

Finansdepartementet
103 33 Stockholm
fi.remissvar@regeringskansliet.se

Yttrande avseende remittering av Europeiska kommissionens förslag till förordning om utveckling av moln och AI: KOM(2026) 502

Sammanfattning

Detta yttrande avser Europeiska kommissionens förslag till förordning¹ om utveckling av moln och AI som presenterats för en stärkt suveränitet och konkurrenskraft inom EU². Yttrandet redovisar ett antal synpunkter och *rekommendationer* utifrån en analys av innehållet i förslaget till förordning (nedan refererat CADA). Den 3 juni 2026 publiceras CADA som utgör ett, av fyra³ relaterade, initiativ för att stärka teknologisk suveränitet⁴ inom EU⁵. Det är ett mycket omfattande paket av policy och regelverk som kan få stor betydelse för alla individer, organisationer och nationer som agerar inom EU. Relaterat CADA är EU:s strategi för fri och öppen programvara (FOSS⁶) viktig.

CADA presenteras i fem dokument⁷ som sammantaget omfattar 514 sidor. Relaterat det nu remitterade förslaget till förordning, CADA, har Regeringskansliet den 8 juli 2026 publicerat en faktapromemoria⁸ som presenterar en sammanfattning av CADA. Denna faktapromemoria (2025/26:FPM99) innehåller även en redovisning av Regeringens bedömningar och uppfattningar om innehållet i CADA. Det kan noteras att i denna promemoria används begreppet 'rådighet', istället för digital suveränitet, för att beskriva syftet med CADA: 'Förordningen syftar till att stärka unionens konkurrenskraft och rådighet genom att utveckla dess s.k. moln- och AI-ekosystem, dvs. EU:s samlade tekniska, industriella och institutionella miljö för att utveckla, driva och använda molntjänster och AI.'

Detta yttrande fokuserar på ett *urval* aspekter som behandlats i CADA. Specifikt behandlar detta yttrande: 1) CADA:s syfte och innehåll; 2) CADA:s problembeskrivning och ramverk för molnsuveränitet; 3) CADA och myndigheters agerande vid upphandling.

1 'Proposal for the Cloud and AI Development Act (CADA)' (EC, 2026a)

2 'The Cloud and AI Development Act will strengthen Europe's sovereignty and competitiveness in the cloud and AI ecosystem.' (EC, 2026b)

3 'Communication on European Tech Sovereignty, accompanied by an EU Open Source Strategy' (EC, 2026c)

4 'Tech sovereignty is Europe's ability to act independently in the digital world by developing and controlling key technologies, data, and infrastructure, while reducing reliance on non-EU providers.' (EC, 2026d)

5 'The European Commission today presented the European Technological Sovereignty Package, a set of measures to strengthen Europe's capacity in semiconductors, artificial intelligence (AI), cloud and open source.' (EC, 2026e)

6 FOSS (eng. Free and Open Source Software) är en delmängd av all programvara (EC, 2026g).

7 '1. COM(2026) 502 - Proposal Regulation Cloud and AI Development Act (CADA)', '2. COM(2026) 502 - Proposal Regulation Cloud and AI Development Act (CADA) Annexes', '3. SWD(2026) 502 - Impact Assessment (Part 1)', '4. SWD(2026) 502 - Impact Assessment (Part 2)', '5. SWD(2026) 502 - Summary of the Impact Assessment' (EC, 2026a)

8 (Regeringskansliet, 2026)

Bakgrund

Om detta yttrande:

Detta yttrande har utformats av professor Björn Lundell (Ph.D.) vid Högskolan i Skövde. De synpunkter och rekommendationer som framförs i detta yttrande baseras på erfarenheter och resultat från flera års forskning inom området för föreslagen förordning. Yttrandet ger uttryck för den enskilde forskarens egen uppfattning och ska därför inte uppfattas som ett ställningstagande från lärosätet (Högskolan i Skövde).

Ett urval källor redovisas i en källförteckning till detta yttrande. Källförteckningen inkluderar även ett antal källor som refererar tidigare lämnade yttranden och rapporter som författaren tidigare bidragit med, vilket inkluderar: rapporter från relaterade utredningar som professor Lundell genomfört och bidragit till på uppdrag av svenska myndigheter (specifikt Statens inköpscentral vid Kammarkollegiet⁹, Konkurrensverket¹⁰ & Myndigheten för digital förvaltning: DIGG¹¹); yttranden till relaterade utredningar som genomförts i Sverige (däribland till: SOU 2021:1¹², Riksarkivets författningsförslag¹³, SOU 2021:97¹⁴ & SOU 2025:12¹⁵); samt yttranden till öppna konsultationer som genomförs inom EU (specifikt relaterat: analyser av programvarusystem (som identifierat allvarliga brister i ENISA's utkast¹⁶ till SBOMs¹⁷), offentlig upphandling¹⁸, interoperabilitet¹⁹, standardisering²⁰ och patent som belastar standarder²¹, s.k. SEPs).

