Marts 2026

DIGITAL SUVERÆNITET – DIN GUIDE TIL AT KOMME RIGTIGT FRA START

DigitalLead.

TEKNOLOGISK INSTITUT

INDHOLDSFORTEGNELSE

DigitalLead.

TEKNOLOGISK INSTITUT

OM GUIDEN

Denne guide er udviklet gennem et Innovationsprojekt som er bevilget af DigitalLead og medudviklet af de tre deltagende virksomheder: Hugin Expert A/S, TypoConsult A/S og Co-Creators CO ApS.

VALG DER VAR FORNUFTIGE DENGANG, MEN HVAD MED NU?

Forestil dig, at jeres største kunde i morgen kræver dokumentation for, hvor deres data behandles, og hvad jeres beredskabsplan er ved et større nedbrud. De fleste virksomheder har truffet deres teknologivalg ud fra fornuftige kriterier: hvad der virker, er modent, sikkert og nemt at levere løsningen på. I dag er det ikke længere nok, at teknologien virker. Ændrede vilkår, skærpede kundekrav, ny regulering, prisstigninger og nedbrud, alt dette gør teknologiske afhængigheder til et strategisk udviklingspotentiale, og en måde at differentiere sig fra konkurrenterne. Denne guide giver jer sprog og værktøjer til at komme rigtigt fra start, så I kan tage kontrol og opnå konkurrencefordele gennem digital suverænitet.

SUVERÆNITET MED PLADS TIL FORBEDRINGER

Europa er strukturelt afhængig af ikke-EU-leverandører. Over 80% af de digitale produkter, services, infrastruktur eller IP, der anvendes i EU, kommer fra leverandører uden for EU (Europa-Kommissionen), og omkring 70% af de grundlæggende AI-modeller globalt kommer fra USA (Bertelsmann Stiftung). I Danmark viser en undersøgelse fra Dansk Erhverv, at 88% bruger mindst én ikke-EU-cloududbyder, 52% ønsker at reducere afhængigheden, 50% ved ikke, om europæiske alternativer er konkurrencedygtige, og 11% ser on-prem som en reel mulighed for dem. Det betyder, at mange organisationer bliver i status quo. Ikke fordi det er det bedste valg, men fordi alternativerne og konsekvenserne ikke er gjort konkrete.

SUVERÆN RÅDERET SOM PROAKTIV KAPABILITET

Denne guide introducerer begrebet **digital suveræn råderet**. Råderet er evnen til at gøre jeres afhængigheder bevidste og risikostyrede. Det handler om at have en beredskabsplan og kunne svare på: Hvad er vi reelt bundet til? Hvad betyder det for vores tempo, compliance og omkostninger? Og hvordan opretholder vi driften, hvis vilkår eller adgang pludselig ændrer sig?

Målet er at bevare jeres strategiske handlekraft, så I kan levere, sælge og drive forretningen på forudsigelige vilkår, også når verden forandrer sig, og transformere jeres stack i det tempo og omfang som passer jeres forretning. Denne guide handler om jeres råderet som virksomhed. De valg I tager for at øge jeres råderet, er ikke kun afgørende for jer selv, men også for suveræniteten for de mennesker, hvis data I behandler. På side 4 kommer vi ind på, hvordan jeres og individets interesser kan mødes eller være i konflikt.

HVOFOR LÆSE DENNE GUIDE?

Denne guide er bygget op, så den tager dig fra overblik til konkret handling. I vil:

- Få et sprog til at diskutere digital suverænitet og digital suveræn råderet, og hvad det betyder for jer, dem som bruger jeres løsning, og dem hvis data indsamles.
- Blive præsenteret for en proces, der tager jer fra analyse til handling.
- Læse cases fra andre danske IKT-virksomheder, og hvordan de arbejder med deres digitale suveræne råderet i praksis.
- Blive præsenteret for værktøjer, som I selv, eller sammen med en facilitator, kan bruge til at finde jeres fokus og prioritering indenfor digital suverænitet.

Hvis I støder på ord I ikke kender, kan I på side 22 og 23 finde en ordliste over anvendte domænebegreber.

Målet er at give jer og jeres virksomhed et konkret grundlag for at træffe bevidste valg om jeres teknologiske afhængigheder. Når du har læst guiden, står du med de argumenter og det sprog, der gør det muligt at forklare jeres prioriteringer, uanset om I taler med bestyrelsen eller ledelsen om risiko, med kunderne om sikkerhed og suverænitet eller med jeres eget udviklingsteam om tekniske løsninger.

DIGITAL SUVERÆNITET OG DIGITAL SUVERÆN RÅDERET

BEGREBET DIGITAL SUVERÆNITET

Digital suverænitet fylder i den offentlige debat, fordi Europas og danske virksomheders digitale afhængigheder ikke længere kun handler om pris og teknologi. Det er nu også et spørgsmål om geopolitiske interesser, jurisdiktion, robusthed, leverandørmagt og at sikre sig mod sikkerhedsbrud eller totale nedbrud. Digital suverænitet kan betyde flere ting. For nogen er det kontrol over egne data, frihed til at skifte leverandør, eller at have retten til selv at sætte vilkårene. Andre fokuserer på om data er beskyttet, og sikkert placeret. Dette på vegne af både dem selv, og for de mennesker, som afgiver data. Uanset betegnelsen er det ikke længere kun et spørgsmål om valg af leverandør, men også om hvor servere er placeret, og hvem der i teorien og i praksis kan få adgang til data. Først ser vi på, hvordan andre definerer digital suverænitet. Derefter præsenterer vi vores egen tilgang: digital suveræn råderet. Denne råderet hviler på fire grundprincipper, som vi gennemgår på næste side.

DIGITAL SUVERÆNITET

I EU betegnes digital suverænitet som at gøre sig mindre afhængige af ikke-EU-leverandører, ved at opbygge egen kapacitet inden for cloud-løsninger og de fysiske komponenter som chips, for at sikre at kritisk infrastruktur er under EU-jurisdiktion, samt at lock-in skal begrænses ved at bruge åbne standarder.

KL og Den Fællesoffentlige Digitaliseringsstrategi 2026-2029 slår fast, at kommunerne er blevet for afhængige af store udenlandske leverandører, særligt dem, der ikke opererer på kommunernes præmisser eller lever op til deres værdigrundlag. Fokus er på fuld kontrol over data og på at synliggøre alternativer til tech-giganterne.

På lex.dk defineres digital suverænitet som egenkontrol over data, digitale tjenester og IT-infrastruktur som kontrast til digital afhængighed af eksterne teknologileverandører som tech-giganterne. Fokus er her på magtforholdet mellem stater/samfund og globale platforme, og på at kritisk digital infrastruktur ikke må ligge udenfor demokratisk kontrol.

Dansk Industri lægger vægt på, at Danmark og EU skal investere strategisk i kritisk teknologi, så der reelt er noget at vælge imellem. Der skal være kontrol over kritiske data og infrastruktur, og fleksibilitet til at skifte til bedre alternativer, når de findes. Pointen er ikke, at vi skal kunne klare alt selv, men at vi skal kunne handle på egne præmisser.

Slutteligt fokuserer IT-Branchen på, at vi skal gøre os mindre afhængige af ikke-EU-teknologi, at Danmark og Europa i højere grad skal have digital autonomi og at vi skal styrke forsyningssikkerheden omkring vores digitale infrastruktur.

