Digital suverænitet i den offentlige sektor

Sammenfattende analyse af erfaringer og indsigter fra ind- og udland

Januar 2026

Bringing Ingenuity to Life.
paconsulting.com

Analysens indhold og disponering

Dette slide viser
indholdsfortegnelsen

Resumé

Baggrund og formål

PA Consulting har i perioden oktober 2025 – januar 2026 gennemført en analyse af digital suverænitet for Digitaliseringsministeriet, Digitaliseringsstyrelsen, KL og Danske Regioner. Analysen udspringer af initiativ 12 i den fællesoffentlige digitaliseringsstrategi 2026-29 og har til formål at afdække myndigheders erfaringer med migrering til alternative teknologier.

Tilgang og metode

Analysen bygger på desk research og interviews med danske og internationale eksperter og består af tre delanalyser:

- Udfordringsbillede
- Nøgleobservationer fra erfaringsopsamlingen
- PA's forslag til løsningsspor

Derudover er der udarbejdet et casekatalog med 15 eksempler på nationale og internationale erfaringer.

Kerneudfordringer for øget digital suverænitet

Analysen identificerer fire centrale udfordringer:

1. Høj afhængighed af større leverandører og manglende konkurrence
2. Manglende kontrol og transparens over egne data
3. Begrænset kontrol og styring af digitale løsninger
4. Sårbarheder i den digitale forsyningssikkerhed

Nøgleobservationer fra erfaringsopsamlingen

Myndighedernes arbejde med digital suverænitet udspringer i høj grad af et ønske om øget uafhængighed, øget kontrol og større digital valgfrihed. Det er ikke ambitionen at opnå fuld digital suverænitet, fordi det ikke anses som realistisk. Økonomiske besparelser er ikke en hovedprioritet, fordi øget kontrol og styring samt migrering til alternative teknologivalg kræver omstilling og investeringer – både teknisk og organisatorisk.

Erfaringsopsamlingen viser, at der findes reelle europæiske alternativer til software (AI, fagsystemer, kontorpakker mv.) samt cloud.

Der ses i mindre grad europæiske alternativer til fysisk it-infrastruktur som fx devices, servere og netværk, som i høj grad produceres og leveres af virksomheder uden for Europa.

Der er identificeret to hovedtyper af virkemidler til at opnå øget digital suverænitet:

- **Virkemidler, som skaber transparens og robusthed** i form af bl.a. risikobaseret strying, exit-strategier og beredskabsplaner
- **Virkemidler, som skaber forandring og handlekraft** i form af bl.a. indkøb og kravstillelse, alternative løsninger, parallelle løsninger og ejerskab til løsninger og data.

På tværs af de undersøgte cases er open source software et gennemgående og centralt greb til at sikre en øget grad af digital suverænitet.

PA's forslag til løsningsspor

PA foreslår tre løsningsspor i form af:

1. **Risikobaseret prioritering og styring af afhængigheder** med forslag om risiko-vurdering af digitale løsninger og it-infrastruktur, exit-strategier og stærkere audit-mekanismer.
2. **Indkøb, krav og arkitektur** med forslag om markedsafdækning med danske it-leverandører, revurdering af it- og arkitekturstrategier, "suverænitetspakke" til offentlige it-udbud samt fælles indkøb af suveræne cloud-ydelser.
3. **Organisation, finansiering og kompetencer** med forslag om at etablere et stærkere vidensgrundlag og puljer til finansiering af indsatser samt lokale og centrale organisatoriske tiltag, som kan være en central drivkraft i udbredelsen af alternative digitale løsninger og open source software.

01

Indledning og forståelsesramme

Dette kapitel udfolder opgavens formål, baggrund og leverancer samt den grundlæggende forståelsesramme omkring digital suverænitet som begreb. Herudover introduceres en model over teknologistakken som en gennemgående analyseramme samt en forståelse af open source software.

Formålet med analysen er at inspirere danske myndigheder til, hvordan en udvikling mod øget digital suverænitet kan se ud

Som input til arbejdet med at sikre en øget grad af digital suverænitet har parterne omkring den fællesoffentlige digitaliseringsstrategi (FODS) bedt PA Consulting (PA) om at udarbejde en analyse af udfordringer, erfaringsbaserede cases og mulige løsningsspor. Det har været et væsentligt element i opdraget, at de skitserede løsningsspor skal hente inspiration i udvalgte cases fra danske og udenlandske myndigheder samt enkelte private virksomheder.

Analysens formål

Parterne i FODS-samarbejdet har bedt om bistand til udarbejdelse af en samlet analyseopgave, som understøtter parternes arbejde med at belyse udfordringer og muligheder ved øget digital suverænitet.

Analysen skal afdække myndigheders erfaringer med migrering til alternative teknologier gennem konkrete eksempler. Afdækningen suppleres med enkelte eksempler fra private virksomheder.

På denne baggrund skal der opstilles en række mulige løsningsspor med nye og kendte greb, som parterne og de danske myndigheder kan arbejde videre med at realisere.

Formålet med analysen er således at inspirere danske myndigheder til, hvordan en udvikling mod øget digital suverænitet kan se ud.

digitaliserings ministeriet | Digitaliserings-styrelsen | DANSKE REGIONER | KL

Analysens baggrund

Baggrunden for analysen er et tydeligt fokusområde i den fællesoffentlige digitaliseringsstrategi 2026-29 om øget digital suverænitet og digital udvikling i Europa.

Regeringen, KL og Danske Regioner har en fælles ambition om at fremme digital suverænitet i den offentlige sektor pga. udfordringerne med bl.a. stigende afhængighed af digitale løsninger og it-infrastruktur fra få, meget store udenlandske virksomheder i kombination med en usikker geopolitisk situation og et intensiveret trusselsbillede.

Digitaliseringsstrategiens initiativ 12 har fokus på at skabe overblik over alternativer og øget konkurrence mhp. at reducere afhængigheder og sårbarheder samt støtte myndighedernes suverænitet over egne løsninger og data.

Det primære fokus er på mulige tiltag for de danske myndigheder. Analysen omfatter stat, regioner og kommuner.

Analysens hovedleverancer

Konkret omfatter analysearbejdet tre primære leverancer:

- **Delleverance 1:** Beskrivelse af en forståelsesramme for digital suverænitet og et overordnet udfordringsbillede, som suppleres med en vurdering af mere teknologinære udfordringer (kapitel 1 og 2).
- **Delleverance 2:** Opsamling af danske og udenlandske myndigheders erfaringer med migrering til alternative teknologier (afrapporteret som selvstændig leverance). Herudover en sammenfatning af den gennemførte dataindsamling med tværgående læringer og nøgleobservationer (kapitel 3).
- **Delleverance 3:** PA's forslag til mulige løsningsspor inkl. anbefalinger (kapitel 4).

Analysen er udarbejdet pba. parternes fælles opgavebeskrivelse og er gennemført i perioden oktober 2025 - januar 2026.

Analysen anlægger en forståelse af digital suverænitet, som primært knytter sig til udfordringer og handlemuligheder for de offentlige myndigheder i Danmark

Analysen fokuserer primært på udfordringer og handlemuligheder for de offentlige myndigheder. Her sondres mellem muligheder for den enkelte myndighed, muligheder på et samlet forvaltningsniveau (stat, regioner og kommuner) og muligheder i det fællesoffentlige samarbejde.

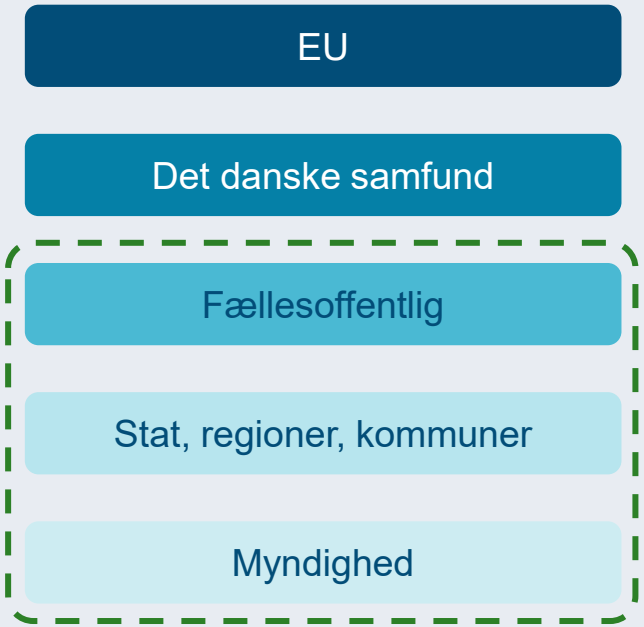
Vores forståelse af digital suverænitet

Der findes ikke én entydig, autoritativ definition af digital suverænitet, men der er efterhånden etableret en række forståelser af begrebet*.

I denne analyse anlægges en begrebsforståelse med tydeligt fokus på de **udfordringer** og **handlemuligheder**, som er relevante for de **offentlige myndigheder** i en dansk kontekst.

Øget digital suverænitet handler om at styrke offentlige myndigheders handlefrihed og kontrol, herunder muligheden for selv at til- og fravælge fx udenlandske tech-leverandørers produkter samt foretage leverandørskifte. Øget digital suverænitet handler ikke om at forbyde eller udfase produkter fra fx USA og andre tredjelande over én kam, men om øget kontrol, driftskontinuitet og færre bindinger til tech-leverandører. Dette kan også omfatte bindinger til danske og europæiske leverandører.

Analyseniveauer



Afgrænsninger

I et samfundsperspektiv handler øget digital suverænitet også om forskellige politiske instrumenter og rammevilkår – lige fra økonomi, digital regulering og erhvervs- og industripolitik til forsvarspolitik, uddannelse og forskning mv.

Denne analyse vedrører primært **digitaliserings-politiske muligheder** for den offentlige sektor. Analysen afgrænser sig derfor fra bredere løsningsspor rettet mod samfundet og EU.

Analysen identificerer løsningsspor med relevans for øvrige aktører, fx it-leverandører, ifm. samarbejdet om myndighedernes digitale løsninger, men **har ikke som formål at udarbejde egentlige erhvervspolitiske tiltag**. Analysen identificerer ligeledes løsningsspor med kobling til indsatser på EU-niveau, men det er **ikke formålet at formulere europæiske policy-initiativer**.

**Dansk Industri: "Digital suverænitet handler om, at virksomheder, organisationer og lande har kontrol over deres data og it-infrastruktur – frem for at være afhængige af udenlandske teknologileverandører og lovgivning.". Dirk Schrödter (Digitaliseringsminister i Schleswig-Holstein): "Digital suverænitet betyder, at enkeltpersoner og institutioner har kapacitet og kompetencer til at udfylde deres roller i den digitale verden uafhængigt, autonomt og sikkert". *European Parliament EPRS Ideas Paper: '"Digital suverænitet' refererer til Europas evne til at handle uafhængigt i den digitale verden og bør forstås både i form af beskyttelsesmekanismer og offensive værktøjer til at fremme digital innovation (herunder i samarbejde med virksomheder uden for EU)".*

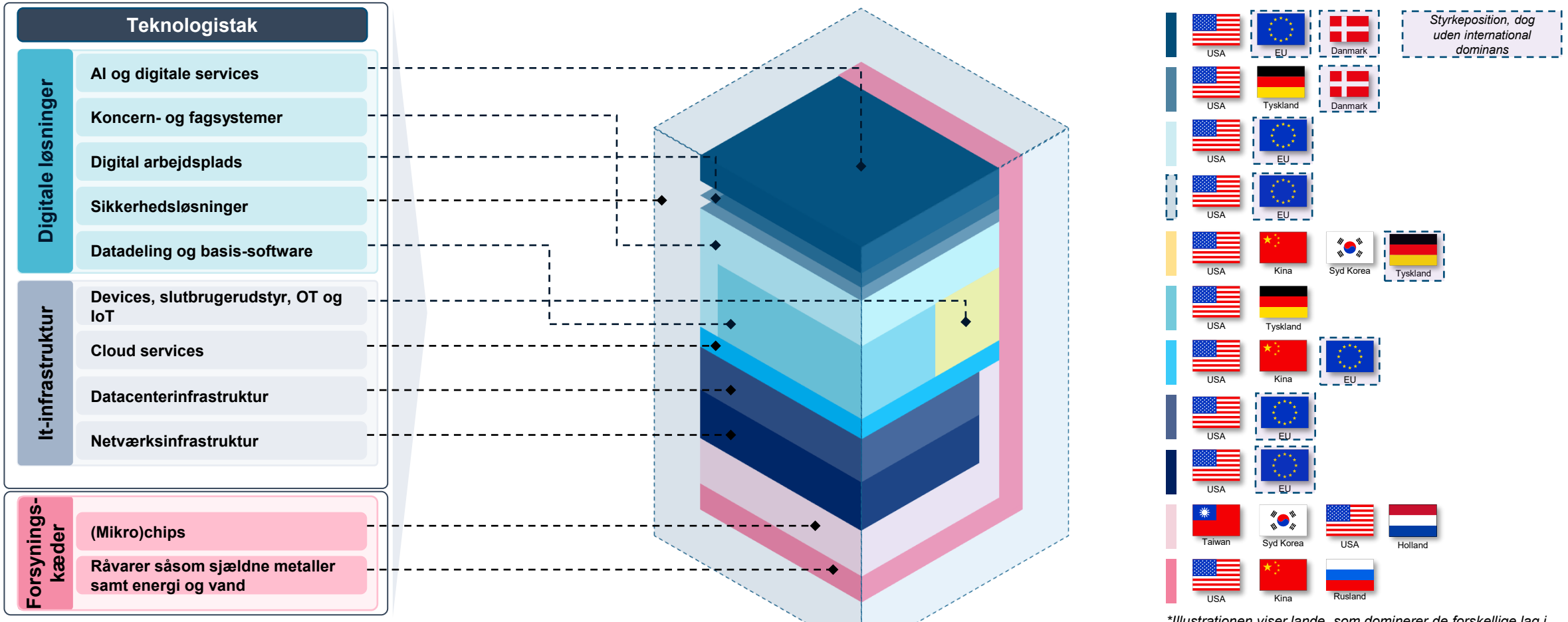
Analysen anvender en model over teknologistakken som en gennemgående forståelsesramme til at strukturere og beskrive både udfordringer og løsningsspor

I nedenstående oversigt er de forskellige elementer i teknologistakken uddybet. Analysen beskæftiger sig ikke med niveauet under it-infrastruktur, som omfatter mikrochips og råvarer, der anvendes i fremstillingen af hardware og den it-infrastruktur, som de digitale løsninger afvikles gennem.