Dessutom har professor Lundell, såväl inom Sverige²² och inom EU²³, bidragit med yttranden och forskningsresultat²⁴ som behandlar innehållet i lagförslag till Cyberresiliensförordningen (CRA).

Om författaren till detta yttrande:

Författaren till detta yttrande (*nedan författaren*) heter Björn Lundell och är professor i datavetenskap vid Högskolan i Skövde där han leder forskningen inom Software Systems Research Group (SSRG). Under lång tid har författaren, tillsammans med kollegor och flera samverkanspartners, genomfört forskning som behandlat flera frågeställningar som i högsta grad berör föreslagen förordning (CADA). Detta inkluderar studier som genomförts inom ramen för olika uppdrag i samverkan med svenska myndigheter, däribland Statens inköpscentral vid Kammarkollegiet, Konkurrensverket och Myndigheten för digital förvaltning (DIGG).

Inom ramen för ett stort antal internationella och nationella forskningsprojekt har författaren, tillsammans med kollegor och samverkanspartners, genomfört ett stort antal studier som behandlat en rad (tekniska, socio-tekniska, juridiska och samhällsrelaterade) frågeställningar avseende hur olika intressenter (enskilda individer, företag, offentliga organisationer, nationer och EU) styr (genom

9 (NPS, 2016)

10 (Lundell et al., 2016)

11 (Lundell, 2020)

12 (Lundell, 2021)

13 (Lundell, 2022a)

14 (Lundell, 2022b)

15 (Lundell, 2025a)

16 (Georgiadou et al., 2025)

17 (Lundell, 2026a)

18 (Lundell, 2026b)

19 (Lundell, 2026c)

20 (Lundell, 2025b)

21 (Lundell, 2022c, 2023a; Lundell et al., 2015, 2019, 2023a)

22 (Lundell, 2023b, 2023c)

23 (Lundell, 2024a, 2024b)

24 (Lundell & Lindroth, 2026/27)

lagstiftning, föreskrifter, policy, rekommendationer, etc.) samt i praktiken agerar då programvarusystem anskaffas, utvecklas, förvaltas och används. De studier som genomförts inom ramen för denna forskning har haft betydande inverkan på kunskapsutvecklingen inom området och samhället i stort.

Den forskning som SSRG bedriver har under flera decennier fokuserat på tre övergripande forskningsutmaningar: inlåsnings effekter, interoperabilitet samt långa livscykler för system och relaterade digitala tillgångar (eng. 'digital assets'). Forskningen har (länge) haft betydande fokus på förutsättningar för utveckling och användning av standarder och FOSS²⁵ (Free and Open Source Software), samt frågeställningar avseende under vilka villkor olika typer av IKT-standarder kan implementeras av programvaruprojekt som utvecklar och tillhandahåller FOSS. Exempelvis genomförde författaren till detta yttrande flera analyser av industriföretags engagemang med FOSS under genomförandet av EU FP6-projektet Calibre (2004-2006). Därefter har författaren, tillsammans med kollegor och samverkanspartners, genomfört omfattande forskning som direkt eller indirekt berör CADA inom ramen för flera internationella och nationella forskningsprojekt.

Vetenskapligt granskade resultat från denna forskning har publicerats och presenterats i en rad olika fora. Flera genomförda studier inkluderar rekommendationer för hur företag, myndigheter och samhället i stort kan (och bör) strategiskt engagera sig med upphandling, utveckling och it-drift av programvarusystem, specifikt relaterat: anskaffning och användning av molntjänster, engagemang med FOSS-projekt och IKT-standarder, samt FOSS-projekts användning och implementation av IKT-standarder. Utöver att genomförd forskning regelbundet publiceras i relevanta vetenskapliga fora kommuniceras dessutom resultat till det omgivande samhället genom nyheter, öppna seminarier och konferenser som riktar sig till det omgivande samhället. Genomförda konferenser inkluderar den årligen återkommande konferensen Hållbar digitalisering²⁶ som, med såväl internationellt som nationellt deltagande, arrangerats sedan 2019 med olika fokus. Konferenser inkluderar även andra internationella konferenser, däribland konferensen 'Öppen programvara i en föränderlig värld: Hur upprätthålls och accelereras affärsmässiga och samhällsliga effekter samtidigt som aktuella utmaningar hanteras?'²⁷ som genomfördes med flera internationella experter den 16 april 2024²⁸. Vidare behandlades exempelvis flera av de frågeställningar som berörs av CADA under konferensen 'Konkurrens bland molnen' som genomfördes den 29 april 2026²⁹. Konferensen behandlade konkurrenshinder och förutsättningarna för konkurrens på it-marknaden, med särskilt fokus på organisationers anskaffning och användning av molnlösningar³⁰.