VORES TILGANG: DIGITAL SUVERÆN RÅDERET

For IKT-virksomheder, der skal kunne tage beslutninger her og nu, er det afgørende at kunne omsætte ambitionerne omkring digital suverænitet til noget, der kan handles på i jeres konkrete stack.

Derfor definerer vi begrebet ***Digital Suveræn Råderet***, som et forretningsnært supplement, der handler om at gøre afhængigheder bevidste og risikobaserede, og omsætte dem til muligheder. Som bl.a. Dansk Industri og KL er inde på, er målet ikke nødvendigvis digital isolation eller at skifte væk fra tech-giganterne, men at man har bevidstheden om, hvilke leverandører man reelt er bundet til, i hvilken grad man er bundet, og:

1. Hvad det betyder for jeres strategiske handlekraft og prioritering, f.eks. at kunne levere løsninger hurtigt fra idé til implementering, at overholde compliance og/eller beskyttelse af data, omkostningsreduktion mm.
2. At der er en klar beredskabsplan og alternativ stack, hvis f.eks. vilkår ændrer sig eller kunderne efterspørger EU-first, hvad man skifter til, kører parallelt eller anden implementeringsform (se side 19)

Digital suveræn råderet bygges ikke gennem ét enkelt teknologisk valg, men gennem løbende prioritering og re-design af jeres stack, baseret på dataværdi, suverænitet, sårbarhed, kritikalitet og kontraktuelle forhold.

Målet er ikke nul risiko, men kendt, styret og dokumentérbar risiko, hvor I har valgfrihed og kender alternativerne så I kan skifte, helt eller delvist, hurtigt eller gradvist, når det giver mening for jeres forretning.

DigitalLead.

TEKNOLOGISK INSTITUT

DE FIRE GRUNDPRINCIPPER SOM DIGITAL SUVERÆN RÅDERET BYGGER PÅ

Strategisk handlekraft er evnen til at træffe bevidste teknologivalg, som understøtter forretningens langsigtede mål og jeres konkurrencedygtighed. Det vigtige er, at kunne handle på egne præmisser, når markedet, kundekrav eller regulering ændrer sig, uanset om det gælder tempo, compliance, databeskyttelse eller andre faktorer.

Bevidst arkitektur og placering handler om at designe arkitektur, vælge komponenter og beslutte placering (f.eks. EU-hosting, open source-komponenter, hybrid-cloud) på en måde, der aktivt understøtter jeres ønskede niveau af kontrol, flytbarhed, sikkerhed og transparens, og som kan forklares til f.eks. udviklere, kunder, slutbrugere og borgere. Det handler også om, at have en beredskabsplan, der er testet, og som kan sættes i drift eller flyttes til efter behov.

Kontrolleret afhængighed er at anerkende, at fuldstændig uafhængighed er urealistisk. Selv valg af EU-first-hosting binder jer blot til en anden leverandør end ikke-EU, men gør jer ikke uafhængige. Det kræver, at I forstår hvilke fordele I får ud af afhængigheden, at I ved, hvor I er mest sårbare, og at I kender både eksplicitte og implicitte exit-omkostninger.

Valg, I kan stå på mål for, handler om at der er konsistens mellem det, I siger, og det, I gør. Hvis I taler om tillid eller sikkerhed, bør jeres teknologi- og leverandørvalg, have dette som en del af kernen. Generelt betyder det, at hvert valg, afspejler de værdier, I står for, og at I kan forklare jeres bestyrelse, jeres kunder og slutbrugerne, hvorfor I har taget de valg I har. Ikke fordi nogen tvinger jer, men fordi I mener det.

Disse fire principper er fundamentet. På næste side, ser vi på hvordan jeres råderet og interesser kan understøtte individets suverænitet og nogle gange vil være i konflikt med den.

DigitalLead.

TEKNOLOGISK INSTITUT

SUVERÆNITET FOR JER, OG FOR DEM SOM BRUGER, ELLER LEVERER DATA TIL JERES LØSNING

Denne guide handler om jeres digitale råderet. Men overfor jer står kunder, brugere og borgere, hvis data I indsamler og behandler. De har deres egne forventninger til suverænitet f.eks. retten til at vide hvor deres data er placeret, hvad der sker med dem, og muligheden for at sige fra og trække data tilbage. Nogle gange trækker de to perspektiver i samme retning, andre gange er de i konflikt. Det er ikke guidens kernefokus, men I bør have med i jeres perspektiv, om I opnår jeres råderet på bekostning af deres suverænitet? Nedenfor er eksempler på områder, hvor interesserne styrker hinanden eller kan være i konflikt.

OMRÅDE	NÅR INTERESSER MØDES	NÅR INTERESSER KONFLIKTER
Hosting og cloudvalg	I vælger EU-kontrolleret-hosting med klare juridiske rammer. Det beskytter jer mod uventet myndighedsadgang, og giver jeres kunder vished om, at deres data ikke kan kræves udleveret til fremmede jurisdiktioner.	I vælger den cloud, der giver jer størst fleksibilitet og laveste pris. Det styrker jeres handlekraft, men jeres kunders data kan nu potentielt tilgås af myndigheder, de aldrig har accepteret.
Dataindsamling	I indsamler kun de data, I faktisk har brug for. Det reducerer jeres sikkerhedsrisiko og compliance-byrde – og begrænser hvor meget af brugernes liv, der ligger i jeres systemer.	I indsamler bredt, fordi data er værdifulde, og I måske får brug for dem senere. Det øger jeres forretningsmuligheder, men brugerne har afgivet data til formål, de ikke kender, og som I måske ikke har defineret endnu.
Teknologisk afhængighed	I bygger på åbne standarder og portable formater. Det giver jer frihed til at skifte leverandør, og giver jeres kunder mulighed for at tage deres data med, hvis de vil væk.	I bygger på proprietære platforme, fordi det er hurtigere og lettere. Det låser jer til leverandøren, men det låser også jeres kunders data. Hvis I ikke kan flytte, kan de heller ikke. Jeres lock-in bliver deres lock-in.
Leverandører og datavilkår	I vælger leverandører med gennemsigtige datavilkår, som I selv kan stå inde for. Det giver jer kontrol over jeres forpligtelser, og jeres kunder kan stole på, at I ved, hvad der sker med deres data.	I accepterer vilkår, der kan ændres ensidigt med 30 dages varsel. Det giver jer hurtig adgang til løsningen, men den beskyttelse, jeres kunder troede, de havde i dag, kan være væk i næste måned.
Tredjeparts-integrationer	I integrerer strategisk og med klare grænser for, hvilke data der deles med hvem. Det giver jer funktionalitet uden at sprede data, og jeres kunder kan få svar, hvis de spørger, hvem der har set hvad.	I integrerer bredt for at accelerere innovation. Data flyder til analytics-tjenester, marketing-platforme, AI-værktøjer. Jeres hastighed købes med deres uigennemsigtighed.
Sikkerhed og kryptering	I krypterer data hele vejen, både i hvile, under transport og under behandling, og det er jer der styrer nøglerne. Det beskytter jer mod læk, manipulation og myndighedsadgang, og det beskytter jeres kunders data mod alle, der ikke skal se dem.	I vælger et sikkerhedsniveau, der er "godt nok" til at overholde loven, men ikke mere. Det holder jeres omkostninger nede, men jeres kunder bærer risikoen, hvis jeres "godt nok" viser sig ikke at være det.