	Teknologistak	Beskrivelse
Digitale løsninger	**AI og digitale services**	AI-platform, automatiseringsløsninger, dataanalyse og apps. Omfatter fx chatbots og virtuelle assistenter, predictive analytics, RPA og RDA, beslutningsstøtte, selvbetjening mv.
	Koncern- og fagsystemer	Større specialudviklede systemer samt standardløsninger, som understøtter regulering og specialiseret opgaveløsning. Koncernløsninger som ERP, ESDH mv.
	Digital arbejdsplads	Styresystemer og samarbejdsværktøjer til it-arbejdspladsen samt relaterede administrative systemer og mindre specialløsninger.
	Sikkerhedsløsninger	End point-sikkerhed (EDR), kryptering og firewalls, brugerstyring (IAM), overvågning og styring (SAC, SAC, SIEM), datastyring (DLP), beredskab og awareness.
	Datadeling og basis-software	Integrationsplatforme, middleware-komponenter, API-styring, datadelingsservices og komponenter, fx til styring af servere.
It-infrastruktur	**Devices, slutbrugerudstyr, OT og IoT**	PC'er, slutbrugerudstyr (mødeudstyr, printere, telefoner, tablets mv.) operationel teknologi (SCADA, drift af maskiner mv.) samt IoT (kameraer og sensorer).
	Cloud services	Skybaseret databehandling, hvor it-ressourcer som servere, lagring, databaser, netværk, software og analyse leveres via internettet og som forskellige services.
	Datacenterinfrastruktur	Fysiske og virtuelle servere og hosting via in-house datacentre og eksterne datacentre (outsourcing).
	Netværksinfrastruktur	Kernenetværk, lokalnetværk, kabler, datalinjer mellem lokationer og forskelligt netværksudstyr.
Forsynings-kæder	**(Mikro)chips**	*Leverandørafhængigheder kan betragtes helt fra råvareniveau (sjældne metaller) over mikrochips samt øvrige materialer, energi og vand, men fokus er på den klassiske teknologistak fra it-infrastruktur til digitale løsninger, der er relevante for myndighederne at håndtere.*
	Råvarer såsom sjældne metaller samt energi og vand	

Det er et grundlæggende karakteristika, at Danmark er en lille nation med betydelige teknologiske afhængigheder – særligt til amerikanske leverandører og produkter

De fleste dele af teknologistakken domineres* af amerikanske og herefter kinesiske produkter og leverandører. Der ses enkelte styrkepositioner i Europa som helhed og i enkelte EU-lande herunder Tyskland, Holland og Danmark.



*Illustrationen viser lande, som dominerer de forskellige lag i teknologistakken set ud fra et dansk perspektiv. Modellen er inspireret af analyser og visualiseringer fra Eurostack.

Open source er et centralt begreb i analysen, og det er afgørende at skabe en tydelig forståelse af, hvad begrebet omfatter

Open source-software (OSS) er et gennemgående begreb i analysen og derfor introduceres begrebet nedenfor for at sikre en tydelig forståelse af heraf. Begrebsforståelsen er baseret på Digitaliseringsstyrelsens publikation om "Open source i den offentlige sektor" (2025).

Definition, licenstyper og tilgange

Definition: OSS er software udgivet under en licens, der giver enhver ret til at bruge, undersøge, ændre og dele softwaren og dens kildekode frit og til ethvert formål. Det kan give myndigheder mulighed for at anvende og tilpasse software efter egne behov, og frigøre myndighederne fra afhængigheder til it-produkter og leverandører.

Licenstyper: Copyleft-licenser har til formål at sikre, at softwaren forbliver åben – også hvis anvendere vælger at videreudvikle eller tilpasse koden. **Permisssive licenser** giver myndigheder, it-leverandører og andre aktører større handlerum, da software i de fleste tilfælde kan anvendes og videredistribueres, herunder indgå i proprietær software. **Proprietære licenser**, hvor brug, ændringer og videredistribution af software er begrænset til leverandørens vilkår.

Tilgange: OSS kan grundlæggende anvendes som en aktiv ressource, fx via leverandører, i myndighedernes it-portefølje (inbound) eller myndighederne kan aktivt bidrage til udviklingen af ny OSS, der kan anvendes af andre (outbound).

Governancemodeller: (1) Foundation-drevet OSS hvor nonprofitorganisationer driver softwaren og sikrer governance, fx Apache, OS2, (2) virksomhedsdrevet OSS hvor kommercielle virksomheder udvikler og vedligeholder softwaren, fx Nextcloud, (3) Konsortium/branchedrevet OSS hvor flere virksomheder samarbejder om at udvikle og vedligeholde software i partnerskaber og (4) Community-drevet OSS hvor softwaren er udviklet af enkeltpersoner eller frivillige fællesskaber uden en større organisation bag.

Eksempler på brug af open source og forudsætninger

Digitale løsninger: Fx kontorpakken LibreOffice, sikkerhedsløsningen OS2BorgerPC, samarbejdsplatformen Open-Xchange og Firefox-browsere. Det omfatter også it-udviklingsværktøjer, fx GitLab til at udvikle, teste, gemme og dele kode og digitale løsninger.

It-infrastruktur: Fx operativsystemer og virtualisering (Ubuntu, Red Hat Enterprise Linux) databaser (PostgreSQL, MariaDB) og netværk og load balancing* (Haproxy, Nginx).

Forudsætninger for brug af open source: De forskellige licenser, tilgange og governancemodeller stiller forskellige krav til myndighedernes kompetencer og investeringer i OSS. Nogle løsninger har dedikeret support og vedligehold, mens andre kræver udvikling og et større organisatorisk set-up, fx et open source programme office (OSPO). Der præsenteres konkrete eksempler på forskellig anvendelse af OSS i analysens kapitel 3 (case-beskrivelser).

Brugen af OSS i de danske myndigheder: Der er ikke fastlagt regler for brugen af OSS i den offentlige sektor, ligesom der ikke findes data på anvendelsen af OSS. Det er PA's generelle indtryk, at størstedelen af de offentlige myndigheder ikke har en strategisk stillingtagen til OSS og primært anvender OSS situationsbestemt (ofte bottom-up) ud fra mere praktiske behov. I analysen præsenteres eksempler på frontløbere (Aarhus Kommune, OS2 og STIL).

**Load balancing (lastbalancering) betyder at fordele netværks- eller computerressourcer (som data, strøm eller web-trafik) ligeligt over flere servere, ladestandere eller enheder for at forhindre overbelastning, forbedre ydeevne, sikkerhed og sikre kontinuerlig tilgængelighed.*

02

Udfordringsbillede

Dette kapitel beskriver et samlet udfordringsbillede, som driver behovet for en øget grad af digital suverænitet hos danske myndigheder.

Introduktion til kapitel om udfordringsbillede

I dette kapitel præsenteres fire kerneudfordringer, som driver behovet for en øget grad af digital suverænitet hos danske myndigheder. Først præsenteres de fire udfordringer i en samlet oversigt, hvorefter udfordringerne bliver uddybet enkeltvis. Opstillingen er udtryk for PA's faglige vurdering og baseret på gennemført desk research som led i analysearbejdet samt validering via interviews med vidanspersoner.

Datagrundlag og forudsætninger

- Udfordringsbilledet er baseret på desk research af en lang række skriftlige datakilder og er blevet drøftet og valideret gennem +30 interviews med forskellige vidanspersoner og organisationer i Danmark og i udlandet. Vidanspersoner omfatter ledere og specialister fra offentlige myndigheder, interesseorganisationer, industri, tænketanke og forskning.
- Se bilagsmateriale for en oversigt over skriftligt kildemateriale og interviewpersoner, som har været involveret i analysen.
- Udfordringsbilledet udtrykker PA's samlede vurdering af de vigtigste udfordringer set i kontekst af den danske offentlige sektor og den anvendte definition af digital suverænitet*.

Tilgang til opstilling af udfordringsbillede

- På den følgende side præsenteres de fire hovedudfodringer i en samlet oversigt.
- Herefter udbydes hver hovedudfordring på en side med fokus på:
  - En kort beskrivelse af den faktiske situation
  - En opsummering af de vigtigste problemer
  - En kort beskrivelse af de vigtigste strukturelle barrierer, som er med til at forklare de forhold, der gør det vanskeligt at håndtere udfordringen
- Kapitlet afrundes med en oversigt med eksempler på, hvordan kerneudfordringerne kommer til udtryk på forskellige måder i de forskellige lag i teknologistakken. Der gives også eksempler på afhængigheder mellem de forskellige teknologilag for at vise, at det kan være svært at afgrænse udfordringer til et bestemt sted i stakken.

**På tværs af den danske offentlige sektor oplever man i stigende grad udfordringer med den voksende afhængighed af digitale tjenester fra få, meget store udenlandske virksomheder og deres indflydelse på den digitale infrastruktur. De fællesoffentlige parter vil derfor analysere udvalgte myndigheders teknologivalg, fremme overblik over alternative udbydere og tjenester samt skabe øget markedspluralitet og konkurrence, der kan reducere leverandørafhængighed, økonomiske sårbarheder og støtte myndighedernes suverænitet over egne løsninger og data. Samtidig skal pilotforsøg i den offentlige sektor supplere arbejdet og bidrage med praktisk erfaringsopsamling på området med henblik på opfølgende aktiviteter (Digitaliseringsstrategien 2022-2025 (udarbejdet af Digitaliseringsstyrelsen, KL og Danske Regioner).*

Der er en række kerneudfordringer, som driver behovet for en øget grad af digital suverænitet hos danske myndigheder

Det samlede problemfelt er komplekst og mangefacetteret – og det kan anskues forskelligt fra land til land. I en dansk kontekst med fokus på den offentlige sektor er der særligt fire hovedudfordringer, som er vigtige at forstå og belyse for bedst muligt at kunne skabe relevante handlemuligheder. De fire hovedudfordringer hænger tæt sammen og er delvist overlappende.

01 | Høj afhængighed af større leverandører og manglende konkurrence

- Markedet for digitale løsninger og it-infrastruktur er i betydelig grad domineret af få aktører (primært amerikanske).
- Der ses også eksempler på høj afhængighed til øvrige danske og europæiske enkeltleverandører.
- Høj afhængighed og mangel på konkurrence skaber teknologiske bindinger, høje priser, risiko for vendor lock-in og begrænset valgfrihed.

02 | Manglende kontrol og transparens over egne data

- Dele af myndighedernes data lagres og behandles i udenlandske cloud-miljøer under fremmede jurisdiktioner.
- Mangel på transparens og kontrol svækker ejerskab og tilliden til beskyttelse af data.
- Det er forbundet med en stor administrativ byrde at skabe et fuldstændigt overblik over de samlede dataflows og lagringslokationer.

03 | Begrænset kontrol og styring af digitale løsninger

- Myndighedernes teknologivalg indebærer i betydelig grad afhængighed af specifikke it-leverandører og proprietære teknologier.
- Lukkede systemer gør det svært at videreudvikle på disse løsninger til egne behov.
- Det kan være vanskeligt at få tilstrækkelig indsigt i nogle indkøbte it-systemer til at udøve effektiv kontrol over disse.

04 | Sårbarheder i den digitale forsyningssikkerhed

- Myndighederne er afhængige af leverandører og underliggende leverandørkæder for software, hardware og services uden for EU.
- Afhængigheder gør myndighederne sårbare over for mulige geopolitiske konflikter, handelsrestriktioner eller lignende.
- Der er en reel risiko for forsyningsstop og sabotage.

Udfordring 01 | Høj afhængighed af større leverandører og manglende konkurrence

Situation

- Den offentlige sektor er på tværs af teknologistakken afhængig af digitale løsninger og services fra få store leverandører. Der anvendes Chromebooks i skolerne, Dell PC'er og iPhones i ministerier og styrelser, Microsoft-kontorpakker til tekstbehandling og e-mail Google som søgemaskine og databaser fra Oracle og Microsoft.
- Der ses generelt en begrænset konkurrence på netværksinfrastruktur, cloud, devices og slutbrugerudstyr samt kontorpakker, imens der ses en større konkurrence på forretningssystemer og datacenterservices med både danske og europæiske leverandører.
- Afhængigheder forstærkes ved, at teknologier ofte er "bundlet" og hænger sammen, fx ved at software, infrastrukturkomponenter og services (fx hosting) købes som en "samlet pakke". Eller ved at teknologierne hænger sammen på tværs af produktkategorier og med integrationer til øvrige løsninger*. Standarder, fx til integration mellem komponenter, er i nogle tilfælde under kommerciel kontrol.

Problemer

- **Økonomiske sårbarheder.** Når store tech-leverandører på flere områder har opnået markedsmagt kan det udfordre forhandlinger om priser og kan medføre, at der betales for meget, eller at der accepteres ugunstige vilkår. Som eksempel er udgifterne til Microsoft-licenser steget markant i både stat og kommuner**.
- **Reduktion af handlefrihed.** Når meget teknologi er koncentreret om få større leverandører, øger det risikoen for vendor lock-in, som begrænser handlefriheden for de offentlige myndigheder. Det er forbundet med betydelige omkostninger og risici at bryde et vendor lock-in. Det kan desuden være svært at påvirke udviklingen af løsninger.
- **Øget usikkerhed**. Problemet omkring afhængighed og vendor lock-in gælder både danske, europæiske og ikke-europæiske leverandører. Der vil dog knytte sig en række geopolitiske risici til leverandører uden for EU, ligesom leverandører uden for EU ikke udelukkende er underlagt europæisk regulering. Det giver sammenlagt en større usikkerhed.

Strukturelle barrierer

- **Markedskoncentration.** En stor del af vores samlede teknologi- og datalandskab er globalt domineret af store amerikanske tech-leverandører og hyperscalers. Det kan gøre det svært for danske og europæiske aktører at konkurrere.
- **Mangel på alternativer og innovationskapacitet i Danmark og EU.** På flere områder i teknologistakken er der få eller ingen reelle alternativer til ikke-europæiske løsninger med hardware som eksempel. På andre områder er der ved at blive opbygget kapacitet, fx inden for cloud og AI. Mere generelt er der ikke den samme adgang til talent og risikovillig kapital i EU som i lande som USA og Kina.
- **Få målrettede investeringer i alternativer.** I en dansk kontekst ses en række eksempler på mindre investeringer i at sikre alternative løsninger, imens der aktuelt ses flere markante og målrettede investeringer i digital suverænitet, bl.a. i lande som Frankrig, Holland og Tyskland.

**Fx består Microsoft 365 af mange produkter: Word, Excel, Teams, SharePoint, Power Platform, Viva osv. De er tæt integrerede, men det er ofte uklart hvordan data flyder mellem dem, hvilke tilladelser der kræves, hvilke afhængigheder der opstår, hvis man fx bygger en løsning i Power Automate, der trækker data fra SharePoint og sender beskeder via Teams mv. Et andet eksempel er medicoteknisk udstyr på hospitaler med en betydelig andel amerikanske produkter, der også indeholder software og services vedr. support, dataopbevaring mv.*
***Kommunernes årlige udgifter til Microsoft-licenser fra 2018 til 2023 er steget fra 3 millioner kroner til 538 millioner, imens staten i 2024 betalte over en halv milliard kroner for Microsoft-licenser, hvilket er en stigning på 20 procent på ét år.*

Udfordring 02 | Manglende kontrol og transparens over egne data

Situation

- En del af den offentlige sektors data er placeret hos virksomheder med jurisdiktion uden for EU, herunder både mere og mindre følsomme data. Der findes ikke præcise opgørelser over, hvor meget data der er tale om*.
- Når clouddata ligger hos en privat leverandør, har denne virksomhed en form for kontrol over dem. Det spiller også en rolle, hvor virksomheden har valgt at placere dataene fysisk, da den fysiske placering kan være underlagt national lovgivning, der giver **myndigheder eller efterretningstjenester mulighed for at tilgå data**. Data er meget værdifulde for leverandøren, da de fx kan anvendes til produktudvikling og træning af AI-modeller.
- Der ses en **øget anvendelse af cloud-baserede distributions- og licensmodeller**. Flere leverandører vælger at introducere opgraderede løsninger med nye funktionaliteter i deres cloud-udgaver og ikke til on-premise-løsninger. Hertil kommer, at AI løsninger ved øge anvendelsen af Cloud bl.a. som følge af skalerbarhed og specialiseret hardware.

