsstyrelserna, Migrationsverket, Myndigheten för digital förvaltning, Naturvårdsverket, Pensionsmyndigheten, Post- och telestyrelsen, Rättsmedicinalverket, Skolverket, Statens servicecenter, Statskontoret, Tillväxtverket, Trafikverket, Tullverket & Utbetalningsmyndigheten
- Upphandlingsdokument (daterat 4 juni 2027) baseras på (men följer endast delvis) EU:s ramverk för molnsuveränitet (CSF)
- Resultat från analyser av RFI-svar kommer redovisas den 28 april 2027 på konferensen **Konkurrens bland molnen 2027** https://www.ssrg.info/konkurrens-bland-molnen-2027/

Referenser (1/3) ...

- Chander, A. & Sun, H. (2022) Sovereignty 2.0, Vanderbilt Journal of Transnational Law, Vol. 55(2), Article 2.
- EC (2025) Cloud Sovereignty Framework, European Commission, 20 October.
- EC (2026a) Cloud Sovereignty Framework: Implementation guidance, European Commission, 1 June.
- EC (2026b) Proposal for the Cloud and AI Development Act (CADA), European Commission, 3 June.
- FM (2025) Försvarsmaktens hybrida multimolnstrategi, FM2004-3120:26, Version 1.0, Försvarsmakten, 18 december.
- Katsikas, S. K. (2025) Towards a cybersecurity-oriented research agenda for digital sovereignty, Procedia Computer Science, Vol. 254, pp. 279-288.
- Kristiansson, S. (2022) Försvaret av den svagaste länken, In Liljeberg, J. & Oksanen, P. (Eds.) Sveket mot cybersäkerheten, Fores, Stockholm, ISBN: 978-91-87379-87-1.
- Lundell, B., Butler, S., Fischer, T., Gamalielsson, J., Brax, C., Feist, J., Gustavsson, T., Katz, A., Kvarnström, B., Lönroth, E. & Mattsson, A. (2022a) Effective Strategies for Using Open Source Software and Open Standards in Organizational Contexts – Experiences From the Primary and Secondary Software Sectors, IEEE Software, Vol. 39(1): 84-92.
- Lundell, B., Gamalielsson, J. & Katz, A. (2023a) Implementing the HEVC standard in software: Challenges and Recommendations for organisations planning development and deployment of software, Journal of Standardisation, Vol. 2.

Referenser (2/3) ...

- Lundell, B., Gamalielsson, J., Katz, A. & Lindroth, M. (2022b) Use of Commercial SaaS Solutions in Swedish Public Sector Organisations under Unknown Contract Terms, In Janssen, M. et al. (Eds.) EGOV 2022: Electronic Government, Lecture Notes in Computer Science, Vol 13391, Springer, Cham, pp. 73-92.
- Lundell, B., Gamalielsson, J., Katz, A. & Lindroth, M. (2022c) Data Processing and Maintenance in Different Jurisdictions When Using a SaaS Solution in a Public Sector Organisation, JeDEM – eJournal of eDemocracy and Open Government, Vol. 14(2), pp. 214–234.
- Lundell, B., Gamalielsson, J., Katz, A. & Lindroth, M. (2023b) Avoiding lock-in effects through obtaining all necessary licences before use of a SaaS solution in a public sector organisation: a case study, European Journal of Law and Technology, Vol. 14(1).
- Lundell, B., Lindroth, M., Gamalielsson, J., Katz, A., Brax, C., Persson, T., Mattsson, A., Gustavsson, T., Feist, J. & Öberg, J. (2025) Half a step behind – bulk disclosure of confidential data in third-party GenAI solutions under the Swedish Public Access to Information and Secrecy Act, Digital Government: Research and Practice, Vol. 6(2), Article No. 25, pp. 1-9.
- Miller, G. (2024) TRANSCRIPT: House Committee Hearing to Assess Microsoft's Cybersecurity Shortfalls, Tech Policy Press, 15 June.
- NIST (2011) The NIST Definition of Cloud Computing, Special Publication 800-145, National Institute of Standards and Technology, Gaithersburg, September.
- Regeringskansliet (2026) Förordning om utveckling av moln och AI, Faktapromemoria, FPM-nummer: 99, Finansdepartementet, Regeringskansliet, 8 juli.

Referenser (3/3) ...

- Sahibli, T. & Olsson, E. (2025) ”It-avtal en risk för svensk beredskap”, Svenska Dagbladet, 5 mars.
- SVK (2021) Öppen antagonistisk hotbild för elförsörjningen, Ärendenr: 2021/4367, Svenska kraftnät, Sundbyberg, 1 november.
- Säpo (2023) Säkerhetspolisen 2022 – 2023, Säkerhetspolisen, ISBN: 978-91-86661-23-6.
- WEF (2021) What is digital sovereignty and why is Europe so interested in it?, World Economic Forum, 15 March. https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/
- Woollacott, E. (2025) Microsoft Can’t Keep EU Data Safe From US Authorities, Forbes, 22 July.

Fler relaterade källhänvisningar finns i referenslistan som publicerats från konferensen Hållbar digitalisering 2026: https://www.ssrg.info/hallbar-digitalisering-2026-referenser/

Välkommen till konferensen **Konkurrens bland molnen 2027** som arrangeras onsdagen den **28 april 2027**: https://www.ssrg.info/konkurrens-bland-molnen-2027/
https://www.his.se/mot-hogskolan/aktiviteter/kalender/2027/konkurrens-bland-molnen-2027/

Välkommen till konferensen **Hållbar digitalisering 2027** som arrangeras (online) torsdagen den **19 augusti 2027**: https://www.ssrg.info/hd2027/
https://www.his.se/mot-hogskolan/aktiviteter/kalender/2027/hallbar-digitalisering-2027/