OVERVEJ FØR NÆSTE TEKNOLOGIVALG

Teknologivalg har konsekvenser for de mennesker, hvis data I behandler. Brug følgende spørgsmål til at vurdere, om jeres valg også holder, når I ser det fra deres side:

- Hvis en kunde spurgte "hvem får mest ud af det her valg, er det jer, mig eller os begge?", hvad ville svaret være?
- Hvis vi forklarede vores databehandling på et salgsmøde, ville kunden nikke eller rynke bryn?
- Hvad gør vi, når det, der er godt for forretningen, ikke er lige så godt for kundernes data?
- Hvis en kunde spørger "hvem besluttede det her?, og hvorfor valgte I dette?", har vi så et klart svar?
- Hvilke værdier ønsker I, at jeres teknologivalg afspejler? Er jeres nuværende leverandører i overensstemmelse med de værdier, I kommunikerer udadtil?

DENNE GUIDE FOKUSERER PÅ JERES RÅDERET

OG HANDLEKRAFT SOM VIRKSOMHED

Den dækker ikke:

- Individets digitale rettigheder som selvstændigt emne
- Dataetik som fagdisciplin
- Borgerrettigheder og demokratisk kontrol over teknologi
- Forretningsmodellers etiske implikationer

Vi anbefaler ressourcer som f.eks. DataEthics.eu, noyb.eu og Dataetisk Råd, som behandler det mere indgående, og komplementerer denne guide indenfor disse områder.

UDVALGTE AFGØRENDE FAKTORER

BEGREBET DIGITAL SUVERÆNITET

Digital suveræntet fylder i den offentlige debat, fordi Europas og danske virksomheders digitale afhængigheder ikke længere kun handler om pris og teknologi. Det er nu også et spørgsmål om geopolitiske interesser, jurisdiktion, robusthed, leverandørmagt og at sikre sig mod sikkerhedsbrud eller totale nedbrud. Digital suveræntet kan betyde flere ting. For nogen er det kontrol over egne data, frihed til at skifte leverandør, eller at have retten til selv at sætte vilkårene. Andre fokuserer på om data er beskyttet, og sikkert placeret. Dette på vegne af både dem selv, og for de mennesker, som afgiver data. Uanset betegnelsen er det ikke længere kun et spørgsmål om valg af leverandør, men også om hvor servere er placeret, og hvem der i teorien og i praksis kan få adgang til data. Først ser vi på, hvordan andre definerer digital suveræntet. Derefter præsenterer vi vores egen tilgang: digital suveræn råderet. Denne råderet hviler på tre grundprincipper, som vi gennemgår på næste side.

EKSEMPLER PÅ AFGØRENDE FAKTORER

REGULATORISK PRES SOM FORRETNINGSVILKÅR

Lovgivning som GDPR, NIS2 og den amerikanske CLOUD Act er ikke længere kun jura, men et vilkår for at drive forretning, og kravene forventes at vokse de kommende år. I kan være fuld compliant, men stadig miste kunder. Når f.eks. CLOUD Act gør det muligt for amerikanske myndigheder at tilgå data, selv hvis det er EU-hosted, er det ikke nok at sige "vi overholder reglerne". For kunden er det vigtige, om de kan være trygge ved, at I er ansvarlige for indsamling, opbevaring og behandling af deres, slutbrugerens eller borgerens data.

NÅR KUNDEN KRÆVER SUVERÆNE LØSNINGER

Hvis en kunde efterspørger en suveræn løsning, skal EU-first eller open source være reelle alternativer. Afhængig af kundens behov og ønsker, kan alternativet handle om enkeltdele (f.eks. hosting) til hele jeres stack.
Det kræver en forberedt og alternativ stack, som er testet og klar, så I kan levere uden at gå på kompromis med kvalitet, tempo eller hvad der er vigtigt for jeres strategiske handlekraft.

LEVERANDØREN HÆVER PRISEN ELLER ÆNDRER VILKÅR

Jeres leverandører ændrer løbende priser, funktioner og vilkår. Små ændringer kan over tid akkumulere til en betydelig omkostning, der påvirker jeres omsætning og handlekraft. At vide hvornår I skal reagere, og have et alternativ klar, er nødvendigt for både at have forhandlingskraft og til at kunne drive jeres løsninger på egne præmisser.

NEDBRUDDET AFSLØRER JERES KRITISKE AFHÆNGIGHEDSPUNKT

Når én central it-leverandør rammes af nedbrud eller sikkerhedsbrud, hvad enten det er den platform, hvor systemer og data er placeret, løsningen der håndterer login og adgang eller andet, kan det skade både stabiliteten af løsningen og påvirke kundens tillid til jer. Ved at arbejde med både beredskabsplaner og alternative stacks er det muligt at reducere afhængigheden af en enkelt platform og skabe en infrastruktur, der kan ændres eller flyttes til, uden at driften går i stå.

SUITE-FORDELE MED SKJULTE OMKOSTNINGER

Suites kan reducere udviklingstid og friktion i hverdagen, men de kan også skabe en dyb forretningsmæssig og teknisk afhængighed, hvor sammenhængen mellem alt fra identitet og mail til dokumenter og sikkerhed er tæt forbundet. Et leverandørskifte bliver dermed ikke kun et teknisk projekt, men en gennemgribende og risikabel forandring for jeres virksomhed, som både positivt og negativt kan være afgørende for jeres handleevne.

DATASIKKERHED OG ANSVARLIG DATAANVENDELSE

Uanset hvad I laver, håndterer I data, der er kritiske for nogen. Det kan være jeres kunder, jeres egen forretning, de personer data handler om, eller samfundet som helhed. Der er i dag skærpet fokus på, hvor data er placeret, og hvem der reelt har adgang, både praktisk og teoretisk. Det handler også om, hvad data bruges til, om det behandles på en forventet og accepteret måde som kan accepteres, og dermed at autoriseret adgang anvendes ansvarligt.

STRATEGISK HANDLEKRAFT

Digital suveræn råderet handler i sidste ende om at sikre jeres strategiske handlekraft. Det er en ledelsesdisciplin, der sikrer, at I driver virksomheden på bevidste valg og ikke på ubevidste afhængigheder. I kan godt være afhængige af en leverandør, men afhængigheden skal være kendt, accepteret og styret. Brug følgende spørgsmål til at tage temperaturen på jeres nuværende handlekraft:

1. Hvilke 3 forretningsmål er vigtigst for os de næste 12-18 måneder (f.eks. vinde kunder i den offentlige sektor, reducere Total Cost of Ownership (TCO), øge udviklingshastigheden, være proaktive på compliance m.fl.)? Og hvordan understøtter, eller modarbejder, vores nuværende stack disse mål?
2. Hvilke principper eller løfter til kunderne må vi aldrig gå på kompromis med (f.eks. driftsstabilitet, beskyttelse af kundedata, brug af open source)?
3. Hvilke krav til sikkerhed, dokumentation eller jura stiller vores vigtigste kunder i dag? Og hvilke krav forventer vi, de vil stille om 12-18 måneder, som vi skal være klar til at imødekomme?
4. Hvilke af de seks afgørende faktorer udgør den største risiko for os? Kan kortlægges ud fra konsekvensmatrix på side 18.

