caisa Det Nationale Center for AI i Samfundet
The National Center for AI in Society

En modulær tilgang til digital suverænitet

Forfattere
Jurowetzki, Roman; Adler-Nissen, Rebecca; Pedersen, Morten Axel

Redaktører
Søgaard, Anders; Feldt, Johannes N.

- Publikationsdato: 9. december 2025
- Publiceret af: Udgivet af CAISA, Det Nationale Center for AI I Samfundet, København og Aalborg, Danmark.
- Dokumentversion: Udgivers PDF, registreret version.
- Citation for publiceret version (APA): Jurowetzki, R., Adler-Nissen, R., & Pedersen, M. A. (2025). *En modulær tilgang til digital suverænitet: Fra ambition til handling med et nationalt AI-orkestreringslag.* CAISA, Det Nationale Center for AI i Samfundet. https://caisa.dk/forskning/en-modulaer-tilgang-til-digital-suveraenitet

En modulær tilgang til digital suverænitet

Af Roman Jurowetzki, Rebecca Adler-Nissen og Morten Axel Pedersen

Kommentar: Fra ambition til handling med et nationalt AI-orkestreringslag

Resumé

Digital suverænitet handler grundlæggende om kontrol – men kontrol kan se ud på mange måder og kan opnås på forskellig vis. Derfor kan det være svært at vide, hvor man skal begynde. Suverænitet handler også om kapacitet: evnen til selv at udvikle, drive og tilpasse digitale løsninger uden at være afgørende afhængig af få aktører. På AI-området kræver det en modulær tilgang for et land som Danmark, hvis ambitionen om kontrol og kapacitet skal omsættes til praksis. Hensyn til sikkerhed, økonomi og rettigheder skal gøres konkrete og teknisk implementerbare – som *AI-byggeklodser*, der gør det muligt at prioritere omkostninger, nytte og risici ved hvert modul. På den måde kan beslutningstagere tage målrettede skridt mod øget suverænitet, uden at låse sig fast eller overse kommende udfordringer og muligheder. Den modulære tilgang giver fleksibilitet til løbende tilpasning, efterhånden som teknologi og samfund udvikler sig. Vi præsenterer her ét forslag til et sådant modul: et *nationalt AI-orkestreringslag*, der gør det muligt at håndtere akutte behov samtidig med, at langsigtede strategiske mål fastholdes – og som giver både offentlige og private aktører et fælles teknisk fundament at bygge videre på.

Hovedpointer

1. Vi har mistet kontrol over vores data og arkitekturer til big tech. I øjeblikket kontrolleres hovedparten af opbevaringen, modelleringen og behandlingen af danske og europæiske data af amerikansk-kontrollerede hard- og software hyperscalers, hvilket vanskeliggør europæisk digital suverænitet. Spørgsmålet er, hvor man kan begynde. Skal EU – og Danmark – prioritere at opbygge suveræn cloud-kapacitet, investere i egne modeller, eller accelerere halvlederresilienstiltag? Inden for AI-området handler digital suverænitet også om at opbygge systemer, der giver myndigheder, virksomheder og borgere mulighed for selv at styre og anvende AI-løsninger.

2. Der er økonomiske, samfundsmæssige og sikkerhedsmæssige risici ved manglende kontrol. En lille gruppe big tech-leverandører bestemmer priser og vilkår, uden at vi har et stærkt forhandlingsgrundlag. Dette er ikke kun en økonomisk udfordring: Organisatorisk mister vi kontrol over selve AI-arkitekturen, samt integrationen af data og modeller. Endelig bliver vi afhængige af løsninger og tilsyn, som vi ikke selv kan inspicere eller tilpasse. Det handler ikke kun om, hvor data ligger, men hvem der kan få adgang, under hvilke procedurer og med hvilke sikkerhedsforanstaltninger. Den manglende kontrol er ikke kun et problem i en krisesituation, eller hvis adgangen

pludselig afbrydes. Kontrol er vigtigt i dagligdagen for virksomheder, myndigheder og borgere.

3. En modulær tilgang til digital suverænitet giver hurtige sejre og fleksibilitet: Der er brug for et alternativ til eksisterende AI-platforme fra amerikanske *hyperscalers*. Vi skal udvikle en fælles løsning for at forhindre fragmentering og stiafhængighed – og dermed styrke den digitale suverænitet, da reel kontrol forudsætter, at vi ikke låses fast i vertikale udviklingsspor defineret af big tech. Ved at flytte fokus til horisontale moduler kan vi understøtte diversitet, muliggøre europæisk samarbejde og reducere teknologisk og arkitektonisk afhængighed.

4. Vi præsenterer et forslag til et fælles horisontalt modul: et *nationalt orkestreringslag,* der muliggør at håndtere både akutte behov og langsigtede strategiske mål for digital suverænitet – og som giver både offentlige og private aktører et fælles fundament at bygge på. Orkesterringslaget forbinder AI-infrastruktur, -modeller, applikationer og brugerinterfaces. På den måde øges graden af AI-suverænitet ved at kontrollere adgang, compliance og datastrømme (routing) og ved at operationalisere fælles compliance-krav og overholdelse. Risikovurderingen og klassificeringen sker fortsat på løsningsniveau, men orkestreringslaget sikrer ensartet håndhævelse af disse valg på tværs af systemer og leverandører. Denne modulære tilgang – en slags "appstore" - reducerer omkostninger og sikrer, at data opbevares decentralt i forlængelse af andelsbevægelsestraditionen, hvor fælles infrastruktur bygges og forvaltes i fællesskab, mens ejerskab og ansvar forbliver lokalt.