25 FOSS (Free and Open Source Software) är en delmängd av all programvara. FOSS (på svenska 'fri och öppen programvara') är programvara som tillhandahålls under villkor och licenser som uppfyller definitionen 'the Free Software Definition' (FSD, 2026) och som uppfyller definitionen 'the Open Source Definition' (OSD, 2026), se vidare Lundell (2020). Fri programvara (på engelska 'Free Software', vanligen förkortat 'FS') är programvara som tillhandahålls under villkor och licenser som uppfyller 'the Free Software Definition' (FSD, 2026). Öppen programvara (på engelska 'Open Source Software', vanligen förkortat OSS) är programvara som tillhandahålls under villkor och licenser som uppfyller 'the Open Source Definition' (OSD, 2026). FOSS har länge använts av forskare som en inkluderande term för FS (Free Software) och OSS (Open Source Software) och under 2024 antog EU förordningen om cyberresiliens (Cyber Resilience Act, CRA) som påverkar förutsättningarna för all programvara och det finns särskilda regler som påverkar förutsättningarna för FOSS (EU, 2024a, 2024b).

26 För en översikt av de konferenser (Hållbar digitalisering) som genomförts under 2020, 2021, 2022, 2023, 2024, 2025 och 2026 se: <https://www.ssr.info/hd2020/>, <https://www.ssr.info/hd2021/>, <https://www.ssr.info/hd2022/>, <https://www.ssr.info/hd2023/>, <https://www.ssr.info/hd2024/>, <https://www.ssr.info/hd2025/> och <https://www.ssr.info/hd2026/>

27 Eng. 'Open Source in a changing world: How to sustain and accelerate business and societal impact while navigating contemporary challenges?' (<https://www.ssr.info/oppen-programvara-i-en-foranderlig-varld/>)

28 Under denna konferens (och en relaterad workshop som genomfördes den 15 april 2024) behandlades flera aktuella frågeställningar (som relaterar CADA) avseende FOSS under flera paneldiskussioner, en posterutställning och fyra inbjudna presentationer som gavs av internationella experter.

29 <https://www.ssr.info/konkurrens-bland-molnen/>

1) CADA:s syfte och innehåll

CADA syftar till att stärka EU:s konkurrenskraft och digitala suveränitet vilket författaren ser som mycket vällovligt. Författaren delar Europeiska kommissionens bedömning angående vikten av att stärka EU:s konkurrenskraft och digitala suveränitet.

Regeringens faktagrunder³¹ använder begreppet *rådighet* (istället för suveränitet) för att betona vikten av att Sverige som nation ska ha kontroll på såväl data som system enligt följande: *'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.'* Av denna formulering framgår även vikten av att tillvarata *'fördelarna med globalt samarbete med internationella partners'* samtidigt som Sverige ska kunna agera självständigt och undvika (oönskade) beroenden som *'begränsar handlingsutrymmet i framtiden'*.

Författaren delar Regeringens bedömning angående vikten av att *Sverige ska ha rådighet över data och system och kunna agera självständigt i linje med europeiska värderingar och intressen*, men med tillägget att det för Sverige och svenska organisationer är av yttersta vikt att ha rådighet över alla digitala tillgångar³² i den betydelse som preciseras av EU:s dataförordning³³ (d.v.s. det krävs rådighet över alla digitala tillgångar och räcker inte med endast rådighet över delmängden data).

Ett mycket tydligt exempel på framgångsrikt globalt samarbete som behöver upprätthållas, stimuleras och (på olika sätt) stärkas är den globala samverkan som under flera decennier skett (och sker) genom programvaruprojekt som utvecklar och tillhandahåller FOSS. Av CADA framgår tydligt att Europeiska kommissionen ser betydelsen av FOSS och det finns förslag för att främja användningen av FOSS som en viktig del av strategin för att stärka EU:s konkurrenskraft och digitala suveränitet. Detta inkluderar att offentliga aktörer ska uppmuntras att använda och återanvända lösningar som utvecklas och tillhandahålls som FOSS³⁴.