HVAD ER EN STACK?

STRATEGISK PROCES FRA USIKKERHED TIL IMPLEMENTERING
De afgørende faktorer på forrige side, rammer ikke jeres virksomhed ens. De rammer forskellige dele af jeres teknologi på forskellige måder. En mindre prisstigning på jeres CRM-system kan være irriterende, men håndterbart. Et nedbrud på jeres cloud-platform kan lukke for jeres service i flere timer og være et tillidsbrud for jeres kunder. For at kunne handle på de forskellige faktorer, skal I først forstå, hvor I er sårbare.

HVORDAN KAN I ARBEJDE MED JERES STACK?
Tænk på jeres stack som et hus bygget af tre lag. Bunden er fundamentet. Det er sjældent synligt i hverdagen, men hvis det svigter, falder alt sammen. Midten er husets indre installationer, el, vand og varme, og det som får huset til at fungere. Toppen er det, I og jeres kunder ser og bruger dagligt.

Når I ændrer jeres stack, kan det sammenlignes med at renovere et hus. Lagene hænger sammen, og ændringer ét sted påvirker resten. At skifte vinduer (toppen) kan være relativt nemt. At omlægge kloakken (midten) kræver mere planlægning. At skulle understøbe fundamentet (bunden) er dyrt og risikabelt, men nogle gange nødvendigt. I modsætning til et hus kan nogle ændringer, selv i bunden af stacken, foretages uden de store omkostninger.
De fleste virksomheder starter enten dér, hvor risikoen er størst, eller der hvor der er mest rum til at eksperimentere.

Toppen: Det brugerne møder
Toppen af stacken er de applikationer og værktøjer, som jeres medarbejdere og kunder bruger dagligt. Virksomheder med kontrol over dette lag vil typisk:
- Kende de vigtigste SaaS-afhængigheder, og ved, eller har, en klar formodning om hvad det vil koste at skifte
- Undgå at bygge forretningskritiske workflows i systemer med risiko for lock-in
- Have evalueret alternativer før de står i en situation, hvor de er tvunget til at skifte.

Toppen er ofte det letteste lag at ændre. Det gør at mange IKT-virksomheder starter i dette lag.

TOPPEN
Applikationer og brugerflade, bl.a.
- Kundevendte applikationer
- Interne medarbejderværktøjer
- Forretningssystemer
- Samarbejdsværktøjer

Midten: Konstruktionen
Midten af stacken er de systemer, der forbinder jeres kode med produktion, og jeres applikationer med underliggende systemer og Bunden. Det er bl.a. databaser, API'er, identitetsstyring og generelt den koordinering, som får det hele til at hænge sammen. Virksomheder med kontrol over dette lag vil ofte:
- Kunne dokumentere hvor data ligger og hvem der har adgang
- Sikre at centrale data kan anvendes på tværs af systemer
- Have standardiserede integrationer, som flere end én person forstår og kan vedligeholde

Kontrol over midten er det der gør jer i stand til at skifte applikationer i toppen uden at miste data, og skifte infrastruktur i bunden uden at ødelægge integrationer.

MIDTEN
Tjenester og data, bl.a.
- Systemarkitektur
- Central datastyring
- Udviklerplatforme
- Databaser
- Systemintegrationer

Bunden: Fundamentet
Bunden af stacken er det tekniske fundament, som jeres kunder aldrig ser, men som kan påvirke dem i sidste ende. Det dækker bl.a. cloud-platforme, netværk og de sikkerhedsløsninger, der krypterer og beskytter data, potentielt hele vejen ned til hardware-niveau. Virksomheder med kontrol over dette lag vil f.eks.:
- Sømløst kunne genskabe løsningen på en anden platform
- Have overvågning, der opdager problemer, før kunderne gør det
- Have designet infrastrukturen med exit som et princip og ikke et tilvalg

Risikoen i bunden er omfattende, men typisk sjælden, selvom vi har set et stigende antal nedbrud over de sidste år. Men når denne del af stacken rammes, så rammer det ofte også en stor del af midten og toppen. Bunden er ofte der hvor ændringer har størst strategisk og teknisk effekt.

BUNDEN
Infrastruktur
- Driftsmiljø
- Netværks- og sikkerheds-services
- Overvågning
- Back-up
- Driftansvar og beredskab

VI BRUGER MANGE SERVICES, HVORAF IKKE ALLE ER OPEN SOURCE – OG DET ER OKAY.

FOR OS HANDLER DET IKKE OM AT UNDGÅ ALLE AFHÆNGIGHEDER, MEN OM AT KENDE DEM OG VURDERE DEM BEVIDST. HVILKE KAN VI LEVE MED? HVILKE VIL VI GERNE HAVE ALTERNATIVER TIL?

NÅR VI HAR DET OVERBLIK, KAN VI TAGE DIALOGEN MED VORES KUNDER – OG LEVERE MED DEN SIKKERHED OG STABILITET, DE FORVENTER.

KRISTIAN STORM JØRGENSEN, TypoConsult A/S

SEKS STYRINGSGREB TIL AT ØGE JERES DIGITALE SUVERÆNE RÅDERET

At identificere de faktorer, der truer jeres strategiske handlekraft, er det første skridt til at øge jeres digitale suveræne råderet, men hvis I ikke handler på disse faktorer, står I stadig i en sårbar situation. Her præsenterer vi seks konkrete styringsgreb, som I kan anvende til at håndtere udfordringerne. Betragt dem som strategiske valg, der hver er designet til at styrke jeres råderet på forskellige områder.

EU-first

Applikationer

Infrastruktur

Open source

Datakontrol

BYG EN STACK, DER ÅBNER NYE MARKEDER

Hvis I vil sælge til kunder med suverænitetskrav, skal det være en del af jeres strategi og infrastruktur og ikke et engangsprojekt. Byg f.eks. et EU-first alternativ til minimum de dele af løsningen, der skal kunne flyttes, eller som er mest sårbare. Det kan i nogle tilfælde kræve en helt alternativ stack. Gevinsten kan være adgang til nye markeder, færre dyre tilpasninger og mindre risiko for at ét kundekrav bliver en stor teknisk omvej. Et skifte til EU-first kræver nye kompetencer, så det er vigtigt at investere i at opbygge denne ekspertise.

(Fokus på bl.a.: Jurisdiktionskontrol via EU-hosting og arkitektur designet for udskiftelighed.)

BLIV DEM, DER ALTID LEVERER

Hvis en central service eller cloud-region går ned, må jeres leverance ikke gå helt i sort. Byg failover ind, hvor det er mest sårbart at fejle, test at I kan skifte spor med mindst mulig friktion og test beredskabsplanen regelmæssigt. Gevinsten er ro i driften, øget oppetid og/eller reduceret time-to-recovery og derigennem færre frustrerede kunder.