5. Adressér afhængighed af forældede systemer i offentlige indkøb. Ovenstående forslag til orkestrering bør ses i sammenhæng med en bredere strategi for gradvist at udfase afhængigheden af ældre big-tech-baserede systemer: Etablér en national eller europæisk målsætning om gradvist at reducere afhængighed af forældede systemer i offentlige udbud. Adresser sti- og systemafhængighed ved at ændre kravspecifikationer i offentlige udbud. Der skal stilles krav om f.eks. åbne API'er og programmatisk adgang til data og funktionalitet, så nuværende og fremtidige AI-løsninger kan kobles på eksisterende systemer gennem åbne protokoller – og så vi undgår at blive låst fast i proprietære platforme udenfor EU's kontrol.

Hvad er AI-suverænitet, og hvilke udfordringer står EU og Danmark med?

Der findes ingen entydig eller universelt accepteret forståelse af digital eller AI-suverænitet (Corture & Toupin 2019; Floridi 2020). En ofte anvendt definition forstår digital suverænitet som evnen til at opretholde kontrol over digital infrastruktur, dataanvendelse og teknologisk udvikling uden ekstern indflydelse (Pohle & Thiel 2020).[1] På AI-området dækker dette særligt fem dimensioner: (1) kontrol over data, indsamlet og processeret nationalt; (2) uafhængig udvikling og styring af digital og fysisk infrastruktur; (3) kapacitet til at beskytte digitale systemer mod interne og eksterne trusler; (4) demokratisk og lovgivningsmæssig selvbestemmelse; og (5) evnen til at regulere og håndhæve normer og værdier i praksis (Adler-Nissen & Eggeling 2024; Pohle & Thiel 2020).

Fraværet af digital suverænitet bliver tydeligt, når offentlige og private aktører primært indtager rollen som købere af løsninger designet og prissat af eksterne leverandører. Koncentrationen af data, infrastruktur og ekspertise i hænderne på få globale virksomheder skaber asymmetriske magtforhold, dybe stiafhængigheder og manglende modvægt (Flensburg & Lei 2023). Denne afhængighed forstærkes af europæisk fragmentering: når aktører forhandler, integrerer og implementerer systemer hver for sig, svækkes den samlede forhandlingsposition, og de samme infrastrukturelle investeringer gentages igen og igen uden opbygning af fælles kapacitet.

Her er det afgørende at skelne mellem pluralisme og fragmentering. Pluralisme i anvendelser – mange forskellige AI-løsninger tilpasset lokale behov – er en styrke i et demokratisk og innovativt økosystem. Fragmentering i infrastruktur – hvor hver aktør udvikler parallelle systemer uden fælles standarder – er derimod ressourcespild, der underminerer skalerbarhed, sikkerhed og forhandlingsstyrke.

Et yderligere lag af afhængighed skyldes, at selv når data opbevares fysisk i Danmark eller EU, kan amerikanske myndigheder i praksis kræve adgang gennem lovgivning som CLOUD Act. Derfor handler digital suverænitet ikke alene om datalokalitet, men om kapacitet: evnen til at udvikle, drifte og regulere teknologier dér, hvor behovet opstår – lokalt, regionalt og nationalt – samtidig med, at centrale infrastrukturer, standarder og sikkerhedsrammer opbygges i fællesskab.

[1] En anden definition, som kommer fra IT-branchen i Danmark, er: "Digital suverænitet er adgangen og evnen til at udvikle, anvende, beskytte og fastholde kritiske og strategiske teknologier, der er nødvendige for vores økonomiske, sikkerhedsmæssige og politiske uafhængighed og beslutningskraft" (IT-branchen 2025).

Disse principper rejser imidlertid et centralt spørgsmål: Hvad vil det konkret sige at være digitalt suveræn?

Nogle af de første lande til at formulere officielle politikker for "digital suverænitet" var Rusland og Kina, ofte betegnet som "cyber-" eller "internetsuverænitet". I Kina indebærer dette ikke blot masseovervågning og "*The Great Firewall*" – landets omfattende system til censur og trafikfiltrering – men også udvikling af nationale platforme og superapps, der fungerer som digital infrastruktur (Jiang 2024). Tencents WeChat og Alibabas Alipay udgør rygraden i landets digitale økosystem for kommunikation, betalinger, forsikringer, transport og digital identitet. I Rusland integrerer den statsligt støttede app MAX beskeder, betalinger, digitale ID'er og offentlige tjenester, og har indlejret AI-funktionalitet gennem chatbots som GigaChat (Reuters 2025).

I USA drives digital kontrol primært af nationale tech-giganter med globalt dominerende infrastrukturer (Bremmer 2021). Den offentlige sektor er derimod ofte begrænset af fragmenterede og forældede systemer og stærk leverandørafhængighed. Erfaringerne – blandt andet beskrevet i *Recoding America* (Pahlka 2023) – viser, hvor vanskeligt det er at bryde eksisterende stiafhængigheder og etablere fælles digital kapacitet, når institutionelle og kommercielle strukturer konstant reproducerer fragmentering - og dermed også udfordrer digital suverænitet.[2]

Siden har også EU sat ambitioner for digital suverænitet, senest med det fælles fransk-tyske topmøde om digital suverænitet d. 18. november 2025 (Declaration 2025), hovedsageligt af økokomiske og sikkerhedsmæssige årsager, men i stigende grad også for at beskytte demokratiet i en erkendelse af, at AI-infrastruktur er samfundsvigtigt.