Problemer

- **Svækket gennemsigtighed, beskyttelse og ejerskab af vores data.** Når data er placeret hos virksomheder uden for EU, er det svært at få et fuldt indblik i, hvordan data reelt opbevares, hvem som kan tilgå data og hvordan data anvendes, fx ved utilsigtede tredjelandsoverførsler i forbindelse med cloud-ydelser, efterretninger eller mere kommercielle anvendelsesformål.
- På trods af relevant lovgivning (fx GDRP og Data Act) kan det være **svært at efterleve national og europæisk regulering,** og dermed kan der være usikkerhed om effekten af vores regulering og de offentlige myndigheders evne til at beskytte kritisk information.
- Manglende kontrol og transparens med offentlige data kan **underminere både myndighedernes og borgernes tillid**, hvilket både er et etisk og demokratisk problem.

Strukturelle barrierer

- **Usikkerhed om hvilken regulering der gælder for vores data.** Det kan være vanskeligt at efterleve krav om transparens eller audit i tredjelande. Hertil kommer, at regulering som fx CLOUD Act i USA kan pålægge amerikanske leverandører at udlevere data, selv når de er lagret i EU.
- **Kompleks og ressourcekrævende opgave at kortlægge dataopbevaring og -anvendelse**. De offentlige myndigheder anvender en bred vifte af forskellige digitale løsninger, hvor data er spredt på tværs af systemer og leverandører i både dansk og udenlandsk jurisdiktion, hvilket gør den samlede styringsopgave med at sikre transparens og compliance kompleks og tidskrævende.
- **Få europæiske alternativer på samme niveau som de amerikanske cloud-løsninger**. Der findes flere eksempler på europæiske alternativer (OVHcloud, Scaleway, Hetzner). De har dog ikke samme tekniske og leverancemæssige kapacitet som de amerikanske hyperscalers, hvorfor myndighederne primært bruger hyperscalers.

**Undersøgelser peger i retning af, at 87 procent af det danske cloud-marked (både privat og offentlig sektor) leveres af få store amerikanske tech-leverandører. Data som ligger hos ikke-europæiske virksomheder kan være opbevaret uden eller inden for grænserne af EU. Selv hvis data opbevares inden for EU, kan der være usikkerhed om, hvad data bliver brugt til, og hvem der kan få adgang til data. Hertil kommer en lang række data, som løbende afgives til ikke-europæiske virksomheder fx ifm. søgninger på internettet via søgemaskiner fra Google og Microsoft. Det kan også ifm. brugen af forskellige typer af apps, hvor undersøgelser viser, at 50% af de apps som de offentlige myndigheder anvender sender data til google, fordi der anvendes googlekomponenter til fejlsøgning i disse apps.*

Udfordring 03 | Begrænset kontrol og styring af digitale løsninger

Situation

- Den offentlige sektor er afhængig af digitale løsninger til at understøtte kritiske funktioner som identitetsstyring, kommunikation og og bagvedliggende leverandørkæder. datahåndtering inkl. følsomme informationer. En **betydelig andel af de digitale løsninger er proprietære løsninger** med afhængighed af specifikke enkeltleverandører, som begrænser indsigt løsningernes opbygning. Desuden kan visse forhold være svære at kontrollere.
- Proprietære it-løsninger udbydes af leverandører i og uden for EU. Flere løsninger integrerer open source-komponenter, men den samlede enterprise-pakke er typisk proprietær.
- Digitale løsninger – både software og hardware – kan desuden indeholde funktioner**, der **indsamler data uden vores viden**.

Problemer

- **Reduceret strategisk handlefrihed**. Hvis leverandører af specialiseret software ejer koden, begrænser det myndighederne mulighed for tilpasning til nye behov.
- **Geopolitisk sårbarhed.** Globale tech-leverandører kan udøve en form for indirekte udenrigs- og sikkerhedspolitik som følge af geopolitiske spændinger. Danmark vil være særdeles eksponeret, da alle samfundsfunktioner stort set er digitale, og både digitale løsninger og it-infrastruktur leveres af ikke-europæiske leverandører eller er baseret på teknologier fra ikke-europæiske lande***.
- **Etiske og demokratiske sårbarheder**. Mangel på indsigt i hvor og hvordan vores digitale løsninger er bygget og sikret, samt hvem som designer, udvikler og styrer teknologien, kan underminere myndighedernes og borgernes tillid.
- **Øget risiko for skjult overvågning**. Der er en øget risiko for overvågning og misbrug af informationer, når teknologien kommer fra leverandører uden for EU.

Strukturelle barrierer

- **Proprietære teknologier.** Leverandører beskytter kildekode og algoritmer.
- **Indkøbs- og udbudspraksis.** Offentlige indkøb er bundet af udbudsregler, der ofte favoriserer etablerede leverandører med dokumenteret compliance. Der stilles kun i mindre grad krav til anvendelse af open source og fuld transparens omkring digitale løsninger. Der gælder særregler for samfundskritisk it (specialkrav, lokationskrav).
- **Begrænset anvendelse af åbne standarder, interoperabilitet og modulær it-arkitekur.** Generelt set er der stor variation i myndighedernes krav om åbne standarder og interoperabilitet.
- **Kompleks og ressourcekrævende opgave at kontrollere og styre vores digitale løsninger.** Der findes paradigmer for både it-sikkerhed og compliance, krav til kritisk it-infrastruktur og styring af applikationer. Bedste praksis er ikke udbredt, og der ses kun i mindre grad systematisk vurdering af bindinger, exit-planer mv.

**Fx, Integrationer med tredjeparter, krypteringsmetoder, autentificeringslogik og adgangskontrol, fejlhåndtering og logning, dataopbevaringsstruktur og metadata, kommunikationsprotokoller og API-kald mv. ** Backdoors, telemetri og automatiseret dataindsamling, som ikke er dokumenteret eller verificerbar. ***Mange danske it-leverandører anvender 3. partsleverandører og komponenter. Det kan fx være udviklingsplatforme og udviklingsrammeværkøjer som kan være knyttet til større, globale techgiganter. På trods af, at leverandøren er i kontrol med egen løsning og underlagt dansk og europæisk regulering, er der en række yderligere afhængigheder, som ikke nødvendigvis er kritiske ifm. daglig produktion, men som kan bremse og forsinke udviklingsopgaver.*

Udfordring 04 | Sårbarheder i den digitale forsyningssikkerhed

Situation

- Den offentlige sektor er dybt integreret med internationale teknologileverandører og er afhængig af globale leverandørkæder for kritiske digitale komponenter – fra chips og hardware til cloud-infrastruktur og software.
- En stor del af disse leverandører er placeret uden for EU, primært i USA og Asien.
- Det betyder, at **forsyningssikkerheden ikke er under dansk eller europæisk kontrol**.
- Politisk uro, handelsrestriktioner eller sanktioner kan hurtigt **påvirke tilgængeligheden** af kritiske teknologier.
- Samtidig er der **begrænset kapacitet** til at producere avancerede chips, cloud-infrastruktur og andre nøglekomponenter i Europa såvel som i Danmark, hvilket forstærker sårbarheden yderligere.
- Tilliden til juridiske aftaler er ikke længere i sig selv et tilstrækkeligt kontrolværn til at give ejere af it-infrastruktur kontrol og styring.

Problemer

- **Forsyningsstop**: Handelskonflikter eller sanktioner kan påvirke leverancer af kritisk hardware eller eksisterende forretningskritisk software og cloud-services*.
- **Indbyggede sårbarheder**: Leverandører uden for EU kan indbygge såkaldte *kill bits* eller *kill switches,* der kan deaktivere systemer.
- **Strategisk afhængighed**: Manglende europæisk produktion og kontrol reducerer handlefriheden i krisesituationer.
- **Øget politisk pres**: Geopolitiske spændinger kan bruges som pressionsmiddel mod Danmark og EU.

Strukturelle barrierer

- **Global leverandørkæde:** Hardware og software er baseret på komponenter og platforme fra primært USA og Asien.
- **Begrænset europæisk kapacitet:** EU har et begrænset antal leverandører med varierende kvalitet inden for ERP, cloud, operativsystemer og kritiske hardwarekomponenter.
- **Kompleksitet i leverandørkæder:** Svært at skabe fuld transparens og kontrol over de samlede leverandørkæder. Det kan desuden være vanskeligt at opnå fuld indsigt i udenlandske ejerforhold hos leverandører.

**Danmark er især sårbar som følge af den massive afhængighed til amerikanske produkter og leverandører. De offentlige myndigheder anvender Microsoft til udviklingsplatform, cloud-infrastruktur, data-, applikations- og automatiseringsplatform, Amazon Web Services (AWS) til hosting og cloudtjenester, Google Cloud Platform (GCP) til dataanalyse og AI, Oracle & IBM til databaser og enterpriseløsninger og ServiceNow til ITSM og workflow-automatisering. Nogle af vores kritiske forretningssystemer er udviklet af ikke-europæiske leverandører eller på ikke-europæisk teknologi – fx er Sundhedsplatformen bygget af en amerikansk leverandør og statens system til økonomistyring er Microsoft-baseret.*

Der er betydelige afhængigheder i hele teknologistakken, men kerneudfordringerne kommer til udtryk på forskellige måder i teknologistakkens lag

Nedenstående oversigt viser eksempler på, hvordan udfordringer kommer til udtryk på forskellige måder i teknologistakkens lag. Der ses flere eksempler på afhængigheder mellem de forskellige teknologilag, hvilket kan gøre det svært at afgrænse udfordringer til et bestemt sted i stakken, fx kan et fagsystem blive udviklet og leveret af en dansk leverandør på en ikke-europæisk teknologiplatform, hostet i et ikke-europæisk land.

Illustrative eksempler

Teknologistak		01 | Høj afhængighed af større leverandører og manglende konkurrence	02 | Manglende kontrol og transparens over egne data	03 | Begrænset kontrol og styring af digitale løsninger	04 | Sårbarheder i den digitale forsyningssikkerhed
Digitale løsninger	AI og digitale services	Meget AI afvikles via amerikanske hyperscalers. Der ses europæiske alternativer i mindre skala.	De fleste AI-løsninger kører på cloud-infrastruktur fra hyperscalers som kan være svære at kontrollere. Dog betydelig opmærksomhed på følsomme data.	AI-løsninger styres efter regulering med høje krav til dokumentation – men det kan være svært at kontrollere data, algoriter, opdateringer mv.	Mange digitale services (low code, automatisering) og AI har afhængigheder på tværs i stakken til fx udenlandske cloud-platforme.
	Koncern- og fagsystemer	Danske it-leverandørers løsninger bygger ofte på ikke-europæiske platforme og standarder, som kan være svære at påvirke og kontrollere.	Stigende tendens imod at levere løsninger (med følsomme data) som software-as-a-service (SaaS) via cloud, hvilket kan være svært at kontrollere.	Det område i stakken som er mest moden ifm. it-styring. Mange proprietære løsninger, som kan være svære at kontrollere og præge udviklingen af.	Selvom løsninger leveres af danske leverandører, kan de bygge på teknologier og standarder som er svære at kontrollere, ligesom data kan opbevares uden for EU.
	Digital arbejdsplads	Høj grad af afhængighed til amerikanske hyperscalers og proprietære løsninger - dog mulighed for OSS-alternativer.	De fleste kontorpakker og samarbejdsværktøjer afvikles som SaaS. Løsninger kan indeholde følsomme data og være svære at kontrollere.	Lavere grad af styring, mindre gennemsigtighed og manglende viden om alternativer som følge af en meget høj grad af vendor lock-in.	Meget stor afhængighed til få produkter og kobling til mange digitale løsninger giver sårbarheder.
	Sikkerhedsløsninger	Afhængighed til amerikanske proprietære løsninger - især til brugerstyring. Der findes dog flere europæiske leverandører og alternative løsninger.	Stigende tendens imod at levere løsninger (med følsomme data) som SaaS via cloud, hvilket kan være svært at kontrollere.	Lavere grad af styring, stor indvirkning på afvikling af øvrige systemer med bruger- og adgangsstyring som eksempel.	Høj afgængighed til få produkter og kobling til flere kritiske digitale løsninger.
	Datadeling og basis-software	Danske it-leverandørers løsninger bygger ofte på ikke-europæiske platforme og standarder, som kan være svære at påvirke og kontrollere.	Det kan være vanskeligt at skabe et komplet overblik over løsniger og data, da data bevæger sig i et komplekst og stort økosystem.	Kan styres på samme vis som fx fagsystemer, men tendens til en lavere grad af styring, på trods af løsningers indvirkning på afvikling af øvrige systemer.	Lav transparens og usikkerhed om afhængigheder.
It-infrastruktur	Devices og slutbrugerudstyr	Høj afhængighed til amerikanske og herefter kinesiske leverandører med betydelige skalafordele og leverancekapacitet med få europæiske alternativer.	Mindre grad af systematisk styring af devices som fx IoT-enheder og kameraer på trods af, at løsninger indsamler data og indeholder software.	Lavere grad af styring, da løsninger anskues som mindre forretningskritiske, på trods af usikkerhed om opsamling og brug af data.	Stor afhængighed af ikke-europæiske produkter. Omvendt ses global konkurrence med produkter fra mange lande.
	Cloud-services	Amerikanske hyperscalers har en dominerende markedsposition - dog med europæiske alternativer som har skaleringsmuligheder.	Stor brug af ikke-europæiske cloudleverandører og brug af danske og europæiske leverandører, som anvender clouds uden for EU, der kan være svære at kontrollere.	Mange hyperscalere bruger lukket teknologi, hvilket gør det svært at inspicere og styre sikkerhed og anvendte teknologier.	Høj afhængighed til amerikanske hyperscalers både fsva. storage og udviklingsplatforme, hvilket giver sårbarheder.
	Datacenterinfrastruktur	Stor afhængighed ift. hardware fra ikke-europæiske lande - dog ses flere OSS-produkter og et større dansk og europæisk marked for datacenterydelser.	Afhængighed til ikke-europæisk basis-software og management-løsninger med risiko, for at data kommer uden for EU og derved bliver svære at kontrollere.	Ofte mangelfuldt overblik over værdikæde og teknologier - dog nogen grad af styring via sikkerhedsprocedurer, ITIL, dokumentation mv.	Data og teknologi er placeret i DK eller EU med høj grad af kontrol, men afhængighed til ikke-europæisk hardware og software giver sårbarheder.
	Netværksinfrastruktur	Stor afhængighed ift. hardware fra ikke-europæiske lande - dog ses flere OSS-produkter og et større dansk og europæisk marked for netværksydelser.	Afhængighed til ikke-europæisk basis-software og management-løsninger med risiko, for at data kommer uden for EU og derved bliver svære at kontrollere.	Ofte mangelfuldt overblik over værdikæde og teknologier - dog nogen grad af styring via sikkerhedsprocedurer, ITIL, dokumentation mv.	Fysisk udstyr i DK med nogen grad af kontrol, men afhængighed til ikke-europæisk hardware og software giver sårbarheder.

Kapitel 3

Nøgleobservationer fra erfarings-opsamling

Dette kapitel præsenterer en sammenfatning af de vigtigste observationer og læringer fra cases og interviews med videnspersoner.

Introduktion til kapitlet om nøgleobservationer fra cases og interviews

I dette kapitel præsenteres en opsummering af nøgleobservationer og læringer med afsæt i den gennemførte erfaringsopsamling og casestudier. Observationerne er baseret på analysens datagrundlag og fordelt på tre temaer.

Datagrundlag og forudsætninger

- Observationerne bygger på desk research af en lang række skriftlige datakilder og +30 interviews med forskellige videnspersoner og organisationer i Danmark og i udlandet. Videnspersoner omfatter ledere og specialister fra offentlige myndigheder, interesseorganisationer, industri, tænketanke og forskning. Se bilagsmateriale for en oversigt over skriftligt kildemateriale og interviewpersoner.
- Observationerne er opstillet af PA og således PA's vurdering af væsentlige læringer og indsigter fra den gennemførte dataindsamling.
- Vi anvender betegnelsen "myndigheder" som en samlet betegnelse for de aktører, der har arbejdet med digital suverænitet. Der er dog også opsamlet enkelte erfaringer fra den finansielle sektor.