(Fokus på bl.a.: Redundans via multi-region eller alternativ hosting, hurtig genetablering med Infrastructure as Code og proaktivitet via overvågning)

FRA SUITE TIL SAMMENSAT STACK SOM PASSER TIL JER

Suites føles smarte, indtil I opdager, at I betaler for funktioner, I ikke bruger.
Opdel jeres stack i udskiftelige dele, som i højere grad er tilpasset de funktioner, I har behov for, og som skaber værdi for jer eller jeres kunder.Det giver en mere forudsigelig økonomi og større konkurrencefordel, fordi I i mindre grad risikerer at stå overfor et alt-eller-intet skifte. Husk dog, at dette påvirker medarbejderne, så involver dem tidligt.

(Fokus på bl.a.: Byg med udskiftelige komponenter via åbne API'er og at vælge supporteret open source)

NÅR DOKUMENTATION ER EN KONKURRENCEFORDEL

Når en kunde spørger "hvor er data, og hvem har adgang?" skal svaret kunne leveres hurtigt. Skab en simpel dokumentations-pakke, som kan anvendes til audits, certificeringer og til at bevise, at I overholder branchekrav. Gevinsten er ikke kun at bestå audit, men også en mere robust intern praksis, fordi I tvinger jer selv til at vide, hvad der foregår i jeres egen stack. Samtidig bliver det et salgsargument, da I ikke bare sælger software, men også sporbarhed, sikkerhed og transparens.

(Fokus på bl.a.: Sporbarhed via automatiserede logs, overblik med dataflow-diagrammer og sikkerhed via restore-tests..)

REDUCÉR LOCK-IN UDEN AT BREMSE UDVIKLINGEN

I har valgt leverandører ud fra praktiske fordele og behov, men lock-in vokser ofte over tid. Start en gradvis afkobling ved at gøre de mest kritiske komponenter udskiftelige. Det giver lavere exit-omkostninger, og mindre risiko for at et ændret kundekrav udløser en akut og dyr omskrivning.

(Fokus på bl.a.: Portabilitet via containere, integration via åbne API'er.)

STRATEGISK KONTROL OVER JERES STACK-ØKONOMI

Hvis I betaler for platformsfunktioner eller tryghed, I ikke bruger, betaler I for bekvemmelighed, som I ikke får værdi af. Vurdér derfor forholdet mellem pris og værdi, og beslut hvor I vil købe de praktiske fordele henne, og hvor I selv vil tage kontrol. Det kan for eksempel være ved at flytte driften til egen hardware, hvor gevinsten dels er lavere omkostninger, og at få en arkitektur, der er lettere at styre.

(Fokus på bl.a.: Skab overblik med cost tagging og hav en billigere driftsplan klar, som er testet)

SUVERÆNITETSSPILLEPLADEN

HVORFOR EN SUVERÆNITETSSPILLEPLADE?

Alle beslutninger har konsekvenser. Når I vælger at fokusere på ét område i jeres stack, skaber det afhængigheder, som ved ændringer kan påvirke andre dele af stacken. Ændringer i bunden af stacken kan få vidtrækkende konsekvenser på tværs af hele arkitekturen, mens ændringer i toppen ofte har færre afhængigheder. Derfor er det vigtigt at forstå jeres behov, kortlægge afhængighederne og vurdere, om fordelene ved en ændring opvejer de konsekvenser, den medfører.

HVAD ER SUVERÆNITETSSPILLEPLADEN?

Suverænitetsspilleplade er en radar med ni centrale parametre. Den fungerer som et konsekvenskort: Når I vælger et styringsgreb, f.eks. EU-first, open source eller øget datasikkerhed, vil det typisk styrke 2-3 parametre, men samtidig svække 1-2 andre. Hvis I f.eks. prioriterer tempo, går det ofte ud over kontrol. Prioriterer I datasikkerhed, følger der ofte øgede omkostninger og højere kompleksitet med. For at gøre disse afvejninger tydelige og mulige at diskutere introducerer vi Suverænitetsspilleplade. Værktøjets formål er at tvinge jer til at tage stilling til, hvad I reelt prioriterer, og hvad I bevidst nedprioriterer. Afsættet skal ikke være ud fra jeres mavefornemmelser, men ud fra et strategisk perspektiv.

HVORDAN BRUGER MAN SUVERÆNITETSSPILLEPLADEN?

Anvend værktøjet i tre trin: 1. Start med nuværende situation, 2. Ønskede scenarie og 3. Vurdér afvejninger.

Start med nuværende situation

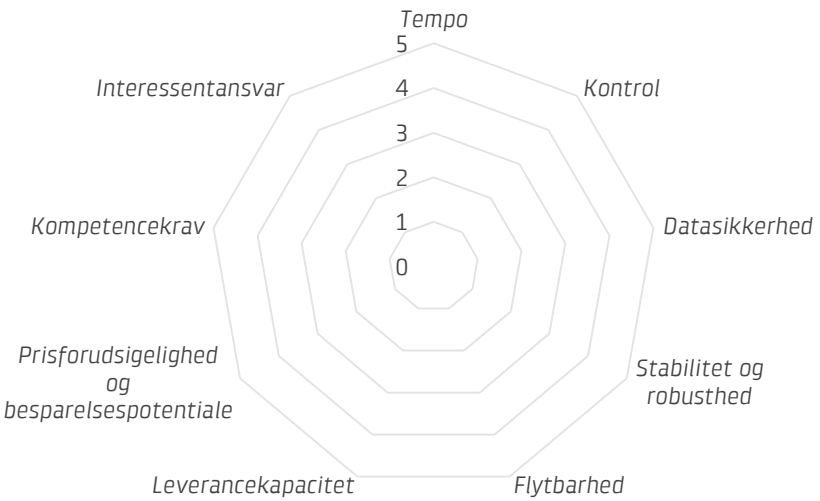
Begynd med at vurdere jeres nuværende situation og eksisterende stack. Saml relevante tekniske kompetencer og ledelsen, gennemgå de ni parametre, og giv jeres nuværende setup en score fra 0 til 5.

Beskriv ønsket scenarie

Visualisér, hvordan et mere suverænt alternativ kan se ud, f.eks. ved at skifte til EU-first-hosting eller ved at implementere open source i stacken. Vær så ærlige som muligt i kortlægningen af alternativet, og notér eventuelle usikkerheder.

Vurdér afvejninger

Sammenlign de to profiler ved at lægge dem oven på hinanden. Forskellen mellem dem viser både gevinsterne og konsekvenserne ved at tilbyde løsningen som et alternativ eller ved at gennemføre et egentligt skifte. Sammenhold herefter resultatet med jeres svar under Strategisk handlekraft på side 4, og vurder om I fortsat opretholder jeres digitale suveræne råderet.



PARAMETRENE:

Tempo = Hvor hurtigt kan I levere, ændre og skalere uden unødig friktion?

Kontrol = Kan I styre adgange, krypteringsnøgler, API'er efter behov, og så det er dokumenterbart?

Datasikkerhed = Hvor robust er data beskyttet mod datalæk, misbrug, manipulering og uautoriseret adgang?

Stabilitet og robusthed = Hvor modstandsdygtig er driften over for nedbrud og forstyrrelser?

Flytbarhed = Hvor realistisk og hurtigt kan I flytte eller genetablere drift ved leverandørskifte eller længerevarende udfald?

Leverancekapacitet = Kan I levere og drifte løsningen med egen nuværende organisation og kompetencer?

Prisforudsigelighed og besparelsespotentiale = Hvor stabile er totalomkostningerne, og hvad er besparelsespotentialet ved et alternativ?