Udfordringen er imidlertid, at Europas udgangspunkt adskiller sig markant fra USA, Kina og Taiwan. Europæiske data opbevares og behandles i høj grad af amerikansk-kontrollerede virksomheder, og denne strukturelle afhængighed gør det svært at opnå reel digital suverænitet. Samtidig er udvikling, drift og forbedring af avancerede AI-modeller ekstremt omkostningskrævende og kræver betydelige datamængder, energi og ekspertise (Luitse 2024; Van der Vlist et al. 2024).

Det efterlader et centralt strategisk spørgsmål: Hvor bør man begynde? Skal EU og Danmark prioritere at opbygge suveræn cloud-kapacitet, investere massivt i egne modeller, eller accelerere halvlederresilienstiltag? Digital suverænitet handler både om beskyttelse og om evnen til at opbygge systemer, der giver myndigheder, virksomheder og borgere reel mulighed for at forme, drifte og anvende AI-løsninger. Et demokratisk samfund kræver pluralisme og innovation tæt på praksisniveau – og her har Danmark potentiale til at blive et europæisk foregangsland. Vi kommer her med et konkret bud på, hvor man kan starte på AI-området.

En modulær tilgang til digital suverænitet

Siden foråret 2025 har CAISA afholdt en række workshops og talt med aktører og organisationer på tværs af den offentlige sektor, erhvervsliv og civilsamfund, herunder den digitale taskforce for kunstig intelligens. Formålet var at kvalificere vores forskning og indsamle erfaringer om AI-suverænitet – ikke kun som beskyttelse og regulering, men også som kontrol, handlefrihed og kapacitet.

Et tema går igen: digitaliseringsinitiativer i både den private og offentlige sektor snubler ofte over uklare krav til compliance i form af usikkerhed om fortolkning af regler og manglende rammer for deres håndtering. Manglende samarbejde mellem juridiske og tekniske domæner skaber blindgyder. Når det f.eks. antages, at brug af sprogmodeller indebærer træning på lokale data – mens der reelt er tale om inferens, hvor modellen blot tilgår data i svarøjeblikket – så taler parterne ofte forbi hinanden. Juridisk og teknisk er det to helt forskellige risikoscenarier. "Compliance" nævnes systematisk som en hovedbarriere for at tage AI i brug, også når kravene faktisk kan opfyldes. Problemet er, at det er svært at håndtere disse udfordringer dér i organisationen, hvor udfordringerne kræver konkrete tekniske og AI-baserede løsninger. Det bremser innovation lokalt, selv når både behov, idéer og kompetencer er til stede.

En anden udfordring er, at når en teknisk afdeling vil udvikle et AI-system – f.eks. til automatisering eller beslutningsstøtte – så bygger den oven på eksisterende, vertikalt integrerede komponenter: data, modeller, infrastruktur og brugerrettede applikationer. Behovsafklaring, design, brugerinddragelse, evaluering og beslutningstagning finder typisk sted lokalt i den enkelte organisation, uanset om udviklingen sker internt eller via leverandører. Men under overfladen ligger andre lag:

[2] Lanceringen af den føderale sundhedsplatform Healthcare.gov i 2013 – der kollapsede ved åbning på grund af komplekse, ukoordinerede it-kontrakter – førte til etableringen af US Digital Service og 18F med det formål at udvikle mere åbne og genanvendelige løsninger på tværs af myndigheder (Pahlka 2023). 18F fungerede i et årti som intern, tværgående teknologienhed, indtil den i marts 2025 blev nedlagt som led i Department of Government Efficiency (DOGE)'s omstruktureringer.

højtydende beregningsmiljøer til AI-modeller, data- og adgangsstyring, cloud-løsninger og sikker drift. Det er her, vi aktuelt møder de største suverænitetsudfordringer.

I takt med at industrien samler sig om få dominerende AI-modeller og cloud-udbydere, bliver det fristende - og praktisk på den korte bane - at udvide brugen af eksisterende big tech-løsninger. I den private sektor sker dette allerede – løsningerne er tilgængelige og virker. Men ikke blot for den offentlige sektor, men også for private aktører rejser der sig et grundlæggende spørgsmål: Har vi reel digital suverænitet, hvis fundamentet for vores teknologi ejes og drives udenfor vores kontrol? Selvom løsningerne nogle gange kan tilpasses EU-krav i forhold til f.eks. GDPR, er de sjældent suveræne, fordi kontrol, kvalitetsgarantier og udviklingsret ligger hos leverandøren. Erfaringer fra USA viser desuden, at en "lad big tech råde"-tilgang hverken sikrer velfungerende offentlige AI-løsninger eller beskytter borgerne.