Tilgang til opstilling af nøgleobservationer

- Observationerne er struktureret efter tre temaer, jf. nedenstående figur.

01 | Strategisk ambition og gevinster
Myndighedernes arbejde med digital suverænitet udspringer af et ønske om øget uafhængighed, øget kontrol og større digital valgfrihed.

02 | Virkemidler til at opnå øget digital suverænitet
Der kan opnås øget digital suverænitet gennem flere virkemidler – fra indkøb og styring til alternative løsninger. Der skelnes mellem virkemidler der skaber forudsætninger og virkemidler der skaber forandring**.*

03 | Forudsætninger for øget digital suverænitet
Digital suverænitet kræver omstilling og investeringer, både teknologisk, organisatorisk og kompetencemæssigt.

Disse tiltag handler primært om at skabe indsigt, reducere risiko og sikre beredskab – uden nødvendigvis at ændre eksisterende digitale løsninger. Disse tiltag er mere aktive og orienteret mod at skabe reelle alternativer, styrke valgmuligheder og sikre kontrol over løsninger.*

Analysen har belyst 15 cases som kan give inspiration til de danske myndigheder

De 15 cases viser eksempler på hvordan offentlige myndigheder arbejder med at sikre en øget grad af digital suverænitet – lige fra strategiske og organisatoriske tiltag, styring og kravstillelse til større open source transformationer og etablering af alternative løsninger til dominerende produkter. Casekataloget indeholder også to eksempler fra den finansielle sektor. Det samlede casekatalog er afrapporteret som en selvstændig leverance.

1. EuroStack
Europæisk digital suverænitet med fokus på at skabe teknologiske alternativer i EU

2. Eu-Kommissionen
€180 mio. udbud af digitalt suveræne clouds i EU-Kommissionen

3. Tyskland: Schleswig-Holstein
Open source-transformation væk fra Microsoft-produkter

4. Tyskland: ZenDis
National aktør som understøtter myndighedernes arbejde med digital suverænitet

5. Holland: Økonomi-ministeriet
National og suveræn AI-chatbot

6. England: Home Office
Open source, hybride cloudmiljøer og digital strategi

7. STIL
Åben og komponent-baseret arkitektur med brug af OSS

8. OS2
Forening af danske myndigheder som driver udviklingen af OSS-produkter

9. KOMBIT
Åben og komponent-baseret arkitektur med fokus på transparens og rettigheder

10. Aarhus Kommune
Strategisk transformations-program for øget digital handlefrihed

11. Aarhus kommune
Omlægning af cloud-infrastruktur fra Microsoft til europæisk leverandør

12. Region Syd
Udbud af logistik-teknologi med krav om digital suverænitet

13. Københavns Kommune
Analyse af risici og bindinger for at øge den digitale handefirhed

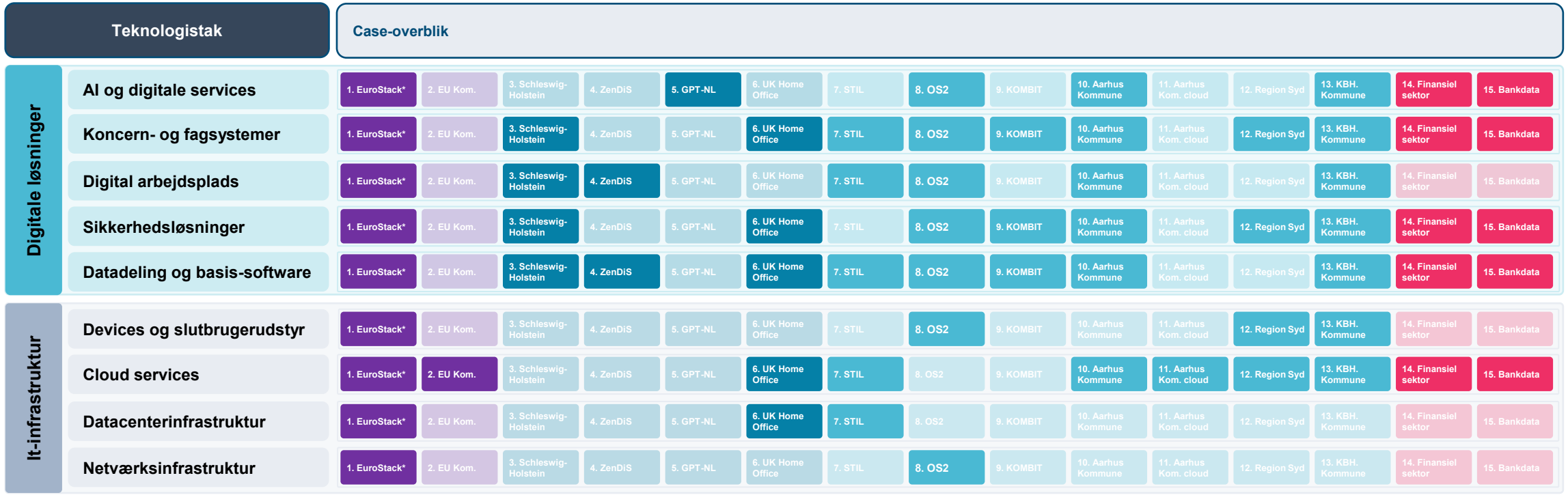
14. Finansiel Sektor
Risikobaseret analyse og styring af kritiske digitale løsninger

15. Bankdata
Øget digital suverænitet via hybridmiljøer og OSS

- Fælleseuropæisk
- Udenlandske myndigheder
- Danske myndigheder
- Privat sektor

De identificerede cases har forskelligt fokus i teknologistakken

Caseanalysen viser, at der findes reelle alternativer til dominerende løsninger inden for digitale løsninger (AI, fagsystemer, digital arbejdsplads) og cloudområdet. Der er færre europæiske alternativer til fysisk it-infrastruktur (devices, servere, netværk), som primært produceres og leveres af virksomheder uden for Europa. Cases om it-infrastruktur fokuserer derfor på styringstiltag eller open source software til konfiguration og overvågning.



**For EuroStack-initiativet er det ambitionen at ramme hele teknologstakken. Initiativet er kun i idé- og strategifasen og der er således ikke realiseret konkrete alternative løsninger endnu.*

Myndighedernes arbejde med digital suverænitet udspringer af et ønske om øget uafhængighed, øget kontrol og større digital valgfrihed

Nøgleobservation 1.1 | **Fuld digital suverænitet er ikke et endemål**

- Fuldstændig suverænitet vil kræve kontrol, valgfrihed og forsyningssikkerhed igennem hele teknologistakken og den underliggende forsyning af bl.a. råvarer og chips. Det er ikke muligt i et dansk eller europæisk perspektiv, hverken på kort eller mellemlang sigt.
- Myndighedernes fokus er i stedet på de områder, hvor de digitale sårbarheder er størst, fx afhængighed af udenlandske cloud-udbydere, proprietære formater eller manglende exit-strategi. Det er et spørgsmål om at forstå sine kritiske afhængigheder og sårbarheder, for at kunne vurdere den samlede risikoeksponering og handlemuligheder.

Nøgleobservation 1.2 | **Der findes reelle alternativer til dominerende produkter**

- Det er muligt at udskifte digitale løsninger og dele af den samlede infrastruktur mhp. at øge den digitale suverænitet. På flere områder i teknologistakken findes modne og velafprøvede alternativer, fx europæiske cloud-løsninger, digitale kontorpakker og samarbejdsværktøjer, sikkerhedsløsninger, programmeringssprog, databaser og operativsystemer mv.
- Der er eksempler på myndigheder, som udvikler nye løsninger "fra bunden" for at skabe alternativer. Der ses både eksempler på mindre fagsystemer og digitale services med lav kritikalitet, fx løsninger til overblik over it-systemer, indberetninger mv., men også mere forretningskritiske løsninger til bl.a. datadeling og sagsbehandling (jf. cases fra Home Office og Schleswig-Holstein).
- Alternativer kan både være open source-software (OSS) og proprietære løsninger som også kan indeholde open source-komponenter.

Nøgleobservation 1.3 | **Øget kontrol og digital valgfrihed er centrale gevinster**

- Myndighedernes ambition med digital suverænitet er at opnå øget kontrol og digital valgfrihed samt færre kritiske digitale afhængigheder.
- Digital suverænitet handler om at balancere pris, kvalitet og kontrol ved indkøb og udskiftning af digitale løsninger og it-infrastruktur. Øget digital suverænitet kan i nogle tilfælde betyde højere omkostninger eller løsninger med mindre funktionalitet (jf. cases fra EU-Kommissionen, Schleswig-Holstein og STIL).
- Der ses flere konkrete eksempler på, at udskiftning af teknologier kan nedbringe omkostninger til licenser, men at migreringen til alternative teknologier indebærer omkostninger til egne kompetencer, nye it-leverandører, governance mv. Økonomiske besparelser bør derfor ikke være det primære formål.

Nøgleobservation 1.4 | **Ny arena for fælleseuropæiske digitale løsninger**

- Der ses flere eksempler på større og mere transformative tiltag i flere europæiske lande (fx Frankrig, Holland og Tyskland) og på fælleseuropæisk niveau (fx EuroStack og Gaia-X), som både har krævet politisk vilje, økonomiske investeringer og nye samarbejder mellem offentlige myndigheder, fonde og private aktører.
- Der er en generel efterspørgsel på flere (fælles)europæiske løsninger, som kan udgøre reelle og suveræne alternativer til dominerende digitale teknologier. Fælles samarbejder kan mindske adgangsbarrierer for de danske myndigheder og tilbyde nye kompetencefællesskaber og skalafordele.

Der kan opnås øget digital suverænitet gennem virkemidler som skaber transparens og robusthed

Nøgleobservation 2.1 | **Risikobaseret styring som virkemiddel**

- Risikobaseret analyse skaber et fundament for prioritering af indsatser. Ved at anvende kendte værktøjer og vurderingsrammer (risiko- og sårbarhedsanalyser, ISO-standarder, NIS2-tiltag mv.) kan myndigheder arbejde struktureret med at kortlægge afhængigheder og risici i og på tværs af teknologistakken ud fra kritikalitet. Herfra kan myndighederne vurdere den samlede risikoeksponering og beslutte konkrete handlinger (jf. cases fra den finansielle sektor og Københavns kommune).
- Det er vigtigt, at analyser omsættes til handlinger og reel styringspraksis, så overblik og risikovurderinger løbende opdateres.

Nøgleobservation 2.2 | **Exit-strategier som virkemiddel**

- Exit-strategier kan understøtte myndighedens udskiftning af leverandører og/eller løsninger med færre risici. Strategien kan bl.a. indeholde procedurer for sikker dataoverførsel, sletning af data hos leverandør, driftskontinuitet samt konkrete planer med tidsramme, governance og risikobetragtninger (jf. casen fra Bankdata og erfaringer fra bl.a. SKI).
- Som led i exit-strategien kan der arbejdes med dokumentation, interoperabilitet og API-adgang samt aftaler med leverandør om fx dataportabilitet og åbne standarder. Ligeledes kan en modulær arkitektur være med til at understøtte mulighederne for at reducere omkostningerne ved fremtidige leverandørskift.

Nøgleobservation 2.3 | **Beredskabsplaner som virkemiddel**

- Hvor exit-planer handler om at beskrive en (erfaringsbaseret) proces til at skifte leverandør eller flytte data og systemer, handler beredskabsplaner om at håndtere uventede driftsforstyrrelser og kunne genoprette data og kritiske it-systemer og sikre fortsat drift, selv under en nødsituation (jf. case fra den finansielle sektor og erfaringer fra bl.a. Statens It).
- Det er en central læring fra den finansielle sektor, at organiationer skal opbygge en kultur for kontinuerlig forbedring, hvor governance, risiko-mapping og beredskabsplaner løbende opdateres i takt med ændringer i trusselsbilledet og regulatoriske krav.

Der kan opnås øget digital suverænitet gennem virkemidler som skaber forandring og handlekraft

Nøgleobservation 2.4 | **Indkøb og kravstillelse som virkemiddel**

- Der kan stilles krav til, at leverandører skal være baseret i EU eller opfylde bestemte suverænitetskriterier, bl.a. krav om hosting i EU eller brug af forventede EU-certificerede cloud-tjenester.
- Krav kan også omfatte åbne standarder (tilgængelige tekniske specifikatoner) og API'er, så løsninger ikke låser organisationer til bestemte platforme og proprietære systemer – evt. i kombination med krav til OSS (jf. cases fra Bankdata, OS2 og STIL).
- Der ses eksempler på indkøbs- og udviklingsmodeller, hvor der etableres nye strategiske partnerskaber mellem myndigheder og europæiske tech-virksomheder for at stimulere markedet og understøtte finansiering og kapacitet til skalering (jf. cases Holland GPT-NL, ZenDis og Schleswig-Holstein).

Nøgleobservation 2.5 | **Alternative løsninger som virkemiddel – især OSS**

- Myndigheder kan sikre en øget grad af digital suverænitet ved at udskifte forskellige elementer i teknologistakken med kendte alternativer – OSS såvel som proprietære løsninger. Her er det vigtigt at overveje erfaringsgrundlaget. Selvom der fx er erfaringer med alternative kontorpakker og samarbejdsværktøjer i Tyskland, vil overførbarheden til en dansk kontekst ikke være 1:1 pga. den høje grad af digitalisering i Danmark, hvor der fx vil være andre behov for integrationer og data for at opretholde nuværende niveau af funktionalitet og afledt produktivitet.
- Der kan ligeledes etableres nye alternativer, fx på AI-området som et eksempel på et nyt felt uden legacy-bindinger (fx i Frankring – Mistral AI og AI-platformen Albert og Holland – GPT-NL).
- Anvendelse af OSS er et gennemgående greb på tværs af de undersøgte cases, hvor mange af løsningerne helt eller delvist baserer sig på OSS.

Nøgleobservation 2.6 | **Parallelle løsninger som virkemiddel**

- Der ses eksempler på myndigheder, som arbejder med at have parallelt kørende løsninger til overlappende formål, hvilket giver øget fleksibilitet samt fall-back og back-up-muligheder, hvis der opstår et behov for at skifte løsning eller flytte data.
- Et eksempel er cloud-området, hvor der er eksempler på myndigheder, som både bruger såkaldte "private clouds", europæiske clouds samt hyperscalers til udvalgte opgaver (fx Aarhus Kommune, Home Office og STIL). Flere overvejer desuden den strategiske balance mellem cloud og on-prem-løsninger. Et andet eksempel er digitale kontorpakker, hvor der ses myndigheder, som etablerer alternative open source-løsninger, der kan tages i anvendelse i en situation, hvor "standardløsningen" ikke er tilgængelig (fx Aarhus Kommune og Statens It).