Författarens **bedömning** är att det inom EU finns ett betydande behov av strategiska engagemang med utveckling och användning av FOSS och gör bedömningen att sådana engagemang med FOSS utgör nödvändiga, men inte tillräckliga, förutsättningar för stärkt konkurrenskraft och digital suveränitet inom EU. Det kan noteras att CADA betonar vikten av FOSS för att möjliggöra en strategi som undviker leverantörsinlåsning och olämpliga beroenden av leverantörer som inte är baserade inom EU³⁵. Det finns även goda exempel och intressanta erfarenheter från strategiskt engagemang med FOSS inom enskilda EU-länder³⁶.

30 Konferensen behandlade bland annat 'Marknadsföring som efterlevnadsmodell för molntjänster' (av André Catry, https://www.ssrp.info/wp-content/uploads/2026/04/Andre-Catry_Marknadsforing-som-efterlevnadsmodell-for-molntjanster.pdf) och under rubriken 'Open Source – Key to Digital Sovereignty and Economic Growth in Europe' gavs (av Dirk Schrödter, https://www.ssrp.info/konkurrens-bland-molnen_schrodter/) en presentation om hur digital suveränitet förutsätter öppen programvara (vilket starkt relaterar CADA).

31 (Regeringskansliet, 2026)

32 '(83) Digitala tillgångar avser element i digitalt format för vilka kunden har nyttjanderätten, inbegripet applikationer och metadata som rör konfiguration av inställningar, säkerhet och förvaltning av åtkomst- och kontrollrättigheter, och andra element såsom uttryck för virtualiseringsteknik, inbegripet virtuella maskiner och behållare. Digitala tillgångar kan överföras om kunden har nyttjanderätt oberoende av avtalsförhållandet med den databehandlingstjänst som kunden avser att byta från. Dessa andra element är avgörande för en effektiv användning av kundens data och applikationer i miljön hos destinationsleverantören av databehandlingstjänster.' (EU, 2023)

33 (EU, 2023)

34 (EC, 2026a)

35 '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, 2026a)

36 Se exempelvis erfarenheter från Tyskland (State Chancellery, 2024).

Författarens **bedömning** av CADA (och av Regeringens faktapromemoria om CADA) är att det hade varit önskvärt med en betydligt mer ingående problematisering av dagens situation där många myndigheter, genom olämpliga ageranden, orsakar inlåsning och konkurrenshinder som motverkar möjligheterna att åstadkomma stärkt konkurrenskraft och digital suveränitet inom EU.

Författaren ser det som mycket angeläget att CADA, på ett mer ingående sätt, kompletteras med redogörelser för nödvändiga åtgärder som ger stärkta förutsättningar för etablering och upprätthållande av digital suveränitet och rådighet över system och (alla typer av) digitala tillgångar.

Författaren **rekommenderar** att CADA (samt relaterade förordningar och regelverk), däribland regelverk som ger förutsättningar för offentlig upphandling, preciseras och kompletteras med justerade regelverk som påverkar enskilda individers och organisationers möjligheter att strategiskt engagera sig med programvaruprojekt som tillhandahåller FOSS. Författaren ser det som mycket angeläget att det preciseras åtgärder som undanröjer de hinder som i dag motverkar etablering och upprätthållande av digital suveränitet och rådighet över system och (alla typer av) digitala tillgångar.

2) CADA:s problembeskrivning och ramverk för molnsuveränitet

CADA presenterar en gedigen problembeskrivning som redovisar flera aspekter som behöver beaktas inför tilltänkt anskaffning och användning av olika molnlösningar.

Forskning visar att många myndigheter underlåter att identifiera och anskaffa alla tillämpliga avtalsvillkor och alla nödvändiga licenser inför tilltänkt anskaffning och användning av olika molnlösningar. Exempelvis visar forskning att många myndigheter anskaffar Microsoft 365 utan att ha identifierat alla tillämpliga avtalsvillkor, utan att ha upprättat någon ändamålsenligt strategi för exit och utan att ha genomfört någon seriös analys av under vilka villkor den egna myndighetens uppgifter kan komma att behandlas och förvaltas (av leverantörer och underleverantörer) vid tilltänkt användning av Microsoft 365. Varje sådan anskaffning orsakar risker och föranleder en ändamålsenlig analys inför tilltänkt anskaffning av en molnlösning.

Författarens **bedömning** är att CADA redovisar en problembeskrivning som bör föranleda ett förändrat beteende bland många beslutsfattare inom myndigheter i Sverige.