Et muligt svar på disse strukturelle udfordringer er er en national platform med lokal kontrol og lokalt ansvar. Hvis det underliggende lag er fælles og compliant, kan AI-viden og praksisnære systemer udvikles lokalt – og deles eller genbruges på tværs, når det giver mening. I dag skal hver kommune og styrelse f.eks. individuelt forhandle kontrakter, opbygge teknisk integration, sikre compliance og vedligeholde opdateringer. Med et fælles orkestreringslag løses disse opgaver én gang nationalt: fælles forhandling, automatisk sikkerhedskontrol og central opdatering. Det hjælper mod leverandørafhængighed og muliggør nem udrulning af opdateringer. Vi foreslår med andre ord en tilgang, der omsætter abstrakte principper om digital suverænitet til konkrete AI-byggeklodser. Det vil muliggøre en prioritering i form af afvejning af omkostninger, fordele og risici, og en skelnen mellem kortsigtede og langsigtede problemstillinger og mellem kritiske og mindre kritiske udfordringer. På den måde kan vi allerede nu tage målrettede skridt mod større AI-suverænitet, uden at skulle låse os fast eller overse fremtidige udfordringer og muligheder, efterhånden som teknologien og samfundet udvikler sig.

Moderne AI-tjenester er modulære. Beslutninger træffes i hvert modul: hvem skal eje applikationen og dens datastrømme? Hvem skal kontrollere orkestrering og dens politikker? Hvilke modeller skal vælges og hostes under hvilke licenser? Og hvor hardwaren, der udfører inferensen, placeres? At holde disse beslutninger funktionelt adskilt (Bergek et al. 2008) forhindrer leverandørforveksling og gør valg om suverænitet eksplicitte, som illustreret i Figur 1.

Figur 1: AI-byggeklodser og digital suverænitet

Applikation

Brugerflader, portaler og systemer
Kendetegn: Decentral udvikling, relativt billig udvikling

Orkestrering

Binder brugere, data og modeller sammen
Kendetegn: Central governance, tung koordinering, platformkarakter

Model

Åbne eller lukkede AI-modeller
Kendetegn: Hurtig udskiftning, dyr udvikling, mange muligheder på markedet, nemt at udskifte

Infrastruktur

Servere, netværk og datalagring
Kendetegn: Dyre og fysiske komponenter, sikkerhed, ejerskab

Med udgangspunkt i Figur 1 kan vi identificere AI byggeklodser og beslutningspunkter indenfor applikation, orkestrering, model og hardware – uden at sammenblande begreber og tale forbi hinanden. Vi gennemgår figuren herunder fra fundamentet (infrastruktur) og op.

Infrastrukturlaget udgøres af computerchips (herunder sjældne råstoffer), computere, lagerkapacitet og netværk. AI-inferens kræver typisk cloud-infrastruktur og kapacitetsplanlægning, og træning af store modeller er typisk yderst ressourcekrævende, og finder kun sted i relativt få organisationer på globalt plan. Mindre modeller kan godt køre på laptops, men igen afhænger hastigheden ikke kun af computerkraft, men også af lagerkapacitet, netværksbåndbredde, mv.

Modellaget udgør den AI-komponent, der træffer beslutninger eller producerer output baseret på mønstre i data – opgaver, der ikke kan løses via traditionel software med simpel regelbaseret logik. Modeller findes i forskellige varianter: sprogmodeller, multimodale modeller (tekst-til-billede, osv.), oversættelsesmodeller (tekst-til-tekst, osv.), klassifikationsmodeller, semantiske søgemaskiner, osv. Nogle er lukkede og kun tilgængelige som service fra leverandører; andre er åbne og kan hostes, tilpasses og inspiceres. Private og offentlige aktører kan i princippet vælge den model, der tilfredsstiller præcisions-, sikkerheds-, sprog-, latens- og omkostningskrav i det givne anvendelsestilfælde. Modeller kan suppleres med domænespecifik viden gennem teknikker som *retrieval-augmented generation* (RAG), mens *fine-tuning* (træning) af modeller til særlige formål kræver betydelige ressourcer

og specialiseret infrastruktur. Modellen er en komponent i systemet, ikke systemet selv.

Orkestreringslaget er den samling af software og procedurer, der forbinder applikationer med AI-modeller og den bagvedliggende infrastruktur. Det styrer, hvilke modeller der benyttes hvornår, hvem der har adgang, hvordan aktivitet logges, og hvordan omkostninger følges. Den aktør, der kontrollerer dette lag, fastlægger i praksis de tekniske rammer for AI-brug på tværs af systemer. Ansvarsfordelingen er central: Applikationerne – f.eks. et kommunalt journalsystem – designer prompter, trækker data fra fagsystemer og vurderer, om output er fagligt og juridisk acceptabelt. Orkestreringslaget fastlægger, hvilke modeller er godkendt, hvordan systemadgang administreres, og hvordan sikkerhedskrav kontrolleres. Ved modelskift sker ændringen centralt, mens logfiler og historik bevares. Promptudvikling, forretningslogik og faglig tilpasning bliver i applikationslaget, hvor domæneekspertisen og det juridiske ansvar ligger. Vurdering af bias og håndtering af følsomt indhold kræver kontekst og forankres derfor i applikationerne – ikke generelt i infrastrukturen. Orkestreringslaget sikrer på den baggrund, at sikkerhedskrav og compliance kan håndhæves ensartet på tværs af modeludbydere og anvendelser.