Nøgleobservation 2.7 | **Ejerskab som virkemiddel**

- Der kan opnås øget kontrol gennem en større grad af ejerskab. Der ses eksempler på myndigheder, som ejer egne løsninger (Home Office, STIL, DIGST, Sundhedsdatastyrelsen mv.), der enten udvikles in-house eller i samarbejde med private it-leverandører, men hvor myndigheden bibeholder IP-rettigheder.
- Der ses også eksempler på andre former for ejerskab, fx ejerskab til data og udvidet brugsret til kode (KOMBIT) eller reelt ansvar for udvikling og vedligehold af open source-løsninger (OS2, Schleswig-Holstein, STIL).
- Ejerskab kan også omfatte aktiver og udstyr fx på datacententer- og netværksområdet (fx Region Nordjyllands Tier 4-datacenter)

Digital suverænitet kræver omstilling og investeringer både teknologisk, organisatorisk og kompetencemæssigt

Nøgleobservation 3.1 | **Digital suverænitet kræver omstilling og investeringer**

- Erfaringer peger entydigt på, at digital suverænitet kræver omstilling og investeringer, hvilket myndighederne er nødt til at overveje som led i fastlæggelsen af egne strategier på området. Investerings- og omstillingsbehov afhænger af de virkemidler, som myndighederne ønsker at anvende, jf. case-beskrivelser.
- Fx er OSS ikke er gratis at anvende, men forbundet med investeringer i kompetencer, implementering, vedigeholdelse samt governance, sikkerhed og support.
- Når myndigheden påtager sig et større ansvar for udvikling og vedligehold af OSS (typisk Copyleft eller Permisive licenser kombineret med en Outbound-tilgang) vil der være større krav til interne tekniske kompetencer, end proprietære alternativer. Manglende intern ekspertise kan føre til stigende afhængighed af eksterne kompetencer som fx it-specialister.

Nøgleobservation 3.2 | **Behov for forskellige typer af investeringer**

- Der er behov for både at investere i tekniske løsninger, organisatoriske tiltag og kompetencer for at arbejde struktureret med digital suverænitet. Det er en erfaring på tværs af cases, at migrering til alternative teknologivalg stiller nye krav til myndighederne.
- Der kan fx være behov for nye kompetencer og governance-modeller til samarbejde med it-leverandører ved indførelse af OSS, der kan være nye styringsopgaver, når myndigheder migrerer fra større hyperscalers til mindre europæiske cloud-leverandører samt behov for juridiske, tekniske og analytiske kompetencer til at gennemføre robuste risikoanalyser, udarbejde exit-strategier og stille de rette krav til åbne standarder og interoperabilitet (jf. cases fra Aarhus Kommune, EU-Kommissionen, Schleswig-Holstein).

Nøgleobservation 3.3 | **Transformative alternativer kræver nye økosystemer**

- Mere transformative alternativer, hvor myndigheden udskifter en større del af sine digitale løsninger (fx Home Office, Schleswig-Holstein), eller hvor der etableres nye alternative løsninger med et større udbredelsespotentiale, kræver typisk et økosystem af fx it-leverandører, non-profit-organisationer, fonde, offentlige myndigheder mv. for at kunne realiseres (se bl.a. EuroStack, GPT-NL, OS2, ZenDis). Der pålægger den ansvarlige myndighed/aktør en central opgave med at koordinere og styre udviklingen af økosystemet.
- Det er etableret erfaringer med nye forretningsmodeller via offentlig-privat samarbejde, hvor staten/den offentlige sektor sikrer en basisfinansiering ifm. etablering af produktudvikling, hvorefter der etableres en forretningsmodel rundt om et til flere konkrete produkter med licensindtægter og forskellige servicetilbud (se bl.a. GPT-NL, OS2, ZenDis).

Nøgleobservation 3.4 | **Alternativer skaber nye afhængigheder**

- Når der etableres alternativer via nye leverandører og forretningsmodeller skabes der altid nye afhængigheder. Det gælder både proprietære løsninger (fx GPT-NL) og OSS (fx ZenDis). Overblik og styring er derfor fortsat centrale discipliner, når myndighederne udskifter løsninger, for at reducere afhængigheder og sårbarheder.
- Det gælder også for OSS, at der kan være nye afhængigheder til bestemte distributionsplatforme eller cloud-tjenester, hvilket kan skabe nye former for leverandørbindinger. Et andet eksempel er, at OSS ofte er drevet af frivillige eller mindre organisationer, hvilket kan skabe nye sårbarheder, hvis kritiske opdateringer eller sikkerhedsrettelser udebliver.

Kapitel 4

PA’s forslag til løsningsspor

Introduktion til kapitlet om løsningsspor

Opstillingen af løsningsspor og indsatser tager afsæt i efaringsbaserede input fra den gennemførte dataindsamling samt PA's faglige vurderinger. PA har identificeret tre centrale løsningsspor med 12 understøttende indsatser og fire anbefalinger som input til parternes videre arbejde med digital suverænitet.

Datagrundlag og forudsætninger

- Løsningsspor og indsatser er formuleret med afsæt i parternes forståelse af digital suverænitet og ambitionen i den fællesoffentlige digitaliseringsstrategi om at fremme digital suverænitet i den offentlige sektor*.
- Forslagene skal ses i lyset af den anvendte forståelses- og analyseramme, som omfatter et bredt fokus på tværs af både digitale løsninger og it-infrastruktur.
- Forslagene er baseret på PA's faglige vurderinger og den gennemførte dataindsamling. Det bemærkes, at der ikke er etableret et mere konkret nationalt eller fællesoffentligt målbillede for digital suverænitet, hvilket indeværende analyse kan være et indspil til. Regeringen har besluttet at etablere en national handleplan i 2026, hvorfor dette ikke indgår som konkret indsats.
- Forslagene har primært karakter af rammesættende tiltag og rummer ikke forslag til konkrete teknologiske alternativer. Der gives dog en række eksempler på alternative digitale løsninger ifm. løsningssporet om organisering, finansiering og kompetencer.

Tilgang til opstilling af løsningsspor

- PA har opstillet tre løsningsspor, som udtrykker forskellige måder, hvorpå myndighederne kan arbejde med at styrke den digitale suverænitet. Disse spor introduceres indledningsvis.
- For hvert spor er der opstillet en række mulige indsatser, som efterfølgende præsenteres i et samlet overblik.
- Alle indsatser er efterfølgende udfoldet i en ensartet struktur med fokus på:
  - Kort beskrivelse af forslaget og dets erfaringsgrundlag
  - Niveau hvor forslaget kan realiseres (myndighed, sektor, fællesoffentligt)
  - Relativ og overordnet vurdering kompleksitet
  - Overordnet vurdering af gevinster og forudsætninger som fx kompetencer, investeringer mv.
- Kapitlet afrundes med PA's samlede anbefalinger.

**På tværs af den danske offentlige sektor oplever man i stigende grad udfordringer med den voksende afhængighed af digitale tjenester fra få, meget store udenlandske virksomheder og deres indflydelse på den digitale infrastruktur. De fællesoffentlige parter vil derfor analysere udvalgte myndigheders teknologivalg, fremme overblik over alternative udbydere og tjenester samt skabe øget markedspluralitet og konkurrence, der kan reducere leverandørafhængighed, økonomiske sårbarheder og støtte myndighedernes suverænitet over egne løsninger og data. Samtidig skal pilotforsøg i den offentlige sektor supplere arbejdet og bidrage med praktisk erfaringsopsamling på området med henblik på opfølgende aktiviteter (Digitaliseringsstrategien 2026-2029 (udarbejdet af Digitaliseringsstyrelsen, KL og Danske Regioner).*

PA har identificeret tre særligt relevante løsningsspor, som repræsenterer forskellige indsatser til at styrke myndighedernes digitale suverænitet

PA har med udgangspunkt i den gennemførte erfaringsopsamling og casestudier identificeret tre løsningsspor. For hvert spor er der beskrevet en række overordnede indsatser, som den danske offentlige sektor kan lade sig inspirere af. Indsatserne vil variere med hensyn til ambitionsniveau, kompleksitet og gevinster. Der er både identificeret indsatser, som kan implementeres af den enkelte myndighed, og indsatser, som kan implementeres nationalt eller på sektorniveau (stat, regioner, kommuner).

Spor 1 | Risikobaseret prioritering og styring af afhængigheder

- Indsatser, der rammesætter og styrker myndighedernes arbejde med risikobaseret prioritering og styring af de mest kritiske digitale afhængigheder.

Spor 2 | Indkøb, krav og arkitektur

- Indsatser, der rammesætter og styrker myndighedernes arbejde med indkøb af digitale løsninger og it-infrastruktur, kravstillelse og leverandørsamarbejde samt arkitekturstyring.

Spor 3 | Organisation, finansiering og kompetencer

- Indsatser, der rammesætter og styrker myndighedernes arbejde med at opbygge organisatoriske kapabiliteter, finansieringsmekanismer og kompetencer.
- Tiltag skal understøtte spor 1 og 2 og desuden fremme myndighedernes arbejde med alternative løsninger for at reducere kritiske afhængigheder.

PA foreslår 12 konkrete indsatser på tværs af de tre løsningsspor

01 | Risikobaseret prioritering og styring af afhængigheder

- 1.1 Analyse og risikovurdering af digitale løsninger
- 1.2 Exit-strategier og beredskabsplaner
- 1.3 Stærkere audit-mekanismer

02 | Indkøb, krav og arkitektur

- 2.1 Markedsafdækning med danske it-leverandører
- 2.2 Genbesøg af it- og arkitekturstrategier
- 2.3 Fælles “suverænitetspakke” til offentlige it-udbud
- 2.4 Fælles indkøb af suveræne cloud-ydelser

03 | Organisation, finansiering og kompetencer

- 3.1 Strategiske alliancer med europæiske lande
- 3.2 Stærkere vidensgrundlag om digitalt suveræne løsninger
- 3.3 Strategisk indkøbspulje til udviklingsprojekter
- 3.4 Lokal transformationsenhed for digital suverænitet
- 3.5 Nationalt center for digital suverænitet og innovation

1.1 Analyse og risikovurdering af digitale løsninger

Formål og indhold

Formål: At understøtte myndighedernes identifikation af egne afhængigheder og risici mhp. prioritering af lokale indsatser for at øge den digitale suverænitet.

Indhold: Myndighederne gennemfører analyser af egen teknologistak, herunder adgang til data. Der foretages dybdegående analyse på teknologier, som enten er samfundskritiske eller forretningskritiske*.

Der etableres et fælles analyse- og "suverænitetstjek"-værktøj med scorecard og modenhedsvurdering, som tager afsæt i eksisterende værktøjer (fx statens rammeværk for it-porteføljestyring, NIS2 mv.).

Der vil være brug for et tilpasset rammeværk, som er målrettet problematikker og kritiske afhængigheder i relation til digital suverænitet, hvor der sikres synergi mellem øvrige risikovurderinger drevet af krav til cyber- og informationssikkerhed.

Erfaringsgrundlag: Finansiel sektor, Københavns Kommune, telesektor, Økonomistyrelsen og Statens It-Råd med fokus på it-styring i staten.

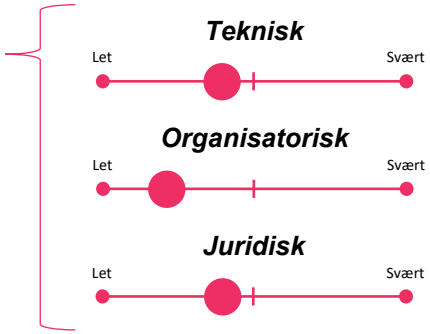
Vurdering

Kompleksitet

Niveau: Den enkelte myndighed, hvor analyseramme udvikles fællesoffentligt.

Tidshorisont: Kan gennemføres på <12 måneder for den enkelte myndighed.

Afhængigheder: Kobling til myndighedens organisering af indsatser, der fremmer digital suverænitet, jf. indsats. 3.4.



Udfordringer adresseret

- 01 | Høj afhængighed af større leverandører og manglende konkurrence
- 02 | Manglende kontrol og transparens over egne data
- 03 | Begrænset kontrol og styring af digitale løsninger
- 04 | Sårbarheder i den digitale forsyningssikkerhed

Gevinster

- Øget transparens over kritiske afhængigheder og risici.
- Bedre risikobaseret prioritering af indsatser for øget digital suverænitet.

Forudsætninger for effektiv implementering

- Ressourcer og økonomi til fælles udvikling af analyseværktøj med dimensioner og risikoscore baseret på digital suverænitet.
- Fællesoffentlig eller sektorbaseret målsætning og evt. forpligtende aftale om at gennemføre analysen hos alle myndigheder.
- Prioritering af ressourcer i den enkelte myndighed til at gennemføre analysen.

Samfundskritisk: It-system, hvor større driftsforstyrrelser resulterer i væsentlige udfordringer for samfundet som helhed i form af økonomiske tab hos stat, virksomheder eller borgere, større misbrug af personfølsomme data og rettigheder, længerevarende nedbrud af kritisk infrastruktur eller reelle trusler for den nationale sikkerhed. Forretningskritisk: It-system, hvor driftsforstyrrelser kan medføre, at størstedelen af myndighedens medarbejdere ikke kan arbejde, eller at myndigheden vanskeligt kan overholde sine forvaltningsmæssige forpligtelser.

1.2 Exit-strategier og beredskabsplaner

Formål og indhold

Formål: At understøtte myndighedernes arbejde med at udarbejde exit-strategier og identificere konkrete handlemuligheder de steder, hvor myndigheden har de største digitale sårbarheder.

Indhold: For områder med størst sårbarhed udarbejder den enkelte myndighed konkrete exit-strategier og/eller kontinuitets- og beredskabsplaner, afhængig af myndighedens konkrete vurderinger af forholdet mellem risikoeksponering, egne kapabiliteter og investeringsmuligheder.

Planerne kan fx omfatte "lagerstrategier" med tilgængelige alternative løsninger, hybrid/multi-cloud-miljøer, der kan give fleksibilitet ifm. dataflyt samt drift og udvikling af digitale løsninger eller egentlige exit-strategier inkl. konkrete implementeringsplaner, der giver mulighed for at igangsætte udskiftninger af løsninger og komponenter. Indsatsen tilrettelægges efter kritikalitet med fokus på samfundskritiske og forretningskritiske løsninger. Audits kan gennemføres af myndigheden selv, i samarbejde med eksterne specialister eller i samarbejde mellem myndigheder.

Erfaringsgrundlag: Finansiel sektor, Statens IT, STIL.

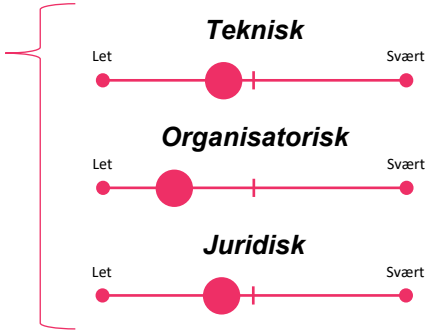
Vurdering

Kompleksitet

Niveau: Den enkelte myndighed – evt. via samarbejder som fx Det Fælleskommunale Databehandlingssekretariat.

Tidshorisont: Kan gennemføres på <12 måneder for den enkelte myndighed.

Afhængigheder: Kan gennemføres i forlængelse af indsats 1.1. Kobling til myndighedens organisering, jf. indsats 3.4.



Udfordringer adresseret

- 01 | Høj afhængighed af større leverandører og manglende konkurrence
- 02 | Manglende kontrol og transparens over egne data
- 03 | Begrænset kontrol og styring af digitale løsninger
- 04 | Sårbarheder i den digitale forsyningssikkerhed

Gevinster

- Øget robusthed og modstandsdygtighed.
- Reduceret risiko ved negativ påvirkning af drift.
- Bedre grundlag for at identificere mulige alternative løsninger.

Forudsætninger for effektiv implementering

- Kræver forudgående analyse af kritiske afhængigheder og samlet risikoeksponering, jf. indsats 1.1.
- Fællesoffentlig eller sektorbaseret målsætning og evt. forpligtende aftale om at gennemføre analysen hos alle myndigheder.
- Prioritering af ressourcer i den enkelte myndighed til opgaven samt evt. økonomi til omkostninger til it-leverandører.

1.3 Stærkere audit-mekanismer

Formål og indhold

Formål: At sikre fuld indsigt i, hvordan data behandles på tværs af hele leverandørkæden mhp. at reducere risikoen for uautoriseret adgang eller dataoverførsel til tredjelande.