Kompetencekrav = Hvor meget specialviden eller kompetenceudvikling kræver jeres alternative stack?

Interessentansvar = I hvor høj grad I kan forsvare jeres valg af teknologi eller leverandører over for kritiske kunder, medarbejdere og bestyrelsen?

TRE BASISEKSEMPLER PÅ SUVERÆNITETSSPILLEPLADEN

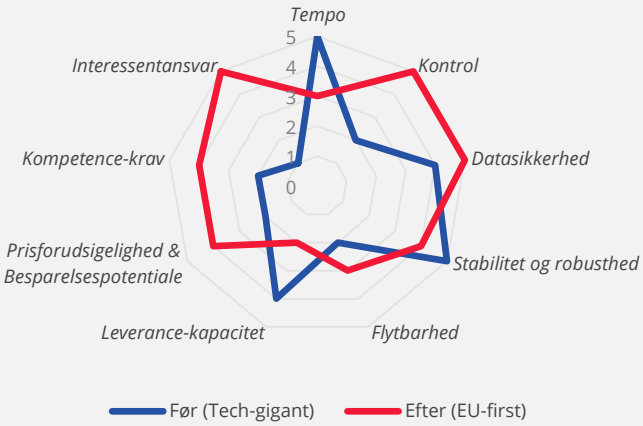
BASISEKSEMPLER

Her er tre profiler der illustrerer typiske afvejninger, som IKT-virksomheder vil stå overfor i skiftet mod digital suverænitet.

Fra tech-gigant (Blå) til EU-first (Rød)

Når en IKT-virksomhed flytter fra en amerikansk tech-gigant til en EU-leverandør, er målet typisk at øge den juridiske og datamæssige kontrol.

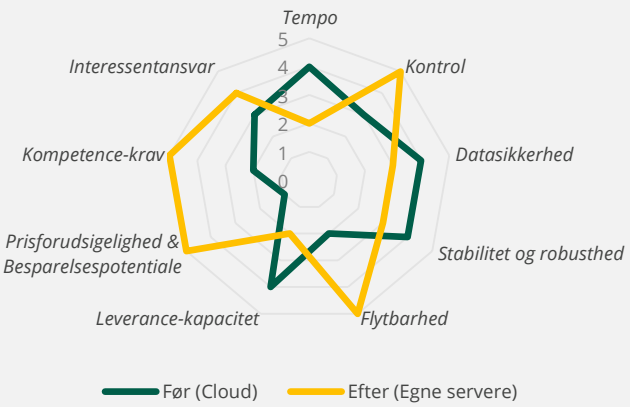
Det, man forventer at opnå, er markant forbedret *Kontrol* og *Datasikkerhed*, samt bedre *Prisforudsigelighed*, da man undgår pludselige, globale prisstigninger. Dog forventes det at medføre et reduceret *Tempo* og en reduceret *Leverancekapacitet*, da man ofte mister et bredt udvalg af avancerede managed services. *Kompetencekrav* øges ofte i en læringsperiode, da ens eget team skal håndtere opgaver, som platformen før løste.



Fra Cloud (Mørkegrøn) til Egne servere (Orange)

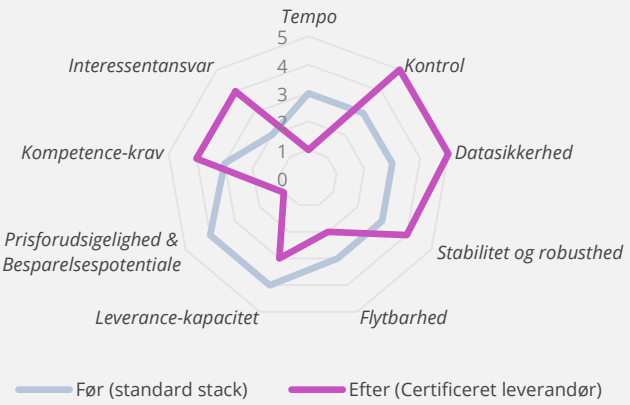
En af de primære grunde til at skifte til egne servere, er forventningen om et stort *Besparelsespotentiale* og fremtidig *Prisforudsigelighed*

Det man forventer at opnå, er *Kontrol* over infrastruktur og performance, samt øget *Flytbarhed*, så I kan placere løsningen, hvor I ønsker. Da virksomheden selv er ansvarlig for alt fra hardware til redundans, øger det *Kompetencekrav*, og ansvaret for *Stabilitet* ligger på virksomhedens egne skuldre. Danske grit42 har opnået store besparelser med en blanding af EU-first og open source.



Fra standard stack (Lyseblå) til Certificeret leverandør (Pink)

Når kundekrav om compliance (f.eks. NIS2, ISO 27001 osv.) bliver en kommerciel nødvendighed, vælger man en leverandør eller stack, der kan levere de nødvendige certifikater og dokumentation. Det styrker *Interessentansvar*, når man finder en leverandør der kan levere dette. De forventede gevinster tæller derudover, en markant styrkelse af *Kontrol* og *Datasikkerhed*, som kan bruges direkte som salgsargument. Den forventede konsekvens er en reduktion i *Tempo*, fordi ændringer skal igennem compliance-processer og dokumentationskrav. Samtidig vil det veje negativt på *Prisforudsigelighed* og *Besparelsespotentialet*, da certificeret infrastruktur ofte er dyrere.



TEKNOLOGISK INSTITUT

VI VALGTE GITLAB FOR AT KUNNE HOSTE LØSNINGEN LOKALT (AF HENSYN TIL BL.A. DATASIKKERHED) OG FOR AT HAVE DEVOPS MED PROJEKTSTYRING SOM EN DEL AF LØSNINGEN. I FORHOLD TIL SKIFTET VÆK FRA JIRA KAN DET MÅSKE BLIVE NØDVENDIGT AT GÅ PÅ KOMPROMIS MED NOGLE MULIGHEDER OMKRING TEKNISK SUPPORT. DET ER ET NO-GO AT HOSTE VERSIONSSTYRING AF VORES SOFTWARE I EN CLOUD LØSNING.

ANDERS L MADSEN, HUGIN EXPERT A/S

LEVERANDØRER OG ANVENDERVIRKSOMHEDER

LEVERANDØRER

Suverænitet kan understøttes på flere måder internt, f.eks. i ens stack, eller mod kunderne, til at øge strategisk handlekraft bl.a. gennem compliance. Her er nogle leverandører, som er med til at understøtte digital suverænitet hos virksomheder.

Man kan gøre sin mail mere suveræn ved at bruge **Proton Mail** (en del af deres suite), som tilbyder zero-access kryptering, så kun brugeren og modtageren kan se indholdet, som sendes. Med deres løsning er Proton selv teknisk udelukket fra adgang til data.

Tyske **Hetzner** tilbyder et alternativ til tech-giganternes cloud-løsninger og beskyttelse mod den amerikanske CLOUD Act ved at være under EU-jurisdiktion. De arbejder mod at tilbyde lignende services som tech-giganterne tilbyder. Hvis man ønsker at holde fast i Azure og deres funktioner, kan man anvende **Bleu**. Bleu er et partnerskab mellem Capgemini og Orange, og så er Azure inden for EU-jurisdiktion.

grit42 har skiftet tech-giganter og US-cloud ud med EU-first og open source, og har udover suverænitetsfordele også betydet konkrete besparelser på licenser både ift. det administrative og deres løsninger mod kunderne.