Applikationslaget er brugergrænsefladen, der hvor borgeren, kunden eller medarbejderen møder en digital løsning, f.eks. en AI-chatbot, hvad enten der er tale om en sagsbehandler, der arbejder i forvaltningen, eller borgere der ønsker hjælp i kommunen, f.eks. i form af et sagsbehandlingsvindue eller en chatbot i en serviceportal. Her designes prompter, trækkes data fra fagsystemer, og her vurderes om AI-genererede outputs er fagligt og juridisk acceptable. Gode applikationer indlejrer institutionelle regler, strukturerer inputs og omdirigerer grænsetilfælde til menneskelig vurdering og beslutningskompetence. Kontrol over applikationen betyder kontrol over arbejdsgange, datastyring og forretningslogik, således processer kan forbedres uden at skulle vente på at leverandører eller centrale godkendelser.

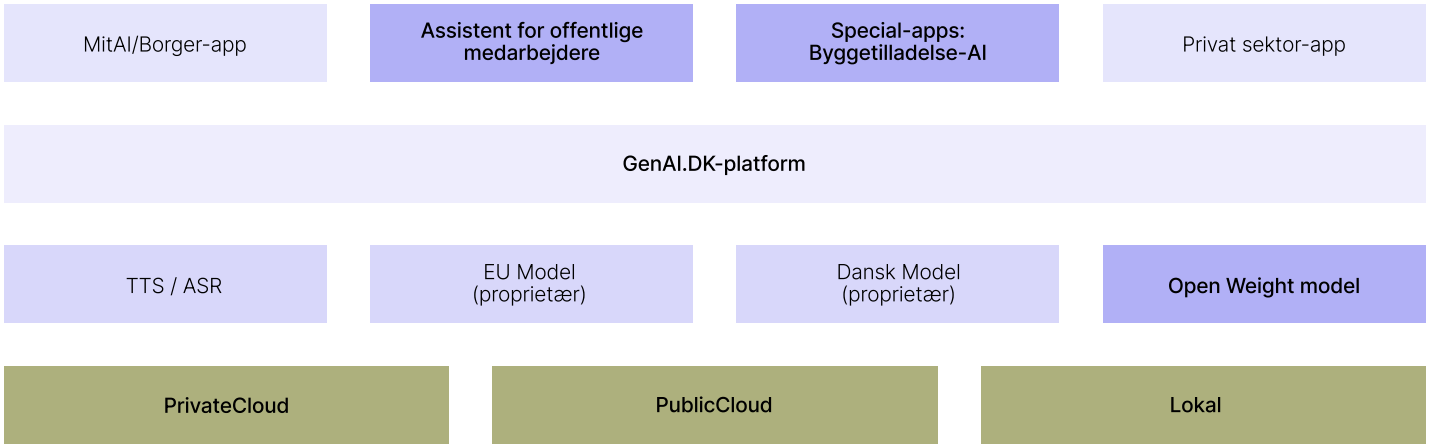
Med udgangspunkt i ovenstående byggeklodser præsenterer vi nu et konkret forslag i form af et national AI-orkestreringslag. Forslaget beror på en balancering af tekniske muligheder, politiske målsætninger og regulative rammer, samt en afvejning af effekt, udgifter og tidshorisont. Mens opbygningen af fuld dansk/europæisk digital suverænitet – herunder hardware – er et langsigtet mål, kan et orkestreringslag etableres på kort sigt ved at flytte fokus fra at eje hele AI-stakken til at kontrollere forbindelsen mellem hardware og software.

Grundprincipper for et nationalt orkestreringslag

Et nationalt orkestreringslag kan i praksis forstås som Danmarks fælles digitale indgangsportal – en "AI gateway" lidt à la en appstore – placeret mellem de applikationer og IT-systemer konkrete medarbejdere og borgere anvender til forskellige formål, og så de AI-modeller og infrastruktur, der leverer regnekraften. Applikationer sender forespørgsler gennem gatewayen, som router dem til godkendte modeller, logger kaldet og returnerer svaret. Organisationer kan benytte både egne og centralt hostede modeller. Logs er tilgængelige for den dataansvarlige organisation, mens aggregeret statistik bruges til central overvågning. Den enkelte organisation beholder kontrollen over sine data og beslutninger; orkestreringslaget leverer fælles teknisk infrastruktur (Figur 2).

Det er vigtigt at understrege, at orkestreringen ikke kan drive sig selv. Reel udøvelse af digital suverænitet via orkestreringslaget forudsætter en central og kompetent driftsenhed – en institutionel operatør eller organisation – med mandat til at udøve den praktiske kontrol. Denne enhed skal forhandle fælles vilkår, fastsætte spillereglerne,

Figur 2: Et nationalt AI-orkestreringslag.



føre tilsyn, foretage løbende modelaudits og træffe beslutninger om, hvornår trafikken skal omdirigeres. Den skal også løbende justere i takt med teknologiens og reguleringens udvikling. Den modulære tilgang betyder, at organisationer kan indstille nye modeller til godkendelse, hvorefter de bliver tilgængelige for andre gennem gatewayen. Uden en sådan samfundsmæssig og juridisk forankring forbliver AI-suverænitet en teoretisk størrelse. Nedenfor skitseres otte grundprincipper:

1. En fælles gateway – én indgang, mange muligheder
I sin grundform fungerer orkestreringslaget som en oversætter. Det modtager forespørgsler fra eksisterende it-systemer (f.eks. et sagsbehandlingssystem), videresender dem til den mest egnede AI-model og returnerer svaret i et standardiseret format. Dermed bliver avanceret AI (byggeklodser) tilgængelig på tværs af den offentlige sektor, uden at hver kommune, region eller styrelse behøver at opbygge og vedligeholde egne, parallelle integrationer til forskellige leverandører. Den ansvarlige organisation forhandler i fællesskab med leverandører af AI-modeller og infrastruktur, hvilket giver bedre priser og ensartede tekniske og kontraktuelle rammer – mens den konkrete juridiske vurdering af anvendelsen fortsat sker lokalt.