Indhold: Myndighederne etablerer stærkere audit-mekanismer for databehandling for alle eksterne leverandører, som også inkluderer tredje- og fjerdepartsleverandører. Audits kan prioriteres efter kritikalitet og risikoeksponering, jf. indsats 1.1, og skal ses i sammenhæng med øvrige tiltag drevet af krav til cyber- og informationssikkerhed. For myndigheder, som er underlagt NIS2, vil der være et metodisk sammenfald i fremgangsmåden til afdækning af kritiske leverandørkæder.

Som led i indsatsen skabes overblik over data, dokumentation af compliance set ift. GDPR, EU AI Act og gældende nationale sikkerhedskrav samt udfordringer i underleverandørers processer (fx cloud-hosting uden for EU). Indsatsen kan suppleres med uafhængige sikkerhedsrevisioner af udvalgte løsninger og kan også kombineres med kravstillelse ifm. kommende udbud og eksisterende kontrakter.

Erfaringsgrundlag: Finansiel sektor, KOMBIT, Sundhedsdatastyrelsen.

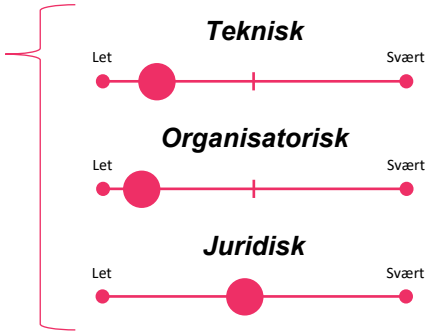
Vurdering

Kompleksitet

Niveau: Den enkelte myndighed.

Tidshorisont: Kan gennemføres på <6 måneder for den enkelte myndighed.

Afhængigheder: Kan gennemføres i naturlig forlængelse af indsats 1.1. Kobling til myndighedens organisering, jf. indsats 3.4 samt kravstillelse til leverandører, jf. indsats 2.3.



Udfordringer adresseret

- 01 | Høj afhængighed af større leverandører og manglende konkurrence
- **02 | Manglende kontrol og transparens over egne data**
- 03 | Begrænset kontrol og styring af digitale løsninger
- **04 | Sårbarheder i den digitale forsyningssikkerhed**

Gevinster

- Øget transparens over databehandling og compliance.
- Bedre beredskab gennem struktureret og kontinuerlig overvågning.

Forudsætninger for effektiv implementering

- Kræver forudgående analyse af kritiske afhængigheder og samlet risikoeksponering, jf. indsats 1.1.
- Intern afklaring af snitflader og synergier til NIS2-initiativer og øvrige audits på it-området.
- Interne ressourcer i myndigheden til at etablere og gennemføre audit-processer, inkl. værktøjer til overvågning og rapportering.

2.1 Markedsafdækning med danske it-leverandører

Formål og indhold

Formål: At afklare muligheder for samarbejde mellem offentlige myndigheder og it-leverandører, perspektiver på den fremadrettede it-udvikling samt kapacitet og kompetencer i markedet.

Indhold: Der gennemføres en markedsafdækning med et udsnit af danske it-leverandører på tværs af teknologistakkens domæner for at afklare, hvordan markedet kan bidrage til at sikre en øget grad af digital suverænitet.

Konkret undersøges leverandørernes vurdering af, hvordan myndigheder og leverandører kan samarbejde om digital suverænitet, både ifm. kommende udbud og justeringer i eksisterende kontrakter. Der kan fx fokuseres på, hvordan danske leverandører kan bidrage med at levere kritiske teknologier (cloud, AI, sikkerhed, data-hosting) under EU/DK-jurisdiktion, tilbyde EU-baserede sovereign cloud-løsninger, dokumentere leverandørkæder, levere "audit-klare løsninger" med sporbarhed og compliance-rapporter samt fælles udviklings- og innovationsprojekter som fx co-creation af open source-løsninger for at reducere afhængighed af proprietære platforme.

Erfaringsgrundlag: Aarhus Kommune, Sundhedsdatastyrelsen, OS2.

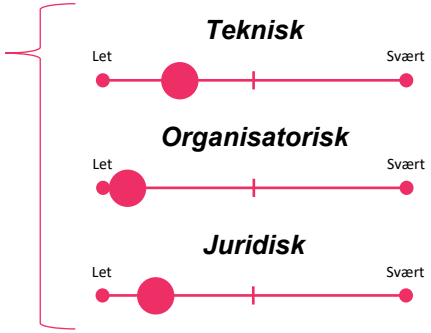
Vurdering

Kompleksitet

Niveau: Fællesoffentligt.

Tidshorisont: Kan gennemføres på <6 måneder som fællesoffentligt initiativ.

Afhængigheder: Kan bidrage med relevant input til indsats 2.3 og 2.4.



Udfordringer adresseret

- 01 | Høj afhængighed af større leverandører og manglende konkurrence
- 02 | Manglende kontrol og transparens over egne data
- 03 | Begrænset kontrol og styring af digitale løsninger
- 04 | Sårbarheder i den digitale forsyningssikkerhed

Gevinster

- Øget indsigt i markedets kapabiliteter og begrænsninger.
- Styrket samarbejde mellem myndigheder og it-leverandører.
- Bedre grundlag for kommende udbud og kontrakter.

Forudsætninger for effektiv implementering

- Tydelig analyseramme, succeskriterier og centrale tematikker for afdækningen.
- Robust metode, der sikrer repræsentativitet på tværs af stakken, produktkategorier, virksomhedsstørrelser mv.
- Struktureret opsamling af resultater inkl. kommunikation til de offentlige myndigheder.

2.2 Genbesøg af it- og arkitekturstrategier

Formål og indhold

Formål: At sikre, at myndighederne genovervejer it- og arkitekturstrategier for bedst muligt at kunne agere strategisk for at opnå øget digital suverænitet.

Indhold: Indsatsen indebærer, at myndighederne genbesøger og revurderer egne it- og arkitektur-strategier med fokus på bl.a. at fremme brugen af open souce-software (OSS) og åbne standarder, modulopbygget arkitektur via containerisation, hybride cloud-miljøer for at reducere proprietære bindinger, fremme konkurrence på markedet og alternative (fall-back) løsninger samt for at understøtte, at offentlige it-systemer uanset valg af software kan udveksle informationer på tværs. Myndighederne kan herfra beskrive tydelige mål, principper og krav til leverandører.

Som led i indsatsen vurderer hver myndighed nuværende kapabiliteter og modenhedsniveauer, herunder anvendte leverancemodeller, udviklingsmodeller, open source-software, standarder mv. Desuden sikres det, at digital suverænitet fremtræder tydeligt i FDA arkitekturprincipper.

Erfaringsgrundlag: Aarhus Kommune, Bankdata, Digitaliseringsstyrelsen (FDA), Home Office, KL/Kombit (rammearkitektur), Statens IT, Sundhedsdatastyrelsen (husregler), STIL.

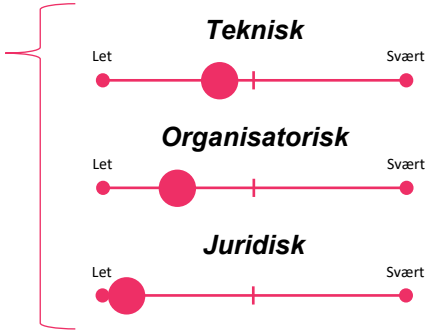
Vurdering

Kompleksitet

Niveau: Den enkelte myndighed.

Tidshorisont: Kan gennemføres på <6 måneder for den enkelte myndighed.

Afhængigheder: Hænger tæt sammen med indsats 3.4 om etablering af lokal enhed for digital suverænitet. Sætter retning og ramme for lokale projekter om digital suverænitet.



Udfordringer adresseret

- 01 | Høj afhængighed af større leverandører og manglende konkurrence
- 02 | Manglende kontrol og transparens over egne data
- **03 | Begrænset kontrol og styring af digitale løsninger**
- 04 | Sårbarheder i den digitale forsyningssikkerhed

Gevinster

- Bedre kobling mellem teknologivalg og organisatoriske kapabiliteter – også på længere sigt.
- Bedre koordination mellem forskellige indsatser og sammenhænge på tværs af teknologistakken gennem arkitekturprincipper, standarder og teknologivalg.

Forudsætninger for effektiv implementering

- National handleplan og principper for digital suverænitet som kan understøttes af evt. forpligtende mål og aftaler.
- Forankring af indsats og strategi i topledelsen og med opbakning hos ansvarlig leder for digitalisering og teknologi.
- Interne ressourcer i myndigheden til at opdatere/udvikle it- og arkitekturstrategi.

2.3 Fælles “suverænitetspakke” til offentlige it-udbud

Formål og indhold

Formål: At etablere en samlet ”videnspakke” med konkrete eksempler på, hvordan offentlige myndigheder kan formulere krav om øget digital suverænitet mhp. skabe øget konkurrence og stimulere markedet. Pakken implementeres i relevante SKI-aftaler.

Indhold: Med afsæt i tilgængelig viden og udbudsmaterialer etableres en samlet suverænitetspakke, som kan understøtte myndighederne ifm. kommende it-udbud og justeringer i nuværende kontrakter. Relevante SKI-aftaler opdateres med inspiration fra indførelsen af grønne krav og sikkerhedskrav.

Pakken kan bl.a. indeholde konkrete eksempler på krav og kontraktklausuler om fx dataflyt (portabilitet), datalokalisering, krypteringsnøgler, omkostningsfri adgang til data, open source-komponenter, privacy-enhancing technologies (PETs), kode-reviews, transparens over leverandørkæder og audits, standardiserede snitflader, udvidet brugsret til kode, åben datamodel, åbne API’er, åbne frameworks og kodebiblioteker, åbne standarder mv. Pakken bør suppleres med vejledning til evalueringsmodeller med anvendelse af nye suverænitetskriterier som input til vurdering af leverandører og produkter.

Erfaringsgrundlag: EU-Kommissionen, Digitaliseringsstyrelsen og KL (arkitektur og OSS), OS2.

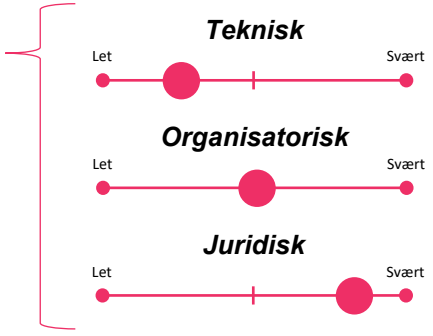
Vurdering

Kompleksitet

Niveau: Fællesoffentligt.

Tidshorisont: Kan gennemføres på 1-2 år (fsv. angår SKI aftaler, kan krav formentlig implementeres hurtigt i de dynamiske indkøbssystemer, men først ved genudbud ifm. rammeaftalerne)

Afhængigheder: Kan med fordel etableres med input fra markedsafdækning (indsats 2.1).



Udfordringer adresseret

- 01 | Høj afhængighed af større leverandører og manglende konkurrence
- 02 | Manglende kontrol og transparens over egne data
- 03 | Begrænset kontrol og styring af digitale løsninger
- 04 | Sårbarheder i den digitale forsyningssikkerhed

Gevinster

- Bedre forudsætninger for kravstillelse til digital suverænitet i den enkelte myndighed.
- Bedre mulighed for at påvirke leverandør-markedet i retning af mere digitalt suveræne løsninger.

Forudsætninger for effektiv implementering

- Ressourcer og økonomi til fælles udvikling af suverænitetspakken samt strategisk afklaring med SKIs bestyrelse.
- Indsamling og strukturering af viden og barrierer fra eksisterende udbudsmaterialer, best-practice eksempler og SKI aftaler.
- Struktureret opsamling af resultater inkl. kommunikation til de offentlige myndigheder.

2.4 Fælles indkøb af suveræne cloud-ydelser

Formål og indhold

Formål: At gennemføre fælles indkøb i den offentlige sektor, som fremmer europæiske og evt. danske alternativer og stimulerer et europæisk marked uden at udelukke bydere fra ikke-europæiske lande.

Indhold: Der gennemføres et til flere nye indkøb af suveræne cloud-ydelser, hvor hvert indkøb har en større volumen på minimum 100 mio. kroner, for at skabe en betydelig interesse for udbuddet – også hos potentielle leverandører i andre lande. Indkøbsgenstanden skal nærmere defineres, men kunne tage afsæt i workload fra store myndigheder eller servicefællesskaber, jf. nedenfor. Der skal stilles krav til suverænitet, som evalueres (med høj vægt) på graden heraf. Udbuddet kunne fx udformes som en rammeaftale med flere delaftaler (lots). Cloud-ydelser vil kunne omfatte infrastructure as a service (IaaS), platform as a service (PaaS) og evt. yderligere services, fx inden for dataplatforme og AI.

Indsatsen kan forankres hos aktører med en central rolle i at drive den digitale udvikling som fx Statens IT (staten) Digital Sundhed Danmark (regioner), tværkommunale it-driftsenheder eller KOMBIT (kommuner). Indsatsen vil også være relevant for de største myndigheder i stat, regioner og kommuner.

Erfaringsgrundlag: EU-Kommissionen, Frankrig (Cloud de Confiance).

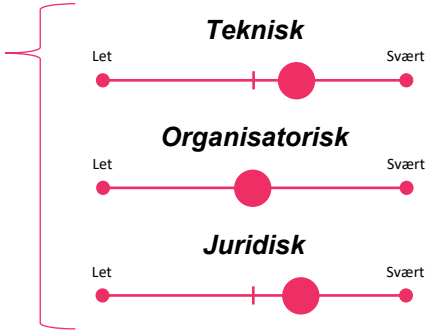
Vurdering

Kompleksitet

Niveau Sektorniveau eller de enkelte myndigheder (såfremt volumen er stor nok). Indsatsen vurderes særlig relevant ifm. samling af kommunernes it-drift i 4-5 nye enheder.

Tidshorisont: Kan gennemføres på et-to år.

Afhængigheder: Der kan indhentes input til denne indsats via markedsafklaring (indsats 2.1) samt input til krav fra indsats 2.3.



Udfordringer adresseret

- 01 | Høj afhængighed af større leverandører og manglende konkurrence
- 02 | Manglende kontrol og transparens over egne data
- 03 | Begrænset kontrol og styring af digitale løsninger
- 04 | Sårbarheder i den digitale forsyningssikkerhed

Gevinster

- Øget digital suverænitet gennem alternative digitale løsninger.
- Stimulering af et europæisk marked for suveræne cloud-ydelser.

Forudsætninger for effektiv implementering

- Strategisk beslutning og tilsagn fra myndigheder om etablering af et til flere indkøb med større økonomisk volumen (+100 mio. kr.)
- Etablering af foranalyse med udbudsstrategi og målrettet markedsdialog mhp. at fastlægge udbudsgenstand.
- Gennemførelse af et til flere EU-udbud med fokus på gensidig læring og genbrug af materialer.

3.1 Strategiske alliancer med europæiske lande

Formål og indhold

Formål: At afklare og beslutte strategiske alliancer med andre europæiske lande for at sikre en hurtigere og mere målrettet acceleration af øget digital suverænitet.
Indhold: Danmark kan gå mere offensivt ind i strategiske alliancer og EU-projekter inden for udviklingen af (1) fælles strategiske greb som fx fælles principper, åbne standarder, certificeringsordninger og konkrete styringsværktøjer og (2) konkrete digitale alternativer, som kan fremme en øget grad af digital suverænitet, jf. erfaringer med europæiske clouds, suveræne AI-løsninger, innovative open source-produkter mv. Mange europæiske lande er allerede i gang, og der er således flere muligheder for at skabe strategiske alliancer og partnerskaber (fx med lande som England, Frankrig, Holland, Italien, Schweitz, Sverige, Tyskland etc.). Dette indsatsforslag vedrører alliancer og partnerskaber på fællesoffentligt/nationalt niveau, men der kan ligeledes afsøges samarbejder ifm. konkrete indsatser i den enkelte myndighed.