Europeiska kommissionen publicerade i oktober 2025 ett ramverk³⁷ för molnsuveränitet³⁸ (nedan refererat *CSF*) som är relevant för tillhandahållande av molntjänster. Ramverket preciserar molnsuveränitet³⁹ i åtta definierade mål⁴⁰ och preciserar nivåer⁴¹ av suveränitet⁴² med en formel för att kvantitativt mäta nivå av suveränitet. Fem nivåer preciseras där nivå 4 är den högsta nivån av suveränitet och nivå 0 utgör avsaknad av suveränitet (d.v.s. 'ingen suveränitet'). Europeiska

37 '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)

38 'Cloud Sovereignty Framework' (EC, 2025)

39 'Sovereignty Objectives' (EC, 2025)

40 De åtta målen för molnsuveränitet är: SOV-1: Strategic Sovereignty; SOV-2: Legal & Jurisdictional Sovereignty; SOV-3: Data & AI Sovereignty; SOV-4: Operational Sovereignty; SOV-5: Supply Chain Sovereignty; SOV-6: Technology Sovereignty; SOV-7: Security & Compliance Sovereignty & SOV-7: Environmental Sovereignty (EC, 2025)

41 Ramverket preciserar nivå 0, 1, 2, 3 och 4 (där nivå 1-4 utgör olika nivåer av suveränitet, där nivå 4 är den högsta nivån och där nivå 0 utgör 'ingen suveränitet'). (EC, 2025)

42 'Sovereignty Effectiveness Assurance Levels (SEAL)' (EC, 2025)

kommissionen publicerade den 1 juni 2026 en vägledning⁴³ som förtydligar CSF. För var och en av de åtta definierade målen i CSF presenteras ett antal kriterier som preciserar respektive mål.

Författarens **bedömning** är att de åtta definierade målen för suveränitet som presenteras i CSF är relevanta och flera är särskilt viktiga att beakta. Det finns dock flera oklarheter kring utformning (exempelvis huruvida viktiga aspekter saknas) och hur tillämpning av ramverket ska ske (exempelvis avseende på vilket sätt myndigheter själva kommer att kunna värdera påståenden från tilltänkta leverantörer) som behöver analyseras närmare. Vidare finns det anledning att ingående analysera hur den värdering av uppfyllelse (med den kvantitativa modell) som CSF innehåller fungerar med syftet att identifiera och utveckla förbättrade förslag på modeller för värderingar.

I Sverige har Skatteverket och flera andra myndigheter genomfört en RFI med utgångspunkt i ramverket, men tyvärr beaktade denna RFI inte den då publicerade precisering som publicerades strax innan (den 1 juni 2026). Inom EU har ramverket använts under 2026 och det finns behov av ingående analyser av denna användning.

Författaren **rekommenderar** att ramverket analyseras närmare utifrån dessa (och andra) aspekter.

3) CADA och myndigheters agerande vid upphandling

CADA utgör ett komplement till regelverk för offentlig upphandling där målet är att underlätta anskaffning av molntjänster⁴⁴. Enligt CADA ska myndigheter vid upphandling av molntjänster och AI-system exempelvis beakta europeiska värden som en del av utvärderingen. CADA redogör för flera problem⁴⁵ som orsakar olämplig behandling av digitala tillgångar genom användning av molntjänster under okända villkor. Exempelvis orsakar användning av globalt tillhandahållna molntjänster från Microsoft olämplig behandling av digitala tillgångar i, potentiellt mycket, problematiska jurisdiktioner⁴⁶.

Däremot saknar CADA redogörelser för olika nationella regelverk, däribland OSL (Offentlighets- och sekretesslag (2009:400)), som i Sverige påverkar myndigheters förutsättningar för användning av Microsoft 365⁴⁷ och flera andra molnlösningar som används under okända och olämpliga villkor. Vidare vore det önskvärt om CADA, än tydligare, skulle uppmärksammat potentiella konsekvenser för organisationer som ingår avtal för användning av globalt tillhandahållna molnlösningar. Exempelvis har två svenska jurister givit uttryck för risker och potentiella problem som följer av att ingå avtal med Microsoft och Google⁴⁸.