Partisia tilbyder en dataplatform, hvor flere parter kan analysere og beregne på den kombinerede data, men at hver partner, kun kan se den del af datasættet, som er blevet aftalt. Her beskyttes data selv under behandling, hvilket kan være relevant ift. NIS2 og GDPR-lovgivning.

GitLab er et suverænt alternativ til GitHub. Det er en open core DevOps-platform, som kan hostes selv, eller hos en valgfri cloud-udbyder. Det giver bl.a. fuld kontrol over egen kildekode og CI/CD-pipelines.

ANVENDERVIRKSOMHEDER

For ICRC og Schwarz Group er det at øge deres digitale suverænitet blevet et strategisk og forretningskritisk anliggende, både for at passe på egne data, og for at mindske risikoen ud mod konkurrenterne. ICRC, som er den internationale Røde Kors komité, ser ikke databeskyttelse som et compliance-spørgsmål, men både som en forudsætning for at operere og for at beskytte oplysninger, som ikke må komme i hænderne på andre. Schwarz Group repræsenterer en anden indfaldsvinkel. Europas største detailkoncern ønskede ikke at have deres forretningskritiske data på AWS, da de er en markedskonkurrent og ønskede samtidig ikke at være afhængige af andre tech-giganter. Schwarz Group byggede sin egen cloud-platform, med en ny ambition om at sælge hosting eller cloud-tjenester ligesom AWS og Azure.

CASES FRA 3 DANSKE IKT-VIRKSOMHEDER

CASES FRA 3 DANSKE IKT-VIRKSOMHEDER

Hvor globale aktører som ICRC og Schwarz Group kan investere massivt i egen infrastruktur, må danske teknologivirksomheder ofte finde mere pragmatiske veje til digital suverænitet. For at gøre principperne i denne guide konkrete, zoomer vi ind på tre virksomheder, der aktivt arbejder med digital suveræn råderet: Hugin Expert A/S, TypoConsult A/S og Co-Creators ApS.

De er alle dybt specialiserede, agile og i varierende grad afhængige af globale værktøjer for at levere effektivt til deres kunder. Gennem et forløb om digital suverænitet har de kortlagt deres vigtigste afhængigheder, og de har udarbejdet planer, der kan håndtere alt fra kundekrav til nedbrud. Deres erfaringer viser, at det er muligt at arbejde pragmatisk og forretningsdrevet med øget kontrol og suverænitet – dér, hvor det gør mest forskel.

HUGINEXPERT

UDGANGSPUNKT

HUGIN EXPERT leverer software til modelbaseret beslutningsstøtte under usikkerhed. Softwaren benyttes blandt andet til prædiktiv analyse, forudseende vedligeholdelse og fejlfinding. Modellerne tilpasses den enkelte kundes data og forretningsbehov. Med kunder inden for sektorer som finans, forsyning, produktion og den offentlige sektor imødekommer HUGIN compliance-krav som GDPR og NIS2. Løsningen er platformsuafhængig og implementeres typisk på kundens egen infrastruktur eller en cloud-platform som f.eks. Azure. Som et nyt initiativ udvikler HUGIN en standardløsning til forudseende vedligeholdelse, der i første omgang er planlagt til drift på Azure. Internt anvendes Jira til projekt- og udviklingsstyring, hvor data er placeret på servere inden for EU.

RATIONALET FOR DIGITAL SUVERÆN RÅDERET OG DIGITALE SUVERÆNE LØSNINGER

HUGIN EXPERTs rationale for at investere både tid og ressourcer i digital suveræn råderet og mere digitale løsninger gælder bl.a.:

- *Kunde- og compliancepres*
  HUGIN arbejder med kunder, der håndterer følsomme og forretningskritiske data, og ofte er underlagt skærpede krav. Det er essentielt at kunne give kunderne et alternativ, som ikke er bundet op på tech-giganterne.
- *Beskyttelse af kerne-IP og udviklingsmiljø*
  Deres værdi ligger i modeller, algoritmer og domæneviden. Ved at bruge digitalt suveræne værktøjer opnås kontrol med både kode, pipelines og data, så de ikke bliver et sårbart afhængighedspunkt.
- *Kontrolleret afhængighed af tech-giganterne*
  HUGIN bruger i dag tech-giganterne til at levere skalerbare løsninger, men vil undgå at det bliver "single point of failure", både juridisk, teknisk og økonomisk. For dem handler det om at kende exit-veje og have realistiske alternativer klar.

FOKUS

For at styrke virksomhedens strategiske råderet har fokus været todelt:

1. At kunne tilbyde et EU-baseret alternativ til Azure. Dette skal både fungere som en beredskabsplan for at sikre forretningskontinuitet ved nedbrud, og som et proaktivt tilbud til kunder med strenge krav til data-compliance (NIS2/GDPR) og EU-jurisdiktion.
2. At opnå fuldt ejerskab over hele udviklingsprocessen – fra versionsstyring af kildekode og CI/CD-pipelines til håndtering af sager og opgaver – ved at konsolidere på en self-hosted platform.

ARBEJDET DER ER I GANG

For den nye standardløsning undersøger HUGIN aktivt et EU-first setup. Dette inkluderer en analyse af, hvordan teknologier som EU-Cloud, nye krypteringsmetoder og confidential computing kan anvendes. Målet er at udvikle et unikt tilbud til de compliance-tunge sektorer, hvor HUGIN kan træne modeller på kundedata uden at få direkte adgang til de underliggende data.

Internt har HUGIN taget de første skridt mod at hjemtage deres udviklingsværktøjer. De har igangsat et pilotprojekt, hvor de på udvalgte projekter tester en egen-hostet GitLab-installation. Formålet er at validere platformens potentiale som en samlet, suveræn DevOps-løsning og opnå:

1. Fuld kontrol over versionsstyring
2. Sikker og auditerbar CI/CD-pipeline
3. En afklaring af, i hvor høj grad GitLab kan være et integreret alternativ til Jira til håndtering af tickets og agil software udvikling.

.

CASES FRA 3 DANSKE IKT-VIRKSOMHEDER

TYPOCONSULT

UDGANGSPUNKT
TypoConsult er specialister i open source-baserede web- og CMS-løsninger (især TYPO3) og har et fundament i suveræne principper. Som reaktion på øget geopolitisk usikkerhed og nedbrud hos store cloud-leverandører, har TypoConsult proaktivt udviklet en EU-baseret beredskabsløsning, der sikrer kunders forretningskritiske kommunikation (f.eks. via SMS til slutbrugere) i tilfælde af nedbrud hos deres primære leverandør.

RATIONALET FOR DIGITAL SUVERÆN RÅDERET OG DIGITALE SUVERÆNE LØSNINGER
TypoConsults rationale for at investere både tid og ressourcer i digital suveræn råderet og mere digitale løsninger gælder bl.a.:

- *Driftssikkerhed*
  Deres løsninger skal fungere, når det gælder. Et nedbrud hos en central cloud-leverandør eller anden platform, må ikke skabe frustration hos kunderne. Det vigtige er at kunne sikre driften, også når den primære leverandør fejler.
- *Beredskabsplan*
  Panikbeslutninger opstår, når planen mangler. TypoConsult har fokus på at have klare planer, for hvornår de reagerer, og hvordan, så de har overskud til at handle på både problemer og muligheder.
- *Afhængighed og økonomi som risikofaktor*
  De arbejder på at reducere lock-in, og at kende alternativer, så man ikke pludselig er bundet til en leverandør, men kan finde løsninger, der er bedre for bundlinjen, uden at gå på kompromis overfor for kunderne.