Erfaringsgrundlag: Digital Commons EDIC, ESTIA – European Sovereign Tech Industry Alliance, Eurostack, Gaia-X, Holland (Økonomiministeriet) OS2, Sverige (RISE), Schleswig-Holstein, ZenDis.

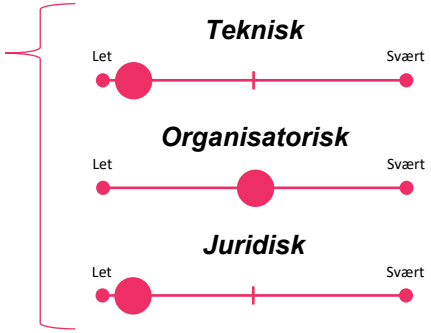
Vurdering

Kompleksitet

Niveau: Fællesoffentligt/nationalt med afsæt i det fællesoffentlige samarbejde.

Tidshorisont: Kan gennemføres på <6 måneder.

Afhængigheder: Stærk kobling til indsats 3.5 om nationalt center for digital suverænitet mhp. synergier og snitflader.



Udfordringer adresseret

- 01 | Høj afhængighed af større leverandører og manglende konkurrence
- 02 | Manglende kontrol og transparens over egne data
- 03 | Begrænset kontrol og styring af digitale løsninger
- 04 | Sårbarheder i den digitale forsyningssikkerhed

Gevinster

- Øget vidensniveau hos centrale aktører.
- Bedre adgang til finansiering og realisering af skalafordele.
- Bedre positionering som ”fast follower” på EU-tiltag.

Forudsætninger for effektiv implementering

- National handleplan og principper for digital suverænitet, som kan rammesætte arbejdet.
- Behov for medfinansiering for at indgå i konkrete EU-initiativer.
- Organisatorisk enhed, som faciliterer, udvikler og koordinerer samarbejder på strategisk niveau.

3.2 Stærkere vidensgrundlag om digitalt suveræne løsninger

Formål og indhold

Formål: At skabe mere viden om muligheder mhp. at øge myndighedernes digitale suverænitet, herunder konkrete virkemidler og deres fordele og barrierer.

Indhold: Via tilgængelig viden og allerede etablerede netværksfora og strategiske enheder hos de fællesoffentlige parter etableres "videnspakker" og understøttende netværksaktiviteter for at sprede viden og erfaringer.

Indsatsen kan til at begynde med tage afsæt i indeværende analyse inkl. de konkrete cases, som viser forskellige virkemidler til øget digital suverænitet.
Parterne bør overveje, hvordan der kan sigtes imod en bredere målgruppe end digitaliseringsansvarlige mhp. at opnå en mere strategisk forankring af agendaen – fx beslutningstagere, leverandører etc.

Erfaringsgrundlag: Digital Commons EDIC, ESTIA – European Sovereign Tech Industry Alliance, Eurostack, Gaia-X, KU, OS2, RISE, ZenDis.

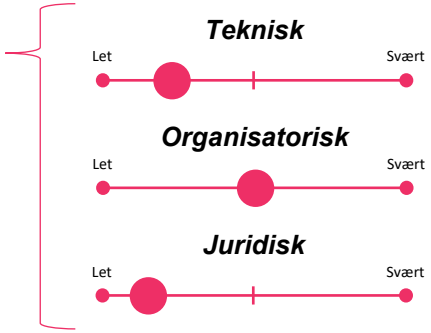
Vurdering

Kompleksitet

Niveau: Sektorniveau med kobling til allerede igangsatte aktiviteter og fora samt fællesoffentlig koordinering via samarbejdet om den fællesoffentlige digitaliseringsstrategi.

Tidshorisont: Kan gennemføres på <12 måneder.

Afhængigheder: Stærk kobling til indsats 3.5 om nationalt center for digital suverænitet mhp. synergier og snitflader.



Udfordringer adresseret

- 01 | Høj afhængighed af større leverandører og manglende konkurrence
- 02 | Manglende kontrol og transparens over egne data
- 03 | Begrænset kontrol og styring af digitale løsninger
- 04 | Sårbarheder i den digitale forsyningssikkerhed

Gevinster

- Øget vidensniveau hos centrale aktører og myndigheder.
- Bedre spredning af viden til beslutningstagere og øvrige interessenter.
- Øget acceleration af konkrete initiativer hos myndighederne.

Forudsætninger for effektiv implementering

- Afklaring af ambitionsniveau og målgrupper både på sektorniveau og i det fællesoffentlige samarbejde.
- Strategisk kobling til igangsatte netværk og initiativer samt samarbejde mellem aktører, som arbejder med agendaen.
- Strategisk kobling til relevante ressortministerier, forskning, interesseorganisationer, tænketanke etc.

3.3 Strategisk indkøbspulje til udviklingsprojekter

Formål og indhold

Formål: At etablere en finansieringsmekanisme, der skaber incitament til at gennemføre indsatser om at etablere digitalt suveræne alternativer hos den enkelte myndighed eller via partnerskaber mellem myndigheder og øvrige strategiske aktører, herunder it-leverandører, teknisk kapable non-profit-organisationer, DTU (Computerome), KOMBIT, OS2, Statens It mv. Mekanismen vil således kunne stimulere offentlig-private samarbejder og nye økosystemer inden for prioriterede områder som fx AI-platform, suveræne clouds og hosting-services, digital arbejdsplads, bruger- og rettighedsstyring, sagsbehandling, skole-PC mv.

Indhold: Puljen medfinansierer strategiske projekter, der implementerer konkrete alternativer, der både kan omfatte open source-løsninger, proprietære løsninger og fælles it-infrastruktur. Puljen skal fungere som en incitamentstruktur for myndighederne og kan kombineres med supplerende EU-finansiering og fælles projekter på tværs af europæiske lande. Puljen kan evt. etableres som lånepulje.

Erfaringsgrundlag: Fællesoffentlig digitalisering med inspiration i bl.a. AI-signaturprojekter, bølgeplaner, skaleringssamarbejder og teknologipuljer.

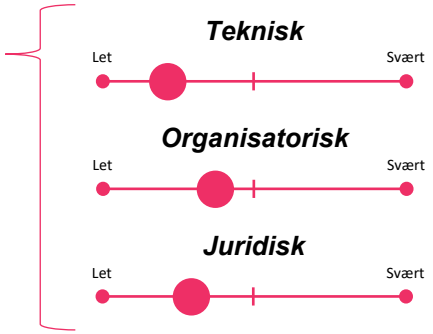
Vurdering

Kompleksitet

Niveau: Fællesoffentligt.

Tidshorisont: Kan gennemføres på <12 måneder.

Afhængigheder: Tæt kobling til indsats 3.5, idet et nationalt center vil kunne administrere puljer og følge strategiske projekter.



Udfordringer adresseret

- 01 | Høj afhængighed af større leverandører og manglende konkurrence
- 02 | Manglende kontrol og transparens over egne data
- 03 | Begrænset kontrol og styring af digitale løsninger
- 04 | Sårbarheder i den digitale forsyningssikkerhed

Gevinster

- Øget acceleration af konkrete initiativer hos myndighederne.
- Øget homogenitet i fremgangsmåde via krav til samarbejdsmodel og koncepter.
- Acceleration af konkrete initiativer hos myndighederne.

Forudsætninger for effektiv implementering

- National handleplan og principper for digital suverænitet, som kan rammesætte arbejdet..
- Afklaring af strategisk ambition, fokus og finansieringsniveau.
- Afklaring af styrings-setup og samarbejde mellem de fællesoffentlige parter.

3.4 Lokal transformationsenhed for digital suverænitet

Formål og indhold

Formål: At etablere en central enhed hos den offentlige myndighed, som får til opgave at gennemføre strategiske analyser og afklaringer samt etablere og gennemføre mere transformative indsatser.

Indhold: Den enkelte myndighed etablerer en lokal kapacitet, som kan organiseres som en permanent enhed eller som et transformativt program. Indsatsen sikrer, at myndigheden udvælger strategiske prioriteringer og har forudsætningerne for at eksekvere disse (fx kompetencer, finansiering mv.).

Mandatet vil afhænge af myndighedens strategi og prioriterede indsatser. Det kan omfatte indsatser for risikovurdering, exit-strategier, beredskabsplaner, arkitektur, kravstillelse og indkøb, jf. denne analyses løsningsspor 1 og 2. Det kan også omfatte mere transformative indsatser, hvor teknologi udskiftes. Baseret på indeværende analyse kan relevante projekter fx omfatte suveræn AI-platform, suveræne clouds og hosting-services, digital arbejdsplads, bruger- og rettighedsstyring, sagsbehandling, suveræn skole-PC mv.

Erfaringsgrundlag: Aarhus Kommune, Bankdata, Schleswig-Holstein.

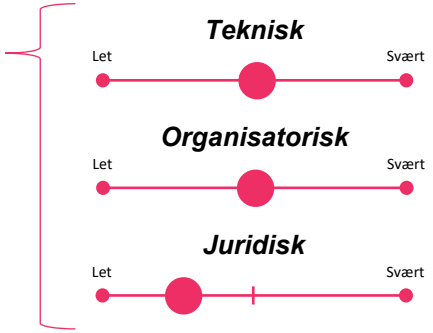
Vurdering

Kompleksitet

Niveau: Den enkelte myndighed.

Tidshorisont: Selve enheden kan etableres på <12 måneder inkl. foranalyse, beslutningsproces og design.

Afhængigheder: Strategisk kobling til indsats 3.5 (centralt suverænitetscenter) samt indsats 3.3. vedr. puljer til finansiering.



Udfordringer adresseret

- 01 | Høj afhængighed af større leverandører og manglende konkurrence
- 02 | Manglende kontrol og transparens over egne data
- 03 | Begrænset kontrol og styring af digitale løsninger
- 04 | Sårbarheder i den digitale forsyningssikkerhed

Gevinster

- Øget vidensniveau og opbygning af kapabiliteter.
- Øget digital suverænitet gennem bedre kontrol, styring og handlefrihed.
- Mulig acceleration af konkrete initiativer hos myndighederne.

Forudsætninger for effektiv implementering

- Afklaring af myndigheders strategiske ambition, fokus, egne kapabiliteter og aktuel situation samt finansieringsniveau.
- Sikre kobling til eksisterende netværk og viden samt afsøge mulige partnerskaber med markedet og andre aktører.
- Strategisk kobling til centrale beslutningstager samt forankring enten politisk eller i topledelsen.

3.5 Nationalt center for digital suverænitet og innovation

Formål og indhold

Formål: Der etableres et nationalt center for digital suverænitet, som får til opgave at være drivkraft for at facilitere og udvikle strategiske nationale initiativer og prioriterede signaturprojekter.

Indhold: Centeret vil fx kunne gennemføre analyser, understøtte videndeling med myndigheder og øvrige strategiske aktører, udarbejde metoder og best practice. Centeret vil kunne bistå med rådgivning og praktisk bistand til myndighederne ifm. lokale analyser og migreringsprocesser til alternative teknologivalg. Endelig vil centeret kunne opbygge stærke kompetencer inden for OSS samt facilitere, igangsætte og evt. (produkt)udvikle digitalt suveræne alternativer (kan også fungere som et OSPO).

Mere konkret kan centeret udvikle analyseværktøjer til risikovurdering, suverænitetspakke til offentlige it-indkøb og samarbejde med SKI om krav til digital suverænitet. Centeret kan understøtte og evt. tage reelt ansvar for udvikling af suveræne alternativer (fx AI-platform, suveræne clouds og hosting-services, digital arbejdsplads, bruger- og rettighedsstyring, sagsbehandling, skole-PC mv.). Organisationsform, mandat, kapabiliteter og governance vil nærmere skulle afklares.

Erfaringsgrundlag: Frankrig (ISN - Institut de la Souveraineté Numérique), Tyskland (ZenDis).

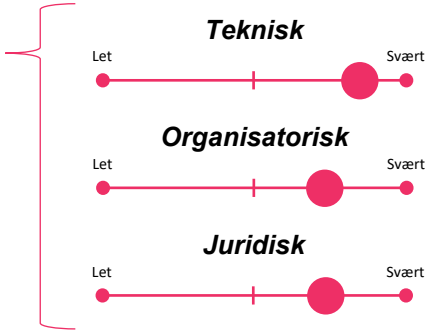
Vurdering

Kompleksitet

Niveau: Fællesoffentlig/national.

Tidshorisont: Kan gennemføres på <18 måneder.

Afhængigheder: Kan fungere som katalysator for flere indsatsforslag, herunder især indsatser om risikovurdering (1.1), kravstillelse (2.3 og 2.4) samt vidensgrundlag (3.1), alliancer (3.2) og incitamenter (3.3).



Udfordringer adresseret

- 01 | Høj afhængighed af større leverandører og manglende konkurrence
- 02 | Manglende kontrol og transparens over egne data
- 03 | Begrænset kontrol og styring af digitale løsninger
- 04 | Sårbarheder i den digitale forsyningssikkerhed

Gevinster

- Øget vidensniveau og opbygning af kapabiliteter på nationalt niveau.
- Mulig acceleration af konkrete initiativer hos myndighederne.
- Øget strategisk autonomi gennem nationale, transformative indsatser.

Forudsætninger for effektiv implementering

- Fællesoffentlig handleplan og principper for digital suverænitet, som kan rammesætte arbejdet.
- Afklaring af strategisk ambition, fokus, nødvendige kapabiliteter samt finansieringsniveau.
- Afklaring af organisationsform, mandat, kapabiliteter og governance.

PA anbefaler risikovurdering, krav til digital suverænitet, koordinerede cloud-indkøb og et nationalt udviklingscenter der kan sikre øget digital suverænitet og innovation (1/2)

PA anbefaler fire tiltag, hvor det vil være mest oplagt at starte og hvor der forventeligt kan skabes størst mulig effekt. Anbefalingerne retter sig direkte imod fire af de 12 foreslåede indsatser, men vil i praksis kunne absorbere øvrige indsatsforslag, for at skabe størst mulig værdi.

	Rationale	Effekter
A. Prioriter risikovurdering af digitale løsninger ***Skab overblik over kritiske afhængigheder og sårbarheder på tværs af den samlede teknologistak hos den enkelte myndighed, for at kunne prioritere indsatser.***	Risikovurdering er et effektivt første skridt mod øget digital suverænitet. Et fælles værktøj til risikovurdering på sektorniveau (stat, region, kommuner) eller fællesoffentligt vil sikre ensartethed og reducere kompleksitet. Indsatsen kan kobles til et fælles nationalt center for digital suverænitet, men vil i så fald skulle afvente etablering. På baggrund af risikovurderingen vil det være naturligt, at myndigherne som minumum overvejer exit-strategier og beredskabsplaner.	Øget transparens og robusthed, bedre prioritering af risikoreducerende tiltag og investeringer, samt styrket beredskab mod kritiske hændelser.
B. Stil krav om digital suverænitet ***Udarbejd en fælles "suverænitetspakke" med klare krav til offentlige it-udbud og SKI-aftaler for at indarbejde risikoreducerende tiltag i kontrakter og løsninger.***	Krav skal stilles fælles for at have effekt og sende et tydeligt signal til markedet. Det skaber incitament for leverandører til at udvikle løsninger, der understøtter suverænitet. Leverandører og indkøbsaktører kan med fordel involveres i en forudgående markedsafdækning og mobiliseringsproces for at sikre ejerskab og markedsparathed.	Ensartede krav på tværs af myndigheder, øget gennemsigtighed og forudsigelighed i udbud, styrket konkurrence og innovation.