43 'Cloud Sovereignty Framework: Implementation guidance' (EC, 2026f)

44 (EC, 2026a)

45 Exempelvis framkom följande uppgifter från en representant för Microsoft under ett hörande i Frankrikes senat: 'In a sworn testimony before the French Senate, a representative of Microsoft affirmed that the company could not guarantee that French data would not be transmitted to US authorities, even in the absence of explicit authorisation. Any data managed by a US-headquartered provider or its subsidiaries is potentially exposed, including sensitive business information, intellectual property, and personal data of EU citizens.' (SWD(2026) 502 final, Part 1/2) (EC, 2026a)

46 'FISA Section 702 permits the US government to conduct targeted surveillance of foreign persons located outside the US to acquire foreign intelligence information. Under Section 702, the US Attorney General and Director of National Intelligence may issue directives compelling US electronic communication service providers to provide such information, including via bulk data collection.' (SWD(2026) 502 final, Part 1/2) (EC, 2026a); (Lundell, 2026d; Lundell et al., 2022a, 2022b, 2023a, 2023b, 2025)

47 'all previous experience and research show unequivocally that it is not even possible to acquire all information concerning traditional cloud-based solutions necessary to assess "appropriateness" within the context of OSL Ch 10 Section 2 a' (Lundell et al., 2025)

Författarens **bedömning** är att det är önskvärt att CADA kompletteras med en analys av vissa nationella regelverk och bedömningar avseende dataskydd⁴⁹ och säkerhet⁵⁰. Vidare vore det önskvärt om CADA betonar vikten av att myndigheter, inför anskaffning och användning av olika lösningar, genomför analyser som säkerställer att påståenden om viss teknisk funktion faktiskt stämmer överens med faktiskt tillhandahållen funktion eftersom leverantörers utfästelser om teknisk funktion kan vara vilseledande eller direkt felaktiga⁵¹.

Forskning visar att många myndigheter anskaffar och använder molntjänster utan att någon föregående konkurrensutsatt upphandling genomförts och utan att myndigheten beaktat några frågeställningar om digital suveränitet och datasuveränitet inför anskaffning av molntjänster för att behandla och förvalta myndighetens digitala tillgångar. Betydelsen av att svenska myndigheter upprätthåller datasuveränitet har exempelvis betonats av Försvarmakten⁵² i Sverige och det vore lämpligt att frågeställningar om datasuveränitet behandlas av CADA.

Författaren **rekommenderar** att varje myndighet, inför tilltänkt anskaffning av en molnlösning, behöver formulera 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 myndighetens digitala tillgångar.

Professor Björn Lundell, Ph.D.
Software Systems Research Group
Högskolan i Skövde

E-post: bjorn.lundell@his.se

48 '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)

49 'The fact that public bodies have actually no control over the engagement of processors and sub-processors makes it difficult for them to ensure that the processing is compliant with the provisions of the GDPR, especially regarding transfers to third countries. However, it must be emphasised that this difficulty does not, in itself, exonerate the controller from its responsibilities in the processing.' (EDPB, 2023)

50 Exempelvis har Säpo rapporterat att 'ett femtontal länder' bedriver spioneri mot Sverige (Säpo, 2023) och Svenska kraftnät har rapporterat att 'USA bedrev spionage mot de nordiska länderna' (SVK, 2021).

51 (Hertogh et al., 2026)

52 '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.' (FM, 2025)

Källhänvisningar

EC (2025) Cloud Sovereignty Framework, Version 1.2.1, European Commission, October.
https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?filename=Cloud-Sovereignty-Framework.pdf

EC (2026a) Proposal for the Cloud and AI Development Act (CADA), Policy and Legislation, European Commission, 3 June. <https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada>

EC (2026b) Cloud and AI Development Act, European Commission, 3 June. <https://digital-strategy.ec.europa.eu/en/policies/cloud-and-ai-development-act>

EC (2026c) Communication on European Tech Sovereignty, accompanied by an EU Open Source Strategy, European Commission, 3 June.
<https://digital-strategy.ec.europa.eu/en/library/communication-european-tech-sovereignty-accompanied-eu-open-source-strategy>

EC (2026d) Strengthening Europe's Tech Sovereignty, European Commission, 3 June.
<https://digital-strategy.ec.europa.eu/en/policies/eu-tech-sovereignty>

EC (2026e) Commission proposes tech sovereignty package to strengthen Europe's digital autonomy and resilience, Press release, European Commission, 3 June.
https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1187

EC (2026f) Cloud Sovereignty Framework: Implementation guidance, European Commission, 1 June. https://commission.europa.eu/document/download/2ad80a48-166f-4c77-a513-80c53ca2a128_en

EC (2026g) The EU Open Source Strategy, European Commission, 3 June.
<https://digital-strategy.ec.europa.eu/en/policies/open-source-strategy>

EDPB (2023) 2022 Coordinated Enforcement Action: Use of cloud-based services by the public sector, European Data Protection Board, Adopted on 17 January.
https://edpb.europa.eu/system/files/2023-01/edpb_20230118_cef_cloud-basedservices_publicsector_en.pdf

EU (2023) Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen). https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=OJ:L_202302854

EU (2024a) Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), Official Journal of the European Union, 20 November.