2. Modularitet som værn mod leverandørbinding (lock-in)
Orkestreringslaget skaber en klar teknisk adskillelse mellem tre niveauer:

- **applikationer** (hvor arbejdet udføres),
- **modeller** (hvor beregningen sker),
- **infrastruktur** (hvor data behandles og lagres).

Når lagene er adskilt, kan man udskifte en model eller en cloud-leverandør "under motorhjelmen", uden at skulle genopbygge hele applikationen. Dog vil skift mellem modeller ofte kræve justeringer af prompts- og forretningslogik i applikationslaget for at bevare brugeroplevelsen. Det styrker forhandlingskraften over for store leverandører og gør det lettere at skifte kurs, når teknologi, priser eller regler ændrer sig.

3. En national drifts- og tilsynsfunktion
Teknologien kan ikke stå alene. Et orkestreringslag kræver en national "institutionel operatør" med mandat til at udøve praktisk digital suverænitet. Denne enhed skal bl.a.:

- godkende, kvalitetssikre og løbende revurdere modeller før og under brug, i samarbejde med relevante fagmiljøer, der kan vurdere drift og performance i praksis,
- sikre, at personfølsomme oplysninger filtreres eller anonymiseres, før de eventuelt sendes til eksterne modeller,
- overvåge sikkerheden centralt og kunne lukke en sårbar model eller rute på tværs af landet med kort varsel,
- håndtere hændelser, sårbarheder og udfasning/sletning af modeller,
- sikre ensartet implementering af f.eks. EU's AI Act og GDPR i den konkrete tekniske praksis,
- mens den konkrete anvendelse og organisatoriske praksis forankres lokalt hos den dataansvarlige.

4. Dataopbevaring og suverænitet
Orkestreringslaget er en kanal, ikke et lager. Orkestreringslaget styrer trafikken, men opbygger ikke nye centrale datapuljer. Ejerskab og ansvar for data forbliver hos den enkelte myndighed eller institution. Orkestreringslaget fører register over adgange og logger aktivitet, men ser ikke ind i de data, der behandles. Dette princip gør det muligt at anvende moderne AI, uden at det samtidig kræver opbygning af nye, centrale dataregistre med øget overvågningsrisiko og uklare ansvarsforhold.

5. Modelvalg, kontrol og økonomisk styring
Et orkestreringslag kan muliggøre model-routing – f.eks. at simple opgaver sendes til mindre og billigere modeller – men det skal ske under fuld kontrol og sporbarhed, så udviklere og myndigheder eksplicit kan vælge og fastlåse modeller i kritiske processer. Kontrol er afgørende for at sikre forudsigelig adfærd, reproducerbare resultater og mulighed for at dokumentere, hvilken model der er brugt til hvad og hvorfor – både af hensyn til kvalitet, sikkerhed og efterlevelse af bl.a. EU's AI Act. Pointen er ikke automatisk at skifte model bag kulissen, men at samle styring af omkostninger, performanceprofiler og risici ét sted.

6. Standarder og åbenhed som fælles bund
Ved at bygge på dokumenterede og konsekvente standarder for API'er, dataklassificering, logning og sikkerhed undgår man at bytte én afhængighed ud med en ny. I praksis vil orkestreringslaget ofte følge de facto-standarder fra store udbydere (f.eks. OpenAI-kompatible API'er), men ved at samle integrationen ét sted kan man håndtere opdateringer centralt og om nødvendigt tilpasse eller udvide standarderne. Åbenhed betyder her, at arkitekturen er gennemskuelig, og at komponenter kan udskiftes, når behovet opstår. Det giver både offentlige institutioner og danske/europæiske virksomheder et fælles teknisk sprog og et fælles fundament at udvikle og samarbejde på.

7. Genbrug af prompts og løsninger
Når adgangen til modeller sker gennem det samme

orkestreringslag, kan løsninger deles på tværs. En effektiv instruks (prompt) til journalisering eller byggesager udviklet ét sted kan umiddelbart genbruges et andet, fordi den tekniske adgangsvej er ens. Over tid kan der opbygges et fælles bibliotek af afprøvede konfigurationer, prompts og applikationer, som institutioner kan tilpasse deres egne behov. Dog viser erfaringer, at effektiv vidensdeling kræver kuratering, dokumentation og faglig kontekst – ikke blot teknisk adgang. Et sådant bibliotek kræver derfor dedikerede ressourcer til at vedligeholde, kategorisere og formidle indhold, så institutioner kan finde og tilpasse løsninger til deres egne behov. Det giver plads til lokale eksperimenter – og gør det muligt at opskalere det, der virker.