PA anbefaler risikovurdering, krav til digital suverænitet, koordinerede cloud-indkøb og et nationalt udviklingscenter der kan sikre øget digital suverænitet og innovation (2/2)

PA anbefaler fire tiltag, hvor det vil være mest oplagt at starte og hvor der forventeligt kan skabes størst mulig effekt. Anbefalingerne retter sig direkte imod fire af de 12 foreslåede indsatser, men vil i praksis kunne absorbere øvrige indsatsforslag, for at skabe størst mulig værdi.

	Rationale	Effekter
C. Koordinerede "sektor-indkøb" af suveræne clouds ***Gennemfør koordinerede sektorudbud af suveræne cloud-løsninger for at opnå stordriftsfordele og sikre fuld kontrol med myndighedernes data.***	Adgang til og kontrol over data er kritisk – især med stigende AI-anvendelse. Koordinerede indkøb er realistiske, attraktive for markedet og skaber tillid til databrug og træning af AI-løsninger. Fælles indkøb og ensartede krav reducerer fragmentering og gør det muligt for leverandører at udvikle og skalere suveræne cloud-løsninger, som kan anvendes bredt. Endelig kan indsatsen fremme udvikling af AI og cloud-løsninger tilpasset offentlige behov.	Understøtter hybrid cloud og valgfrihed, sikker datalagring og robuste infrastrukturer til AI-udvikling. Stimulerer det europæiske og danske cloud-marked.
D. Etabler et nationalt center for digital suverænitet og innovation ***Skab en fælles og central drivkraft for accelereret udvikling og implementering af digitale alternativer.***	Et nationalt center kan sætte retning og skabe rammer for strategiske alliancer, indkøbspuljer og kravstillelse. Investeringspuljer kan have en virkning som isoleret forslag, men vil have større effekt i kombination med strategiske tiltag og fælles samarbejdsmodeller. Centret kan etableres som en taskforce drevet af offentlige aktører (fx som taskforcen for AI) med fokus på at understøtte udviklingen mod digital suverænitet – uden selv at bygge løsninger. Alternativt kan det oprettes som et offentlig-privat selskab eller partnerskab, der understøtter udviklingen af konkrete digitale alternativer.	Faciliterer samarbejde og (med)udvikling af sikre digitale teknologier, som styrker innovation og kompetenceopbygning, og accelererer implementering af suveræne løsninger i den offentlige sektor.

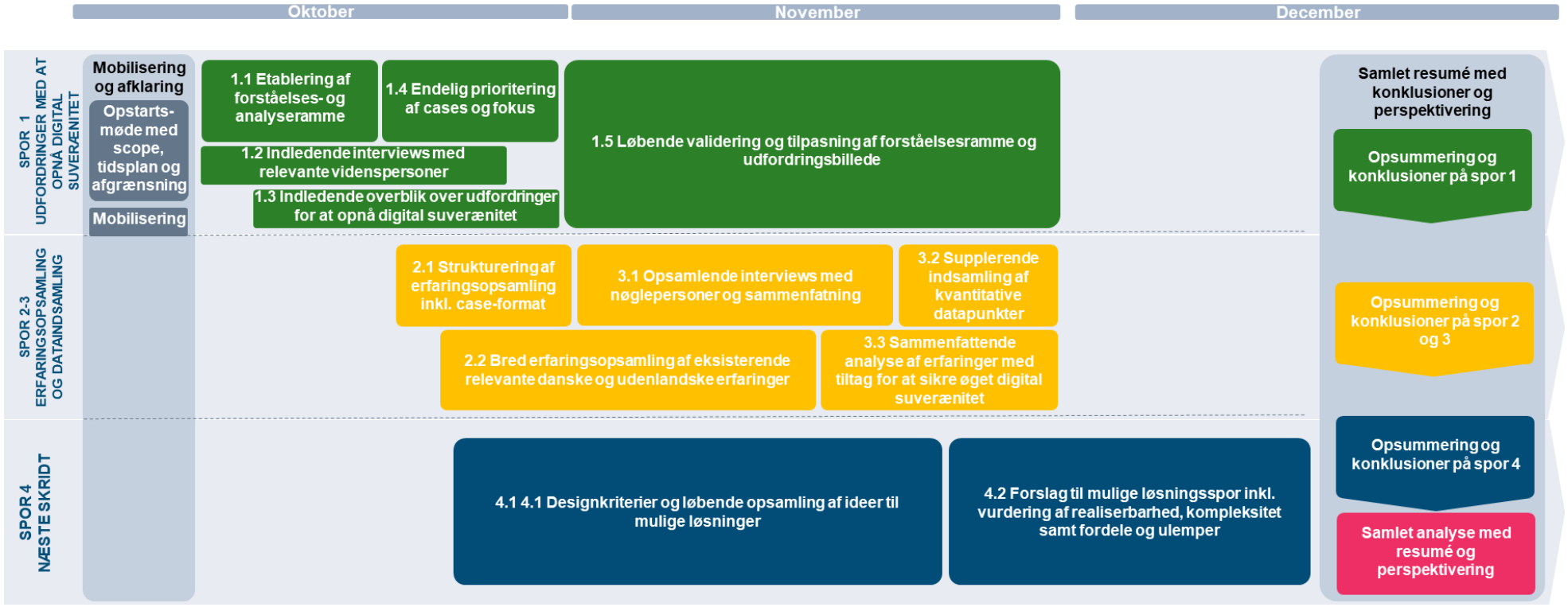
Bilag

Analysens metode og datagrundlag

PA's fremgangsmåde i analysen

Analyseprocessen har overordnet været tilrettelagt som et iterativt forløb, hvor der er arbejdet i parallel på analysens tre hovedleverancer og med løbende inddragelse af analysens styregruppe samt projektgruppe bestående af forskellige kompetencer fra parterne i FODS-samarbejdet.

Der er arbejdet iterativt med analysens leverancer inden for den overordnede projektplan



Datagrundlag og fremgangsmåde ift. udarbejdelse af cases

Der er ifm. analysearbejdet udvalgt og beskrevet i alt 15 cases mhp. at hente inspiration og erfaringer om digital suverænitet fra danske og udenlandske myndigheder. Der indgår seks cases fra danske myndigheder, herunder cases fra OS2 og KOMBIT, som medtages i denne kategori*. Der indgår seks cases fra udenlandske myndigheder – herunder to fælleseuropæiske. Der indgår to cases fra den finansielle sektor.

Fremgangsmåde og datagrundlag for udarbejdelse af cases

Udvælgelse af cases	• Det har været et krav, at der skulle vælges tre typer af cases – cases fra offentlige myndigheder i Danmark, cases fra offentlige myndigheder i udlandet og få cases fra det private erhvervsliv. Det har ikke på forhånd været fastlagt, hvor mange cases der i alt skulle indgå i arbejdet, ligesom der ikke på forhånd har været fastlagt en fordeling af cases mellem de tre typer. • Cases er identificeret gennem en proces, hvor PA har foretaget en indledende identifikation af mulige cases med afsæt i drøftelser med analysens styregruppe om, hvilke temaer og problemstillinger det har været mest relevant at få belyst. Denne indledende bruttoliste er suppleret gennem yderligere dialog med styregruppen samt med den etablerede projektgruppe. På den baggrund har PA udarbejdet et samlet motiveret oplæg, hvorefter cases er udvalgt.
Skriftligt materiale	• Der er i forbindelse med alle cases anvendt offentligt tilgængeligt, skriftligt kildemateriale. Det drejer sig typisk om strategier, analyser, evalueringer, forskningsartikler samt oplysninger vedr. formål, historik, opgaver og organisering på case-organisationernes hjemmesider. • Det skriftlige materiale er anvendt ifm. identifikation og udvælgelse af cases, forberedelse af de gennemførte interviews samt ifm. udarbejdelse af case-beskrivelser.
Kvalitative interviews	• Det gælder for alle cases, at der som supplement til det skriftlige materiale gennemført et kvalitativt interview med en centralt placeret ressourceperson. Der har været anvendt en semistruktureret tilgang, hvor der i interviewet er taget afsæt i motivationen for udvælgelsen af den pågældende case. På den baggrund er der spurgt aktivt ind til læringer og erfaringer, samt hvad der har været særligt i kontekst for den konkrete case. Endelig er der spurgt mere åbent til øvrige forhold med relevans for erfaringsindsamlingen. • For tre cases har det ikke været muligt at gennemføre interviews med den ansvarlige myndighed, hvorfor der i stedet er foretaget interview med en central vidensperson, som har været involveret i udviklingsarbejdet. Det drejer sig om Eurostack, Home Office og GPT-NL.
Opsamling af erfaringer og læring	• På baggrund af gennemgangen af det skriftlige materiale samt de gennemførte interviews er der foretaget en systematisk opsamling af centrale observationer og erfaringer. De centrale observationer er søgt detaljeret i de enkelte case-beskrivelser, hvor andre læringer og relevante erfaringer også er medtaget. Alle væsentlige pointer er på denne måde forsøgt sammenfattet og overbragt som led i analysearbejdet.

Overblik over anvendt kildemateriale (1/3)

[1] Den fællesoffentlige digitaliseringsstrategi 2026-2029

[2] Kommunernes digitaliseringsstrategi 2026-2030

[3] https://www.computerworld.dk/art/290654/fem-amerikanske-techgiganter-styrer-danmark-det-kan-faa-store-konsekvenser

[4] https://www.danskindustri.dk/vi-radgiver-dig/digital-suveranitet/forslag-til-digitaliseringsministeriets-handlingsplan/

[5] EuroStack – A European Alternative for Digital Sovereignty

[6] Future of Europe – EPRS Ideas Papers

[7] #EUROSTACK: EUROPEAN STRATEGIC SOVEREIGN DIGITAL INFRASTRUCTURES

[8] EuroStack: White-paper

[9] The Draghi report on EU competitiveness

[10] https://commission.europa.eu/news-and-media/news/commission-moves-forward-cloud-sovereignty-eur-180-million-tender-2025-10-10_en

[11] Cloud Sovereignty Framework | European Commission

[12] Commission launches a new procurement process for Cloud Services - European Commission

[13] Open Innovation and Open-Source Strategy of Land Schleswig-Holstein

[14] DIU Almdel Bilag 97 Slides DIU høring digital suverænitet

Overblik over anvendt kildemateriale (2/3)

[15] https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/news/centre-digital-sovereignty

[16] ZenDiS: Co-creating Digital Sovereignty - ZenDiS | Zentrum Digitale Souveränität

[17] https://www.zendis.de/en/what-we-offer

[18] Product | openDesk

[19] Netherlands AI Strategy Report - AI Watch - European Commission

[20] Presentation CLIN 2025 - GPT-NL

[21] https://www.publictechnology.net/2025/03/20/international-relations/home-office-signs-85m-digital-deal-to-support-consistent-repeatable-architecture-for-border-it-systems/

[22] https://github.com/orgs/UKHome

[23] https://www.kl.dk/oekonomi-og-administration/oekonomi-og-styring/omstilling-og-udvikling/nyhedsbrevet-raaderum/2018/nr-4/os2-samarbejdet-skaber-vaerdi-via-en-ny-model-for-udvikling-af-digitale-loesninger

[24] https://gaia-x.eu/wp-content/uploads/2025/01/Gaia-X-Brochure_Overview-2025.pdf

[25] https://www.kk.dk/dagsordener-og-referater/Borgerrepr%C3%A6sentationen/m%C3%B8de-27032025/referat/punkt-28

[26] https://pro.ing.dk/digitech/artikel/koebenhavns-kommune-vil-granske-sin-afhaengighed-af-tech-giganter-sparker-gang-i-stor-analyse

[27] https://digst.dk/media/2zlfki2v/open-source-i-den-offentlige-sektor.pdf

[28] Sammen griber vi de digitale muligheder

Overblik over anvendt kildemateriale (3/3)

[29] Digitaliseringsstrategi 2024-2027 – Et bedre københavnerliv

[30] ”Analyse af udfordringer og løsninger inden for samspillet mellem cloud og AI” – Digitaliseringsministeriet

[31] The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy

[32] “Software Reuse through Open Source Software in the Public Sector - A qualitative survey on Policy and Practice” - RISE

[33] Gateways Comparing Digital Communication Systems in Nordic Welfare States

[34] “Danmarks digitale afhængighed: En analyse af Danmarks afhængighed af amerikanske it-produkter og –løsninger samt EU’s muligheder for at opbygge en stærk position inden for centrale it-områder” – IDA

[35] “Friends with (digital) benefits: examining the EU’s strategic tech ties” - Politico

[36] Hovedtal fra Finanstilsynet | Finanstilsynet

[37] DORA Oversight Guide - European Insurance and Occupational Pensions Authority

[38] https://www.dst.dk/en/Statistik/temaer/digitalisering

[39] Bankdata - United in Code, Empowered by Talents

[40] 693abbcf1cf88573083d1e26_AIsovCAISA.pdf

[41] Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern

[42] https://www.kl.dk/oekonomi-og-administration/oekonomi-og-styring/omstilling-og-udvikling/nyhedsbrevet-raaderum/2018/nr-4/os2-samarbejdet-skaber-vaerdi-via-en-ny-model-for-udvikling-af-digitale-loesninger

PA har interviewet en række relevante videnspersoner fra både offentlige og private aktører, herunder internationale profiler

	Organisation	Rolle
Offentlig sektor i Danmark	**Københavns Kommune**	Afdelingschef for projekter og udvikling, Koncern IT
	Københavns Kommune	Sagsbehandler, ØKF
	Aarhus Kommune	Digitaliseringschef
	Aarhus Kommune	It Chef
	Region Syd	It Arkitekt
	Statens IT	Direktør
	Region Nord	Chef for IT-Drift, Support og Cyber og Informationssikkerhed
	STIL	Kontorchef i Kontor for Central Komponenter og Registre
	STIL	Kontorchef Center for Drift, Infrastruktur og Op. Sikkerhed
	STIL	Vicedirektør
	SKI	Markedsdirektør
	SKI	Chefrådgiver
	SKI	Kundechef

	Organisation	Rolle
Off. Sektor i DK	**Sundhedsdatastyrelsen**	Afdelingschef
	Sundhedsdatastyrelsen	Chefarkitekt
	Københavns Universitet	Professor
	OS2	Sekretariatschef
	KOMBIT	Chef for Design & Arkitektur
	DBC	Udviklingschef
Internationalt	**Schleswig-Holstein**	CIO
	EuroStack	Direktør for Digitalisering, Bertelsmann Stiftung
	TNO	Produkt Manager for GPT-NL
	GPT-NL	PA Partner
	GPT-NL	PA Ekspert
	RISE	Senior forsker
	EU Kommissionen	Afdelingschef, Cloud og Software Services

	Organisation	Rolle
Int.	**UK Kontrol og Migreringsmyndighed**	PA Partner
	ZenDiS	CEO
Privat sektor	**Bankdata**	Senior direktør
	Bankdata	Lead Arkitekt
	Magenta	CEO
	Finansiel Sektor	PA Partner
	Finansiel Sektor	PA Ekspert, DORA
	Finansiel Sektor	PA Ekspert, DORA
	Tænketanken for Digital Infrastruktur	Direktør
	Aeven	Vicedirektør
	OpenXchange / IDA	Arkitekt / Formand for IDA IT
	Dansk Industri	Branchedirektør, DI Digital
	Teleindustrien	Direktør

Bringing Ingenuity to Life.