EU (2024b) Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen), Europeiska unionens officiella tidning, 20 november.

FM (2025) Försvarsmaktens hybrida multimolnstrategi, FM2004-3120:26, Version 1.0, Försvarsmakten, 18 december.

FSD (2026) The Free Software Definition, The Free Software Foundation.

<https://www.gnu.org/philosophy/free-sw.en.html#fs-definition>

Georgiadou, I., Gavrilă, R., Łokietek, T., Sroka, K. & Czyż, A. (2025) SBOM Landscape Analysis: Towards an Implementation Guide, European Union Agency for Cybersecurity, ENISA, Draft 1.2, December. https://www.enisa.europa.eu/sites/default/files/2025-12/SBOM%20Analysis%20-%20Towards%20an%20Implementation%20Guide_v1.20-Published.pdf

Hertogh, M., Quakkelaar, D., Raymakers, T., Sarma, M. H., Muench, M., Bos, H. & van der Kouwe, E. (2026) Rain: Transiently Leaking Data from Public Clouds Using Old Vulnerabilities, In 2026 IEEE Symposium on Security and Privacy (SP), IEEE Computer Society, Los Alamitos, pp. 1189-1205.

Lundell, B. (2020) Analys av DIGG:s policy för utveckling av programvara, Höskolan i Skövde, Skövde, ISBN: 978-91-983667-6-1, 100p, <http://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-18895>

Lundell, B. (2021) Yttrande över betänkandet Säker och kostnadseffektiv IT-drift (SOU 2021:1), Dnr. HS 2021/469, Höskolan i Skövde, Skövde, 7 maj (*Yttrandet skickat till Finansdepartementet, Stockholm*).

Lundell, B. (2022a) Enskilt yttrande över Riksarkivets förslag till författningar (Dnr. RA-KS 2021/18), Dnr. HS 2021/842, Höskolan i Skövde, Skövde, 28 januari (*Yttrandet skickat till Riksarkivet, Stockholm*).

Lundell, B. (2022b) Yttrande över betänkandet Säker och kostnadseffektiv IT-drift (SOU 2021:97), Version 1.0, Dnr. HS 2022/245, Höskolan i Skövde, Skövde, 21 mars (*Yttrandet skickat till Finansdepartementet, Stockholm*).

Lundell, B. (2022c) Feedback to the European Commission's Call for Evidence for an impact assessment on Intellectual Property – new framework for standard essential patents (SEPs), 9 May, published as feedback reference: F3257432, European Commission.

Lundell, B. (2023a) Comments on the European Commission proposal for a Regulation on SEPs, Dnr. HS 2023/568, Höskolan i Skövde, Skövde, 10 August, also published as feedback reference: F3434461, European Commission.

Lundell, B. (2023b) Yttrande över lagförslag till EU:s Cyber Resilience Act, Version 1.0, Dnr. HS 2023/495, Höskolan i Skövde, Skövde, 19 juni (*Yttrandet skickat till Carl-Oskar Bohlin, Minister för civilt försvar, Försvarsdepartementet & Regeringskansliet*).

Lundell, B. (2023c) Yttrande över lagförslag till EU:s Cyber Resilience Act, Version 2.1, Dnr. HS 2023/495, Höskolan i Skövde, Skövde, 28 augusti (*Yttrandet skickat till Erik Slottnér, Civilminister, Finansdepartementet & Regeringskansliet*).

Lundell, B. (2024a) Openness Concepts and Translation Incoherence: Clarifying the EU Cyber Resilience Act (CRA), Version 1.0 (Dnr. FP 2024/30), Höskolan i Skövde, 25 April (*Yttrandet skickat till Benjamin Bögel, Policy Officer on Cyber Security, European Commission*).

Lundell, B. (2024b) Openness Concepts and Inconsistencies between different language versions of the EU Cyber Resilience Act (CRA), Version 2.0 (Dnr. FP 2024/30), Höskolan i Skövde, 8 October (*Yttrandet skickat till Benjamin Bögel, Policy Officer on Cyber Security, European Commission*).

Lundell, B. (2025a) Yttrande över betänkandet AI-kommissionens Färdplan för Sverige (SOU 2025:12), Version 1.0, Dnr. HS 2025/373, Högskolan i Skövde, Skövde, 3 juni (*Yttrandet skickat till Finansdepartementet, Stockholm*).