8. Trinvis udvikling og udbygning

Et orkestreringslag behøver ikke være fuldt udbygget fra dag ét. Man kan begynde med en simpel gateway for udvalgte modeller og myndigheder og herfra gradvist udvide med mere avanceret compliance-kontrol, automatiseret anonymisering, integration til flere europæiske cloud-løsninger og yderligere sikkerhedsfunktioner. På den måde kan investeringer, regulering og praksis udvikle sig i takt – uden at kontrollen med AI overlades til markedet alene.

Konklusion

Digital suverænitet er ikke et enten/eller-spørgsmål, men et spørgsmål om realistiske prioriteringer på tværs af teknik, organisation, politik og jura. Det handler ikke kun om hardware og software, men også om samfundsmæssige snitflader og compliance. På AI-området er et første skridt at genvinde kontrol over de centrale moduler, der orkestrerer de AI-byggeklodser, som konkrete løsninger bygger på. Det handler ikke om at konkurrere med markedet om apps eller systemer, men om at give offentlige og private aktører adgang til godkendte strukturer og processer, så de sikkert og hurtigt kan udvikle og innovere.

En modulær tilgang til suverænitet på AI-området – med et nationalt orkestreringslag som løftestang – omsætter abstrakte principper om digital suverænitet til konkret handling. Orkestreringslaget – vores nationale AI-gateway – forbinder infrastruktur, modeller og applikationer og skaber fleksibilitet, reducerer leverandørafhængighed og ensartet efterlevelse af bl.a. GDPR og AI Act. Ved at prioritere åbne standarder og decentral databehandling undgår vi nye afhængigheder, samtidig med at vi styrker handlefrihed, ansvarlighed og sikkerhed.

Det er vigtigt at understrege, at det foreslåede orkestreringslag er en overordnet skitse. Vi udfolder f.eks. ikke her den fulde cybersikkerhedsarkitektur. Et konkret

Case: Frankrig – Albert som nationalt orkestreringslag

Frankrig udgør i dag et af de mest konkrete europæiske eksempler på, hvordan digital suverænitet kan omsættes til en modulær AI-arkitektur. Centralt står Albert – en statslig platform drevet af den tværministerielle digitaliseringsenhed DINUM. Albert fungerer som et fælles orkestreringslag, der gør generativ AI tilgængelig for hele centraladministrationen via én kontrolleret indgang. Platformen er bygget op langs de lag, vi har beskrevet ovenfor:

- **Infrastruktur.** Albert driftes på SecNumCloud-certificeret infrastruktur (bl.a. OVHcloud og Scaleway), hvilket sikrer, at data behandles under fransk jurisdiktion og efter nationale sikkerhedskrav.
- **Modeller.** Frankrig satser overvejende på åbne modeller – herunder franske Mistral-modeller og Llama – som finjusteres til offentlig forvaltning. Modellerne kan udskiftes og kombineres uden at forstyrre de systemer og arbejdsgange, der er bygget ovenpå.
- **Orkestrering.** Kernen er Albert API'et, et fælles, OpenAI-kompatibelt API*, som alle ministerier kan tilgå. Her håndteres routing, sikkerhed, logning og omkostningsstyring centralt, så den enkelte myndighed ikke skal opbygge sin egen AI-infrastruktur fra bunden.
- **Applikationer.** Oven på dette lag er blandt andet "L'Assistant IA" udrullet til titusinder af embedsmænd, og mere end 200 fagspecifikke løsninger til sagsbehandling, analyse og vidensarbejde, trækker allerede på den samme kernefunktionalitet.

Albert er samtidig et governance-projekt. DINUM fungerer som "institutionel operatør", der validerer modeller, håndterer sikkerhedshændelser og sikrer konsistent efterlevelse af GDPR og AI Act. Når en model først er godkendt og integreret i orkestreringslaget, kan den anvendes på tværs af staten uden, at hver enkelt myndighed skal gentage den juridiske og tekniske vurdering.

Perspektiver for Danmark

Den franske erfaring viser, at det er muligt at opnå reel kontrol uden at eje hele den underliggende forsyningskæde. Ved at placere den centrale styring i orkestreringslaget undgår man omfattende leverandørbinding og bevarer friheden til løbende at skifte eller supplere modeller og infrastruktur. Et fælles bibliotek af godkendte services og konfigurationer reducerer behovet for parallelle, fragmenterede løsninger i hver styrelse.

Endelig illustrerer Albert, at en national AI-infrastruktur ikke behøver at starte som et tungt flerårigt anlægsprojekt. Platformen opstod som et internt udviklingsinitiativ og er siden blevet udbygget trinvis i takt med behov, erfaringer og regulering. Det peger på en vej, hvor også Danmark kan etablere et nationalt orkestreringslag hurtigt, pragmatisk og modulært – og derfra gradvist øge digital suverænitet.

*"OpenAI-kompatibelt" refererer til et API-format, der er blevet en de facto-standard for kommunikation med sprogmodeller – ikke til virksomheden OpenAI. Formatet bruges bredt af både open source-modeller og kommercielle alternativer, hvilket netop muliggør leverandøruafhængighed.

design må sikre segmentering og stærk sikkerhed fra starten, så der tages højde for potentielle angrebspunkter. Ligeledes kan man spørge *hvis* suverænitet, der vil blive styrket ved et nationalt AI-orkestreringslag? Er det statens eller borgernes? Eller organisationer, det være sig offentlige, private eller NGO'er? Med henvisning til den lange danske tradition for partnerskaber på tværs af sektorer og interesser såsom andelsbevægelser, kan en national institutionel operatør af orkestreringslaget forvaltes i fællesskab med et klart mandat, mens ejerskab og ansvar forbliver lokalt.

Danmark kan med denne tilgang styrke digital suverænitet på kort sigt, uden at skulle opbygge eller eje hele teknologistakken i form af nationalt eller europæisk-baserede cloud- og foundationmodeller. Investeringen i et fælles orkestreringslag er lavere end de løbende omkostninger ved inkompatible, fragmenterede systemer – og skaber en varig kapacitet til at bruge og udvikle AI på en måde, der kan justeres, genbruges og revideres over tid.

Danmark har muligheden for at blive et EU-foregangsland for digital og AI-suverænitet, men står ved en skillevej: Enten fortsætter vi med leverandørstyrede økosystemer og stiafhængighed, eller også vælger vi et fælles AI-fundament, der forener kontrol og sikkerhed med innovation, pluralisme og strategisk modularitet.

Tak

Vi takker Bjarke Grønberg, Violaine Michel Lange, Jacob Lillelund, Mike Riess, Kim Sovsø og de øvrige deltagere ved en workshop i maj 2025 for deres aktive deltagelse og bidrag med værdifuld indsigt og ideer. Vi takker desuden Kristin Anabel Eggeling, og vores to eksterne reviewers og kollegaer for konstruktiv og grundig feedback. Briefets indhold og synspunkter er udelukkende forfatternes ansvar.

Om forfatterne

Roman Jurowetzki er lektor i innovation og anvendt datavidenskab ved Aalborg University Business School og chefforsker i CAISA. Rebecca Adler-Nissen er professor i international politik ved Institut for Statskundskab på Københavns Universitet, og centerleder af CAISA. Morten Axel Pedersen er professor i antropologi og social data science ved Institut for Antropologi og Copenhagen Center for Social Data Science (SODAS) på Københavns Universitet og chefforsker i CAISA.

Om CAISA

Det Nationale Center for Kunstig Intelligens i Samfundet (CAISA) er et nationalt konsortium, der samler forskere fra Københavns Universitet, Aalborg Universitet, Aarhus Universitet, IT-Universitetet og DTU i tæt samarbejde med Pioneer Centre for AI (P1).

Som Danmarks uafhængige forskningscenter for kunstig intelligens i samfundet sætter CAISA borgerne i centrum. Vi udfører banebrydende tværfaglig forskning og skaber overblik over nye videnskabelige gennembrud. Funderet i ny og tværfaglig forskning rådgiver vi beslutningstagere i den offentlige og private sektor i, hvordan de bedst udvikler og anvender kunstig intelligens i praksis, så den bidrager til vækst, understøtter demokratiet o g styrker digital selvbestemmelse.

CAISA er finansieret i en treårig pilotperiode med 20 millioner kroner fra Digitaliseringsministeriet og 30 millioner kroner fra forskningsreserven.

Referencer

- Adler-Nissen, R., & Eggeling, K. A. (2024). The discursive struggle for digital sovereignty: Security, economy, rights and the cloud project Gaia-X. JCMS: Journal of Common Market Studies, 62(4), 993-1011.
- Bergek, A. Jacobsson, S., Carlsson, B.,Lindmark, S. & Rickne, A. (2008). Analyzing the functional dynamics of technological innovation systems: A scheme of analysis. Research Policy 37 (3), 407-429.
- Bremmer, I. (2021). The Technopolar Moment: How Digital Powers Will Reshape the Global Order. Foreign Affairs, 100(6), 112–128.
- Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? New Media & Society, 21(10), 2305-2322.
- Declaration (2025) Declaration for European Digital Sovereignty 18 November 2025, https://assets.innovazione.gov.it/1763560898-declaration_on_digital_sovereignty.pdf
- Flensburg, S., & Lai, S. S. (2023). Follow the data! A strategy for tracing infrastructural power. Media and Communication, 11(2), 319-329.
- Floridi, L. (2020) The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. Philos. Technol. 33, 369–378.
- Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M. G., Bômont, C., ... & Zanin, C. (2023). Contested spatialities of digital sovereignty. Geopolitics, 28(2), 919-958.
- IT-Branchen (2025): Digital suverænitet. IT-branchens perspektiver og anbefalinger. https://itb.dk/wp-content/uploads/2025/06/digital-suveraenitet-it-branchen-udspil-2025.pdf
- Jiang, Min. (2024) "Models of State Digital Sovereignty From the Global South: Diverging Experiences From China, India and South Africa." Policy & Internet 16.4: 727-738.
- Luitse, D. (2024). Platform power in AI: The evolution of cloud infrastructures in the political economy of artificial intelligence. Internet Policy Review, 13(2).
- Pahlka, Jennifer (2023): Recoding America: Why Government Is Failing in the Digital Age and How We Can Do Better, Metropolitan Books.
- Pohle, J. & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4).
- Reuters (2025, August 21). Russia orders state-backed MAX messenger app, WhatsApp rival, pre-installed on phones. Reuters. https://www.reuters.com/technology/russia-orders-state-backed-max-messenger-app-whatsapp-rival-pre-installed-phones-2025-08-21/
- Van der Vlist, F., Helmond, A., & Ferrari, F. (2024). Big AI: Cloud infrastructure dependence and the industrialisation of artificial intelligence. Big Data & Society, 11(1).