Lundell, B. (2025b) Comments on the Revision of the Standardisation Regulation, Dnr. HS 2025/450, Högskolan i Skövde, Skövde, 21 July, also published as feedback reference: F3581814, European Commission.

Lundell, B. (2026a) Contributions to the ‘Open Consultation on the SBOM Implementation Guide’, SBOM Landscape Analysis - Towards an Implementation Guide, European Union Agency for Cybersecurity (ENISA), 16 January.

Lundell, B. (2026b) Comments on the revision of EU rules on public procurement, Dnr. HS 2026/81, Högskolan i Skövde, Skövde, 25 January, Feedback concerning ‘Revision of EU rules on public procurement’, also published as feedback reference: F33367416, European Commission.

Lundell, B. (2026c) Comments on the review of the European Interoperability Framework, Dnr. HS 2026/501, Högskolan i Skövde, Skövde, 15 July, published as feedback to the European Commission’s call for evidence on a review of the the European Interoperability Framework, feedback reference: F33510915, European Commission, 15 July.

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/18412-European-interoperability-framework-review/F33510915_en

Lundell, B. (2026d) No Competition, No Compliance: How Procurement Practices Decide Your Data Protection Outcomes?, Keynote presentation, In Nordic Privacy Arena 2026, Stockholm, 28-29 September. <https://dpforum.se/nordic-privacy-arena/nordic-privacy-arena-2026/>

Lundell, B., Gamalielsson, J. & Katz, A. (2015) On implementation of Open Standards in software: To what extent can ISO standards be implemented in open source software?, International Journal of Standardization Research, Vol. 13(1), pp. 47-73. <https://doi.org/10.4018/IJSR.2015010103>

Lundell, B., Gamalielsson, J. & Katz, A. (2019) Implementing IT Standards in Software: challenges and recommendations for organisations planning software development covering IT standards, European Journal of Law and Technology, Vol. 10(2). <https://ejlt.org/index.php/ejlt/article/view/709/>

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. <https://journals.open.tudelft.nl/jos/article/view/6695>

Lundell, B., Gamalielsson, J., Katz, A. & Lindroth, M. (2022a) 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. https://doi.org/10.1007/978-3-031-15086-9_6

Lundell, B., Gamalielsson, J., Katz, A. & Lindroth, M. (2022b) 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. <https://doi.org/10.29379/jedem.v14i2.749>

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).

<https://ejlt.org/index.php/ejlt/article/view/861>

Lundell, B., Gamalielsson, J. & Tengblad, S. (2016) IT-standarder, inlåsning och konkurrens: En analys av policy och praktik inom svensk förvaltning, Uppdragsforskningsrapport 2016:2, Konkurrensverket, ISSN: 1652-8089.

Lundell, B. & Lindroth, M. (2026/27) Fri och öppen programvara under Cyberresiliensförordningen: Konsekvenser för svenska företag?, *Juridiskt Tidskrift* (*accepterad för publicering*).

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.

<http://doi.org/10.1145/3673659>

NPS (2016) Open IT-standards, National Procurement Services (Kammarkollegiet), Stockholm, Dnr 96-38-2014, 7 March. <https://www.avropa.se/globalassets/dokument/open-it-standards.pdf>

OSD (2026) The Open Source Definition, Version 1.9, Open Source Initiative, Last modified 22 March 2007. <https://opensource.org/osd>

Regeringskansliet (2026) Förordning om utveckling av moln och AI, Faktapromemoria, FPM-nummer: 99, Finansdepartementet, Regeringskansliet, 8 juli.

<https://www.regeringen.se/contentassets/33c29cbc651d40abb7b873433a6007a6/forordning-om-utveckling-av-moln-och-ai-202526fpm99/>

Sahibli, T. & Olsson, E. (2025) "It-avtal en risk för svensk beredskap", *Svenska Dagbladet*, 5 mars.

<https://www.svd.se/a/Vz2zld/advokater-it-avtal-en-risk-for-svensk-beredskap>

State Chancellery (2024) Open Innovation and Open Source Strategy of Land Schleswig-Holstein, The Minister-President, State Chancellery, Kiel, Version 1.00, 20 November.

SVK (2021) Öppen antagonistisk hotbild för elförsörjningen, Ärendenr: 2021/4367, Svenska kraftnät, Sundbyberg, 1 november.

<https://www.svk.se/siteassets/3.sakerhet-och-beredskap/sakerhetsskydd/dokument/oppen-antagonistisk-hotbild-for-elforsorjningen-2021.pdf>