FOKUS
De to vigtigste fokusområder for TypoConsult har været:

1) At formalisere og udbygge deres beredskabsløsning til en egentlig beredskabsplan, der kan garantere kunders forretningskontinuitet, selv under uforudsete driftsmæssige udfordringer.
2) Systematisk at vurdere og vælge suveræne alternativer til både kunde- og interne systemer, hvor det giver den bedste balance mellem fleksibilitet, sikkerhed og omkostningseffektivitet.

ARBEJDET DER ER I GANG
Beredskabsløsningen er blevet succesfuldt testet på EU-infrastruktur og har bevist sin stabilitet, performance og funktionalitet. TypoConsult arbejder nu på at tilbyde dette som en suveræn kommunikationsløsning, der kan tilbydes som en selvstændig service til både eksisterende og nye kunder.

Internt har TypoConsult evalueret europæiske alternativer til understøttelse af webløsninger, som f.eks. CDN (Content Delivery Network). Her er der truffet strategiske valg baseret på en afvejning af strategisk handlekraft og datasårbarhed.

Virksomheden anerkender sin afhængighed af Google-suiten til administrative opgaver. Selvom en fuld migrering er nedprioriteret grundet kompleksiteten, er der taget aktive skridt for at afsøge alternativer. Gennem forløbet er LibreOffice blevet testet for at vurdere dets potentiale som en fremtidig erstatning for dele af suiten.

CASES FRA 3 DANSKE IKT-VIRKSOMHEDER

CO-CREATORS

UDGANGSPUNKT
Co-Creators CO ApS arbejder med innovations- og forskningssektoren, omkring udvikling af digitale platforme med fokus på fleksibilitet og modulær arkitektur, som understøtter samarbejde hos kunderne. Co-Creators bygger løsninger på en moderne stack, med Lovable til at kode frontend og backend, Supabase til database samt GitHub og Netlify til at levere løsningerne både til produktion og til drift.

RATIONALET FOR DIGITAL SUVERÆN RÅDERET OG DIGITALE SUVERÆNE LØSNINGER
Co-Creators CO's rationale for at investere både tid og ressourcer i digital suveræn råderet og mere suveærne løsninger gælder bl.a.:

- *Kundekrav om EU-first eller suveræne løsninger*
  Det er vigtigt at kunne tilbyde en mere suveræn stack til de kunder, som kommer og efterspørger EU-first eller suverænitet. Det ses også som at være på forkant med kundernes kommende compliance-krav.
- *Kontrol over eget værktøjssystem*
  For Co-Creators er deres metode og deres værktøjer deres produkter. De ønsker ikke at være låst til tech-giganterne i forbindelse med deres kerneydelser.
- *Strategisk signal til markedet*
  Ved aktivt at arbejde med digital suveræn råderet kan Co-Creators positionere sig som en partner, der både forstår moderne cloud-udvikling og de nye krav om suverænitet. De har også en ambition om, at vi som samfund søger mod mere suveræne løsninger.

FOKUS
Deres kernefilosofi er altid at kunne tilbyde et dokumenteret EU-first alternativ til deres foretrukne stack. Udfordringen er at sikre, at dette alternativ ikke markant forringer den bekvemmelighed og hastighed i deployment, som er afgørende for deres forretning. Målet er ikke at skifte alt, men at have et reelt, testet alternativ klar, samt at kende de positive og negative effekter, både internt og for kunderne, når der leveres gennem denne alternative stack.

ARBEJDET DER ER I GANG
Co-Creators prioriterer at finde EU-alternativer til de mest kritiske dele af deres deployment-pipeline. De har sikret, at deres generelle stack og Supabase-database kører på EU-servere og undersøger nu Hostinger, som er EU-baseret, både til databaser, men også til hosting af GitLab, som et alternativ til GitHub. Målet er at skabe en parallel EU-first stack, der i så høj grad som muligt, matcher den oprindelige fleksibilitet og bekvemmelighed så kundekrav om suverænitet kan imødekommes uden at gå på kompromis med tempoet.
Co-Creators anvender Google-suiten til en del af deres administrative processer. Her undersøges alternativer til Google Meet, som kan føles kompromitterende. Det gælder bl.a. WIRE Conference (WIRE allerede bruges til intern kommunikation), Proton Meet, Whereby eller Jitsi. Det er dog vigtigt, at der ikke introduceres for meget friktion internt ved mødeoprettelsen.

VI HAR ALTID PRIORITERET SIKKERHED OG KONTROL, MEN DEN STØRSTE FORSKEL ER, AT VI NU ARBEJDER ENDNU MERE METODISK MED EN PLAN B. FORLØBET HAR GIVET OS VÆRKTØJERNE TIL AT OPERATIONALISERE ET SUVERÆNT ALTERNATIV, SÅ VI STÅR SOM EN FORBEREDT PARTNER, DER PROAKTIVT KAN TILBYDE KUNDER MED SÆRLIGE KRAV PRÆCIS DEN TECH STACK, DE HAR BEHOV FOR. VI HAR OMSAT VISIONEN OM SUVERÆNITET TIL PRAKTISK OG MÅLBAR RÅDERET.

TOBIAS SAMI AUGUSTENBORG, CO-CREATORS CO APS

HVOR STARTER MAN?
FØRSTE TRIN: AFKLARING

STRATEGISK PROCES FRA USIKKERHED TIL IMPLEMENTERING

Digital suveræn råderet opbygges ikke gennem tilfældige suveræne teknologivalg, men via følgende strukturerede proces:

1. Afklaring, som kortlægger de ydre faktorer, teknologiske afhængigheder og strategiske handlekraft.
2. Planlægning af hvad I reagerer på, hvornår og i hvilken grad, uanset om det er ydre faktorer eller for at øge jeres strategiske handlekraft. Her designer og undersøger I også, hvordan jeres alternative stack ser ud.
3. Implementering, hvor I udskifter enkelte komponenter, skifter til alternativ stack, tilbyder det som mulighed eller kører det parallelt med den primære stack. Det er ikke nødvendigvis en alt-på-én-gang proces, men kan også tages fra komponent til komponent.

Første skridt:

Afklaring

Forstå den nuværende situation og hvad der er vigtigst for jer. Uden et ærligt og detaljeret billede af jeres nuværende situation og jeres prioriteter inden for strategisk handlekraft, bliver planlægning og skitsering af alternativer mere på mavefornemmelse end strategisk forankret. Det kan være fristende at springe afklaringsfasen over, og vælge nogle suveræne løsninger som alternativ. Gør I det, er der risiko for at suverænitet ender som et politisk, ideologisk eller juridisk projekt som ikke understøtter jer forretningsmæssigt, i samme grad, som der er potentiale for.

Tag udgangspunkt i jeres eksisterende stack og kortlæg jeres mest kritiske systemer og leverandørafhængigheder. Dette giver et første billede af jeres sårbarheder og risiko for lock-in. Brug suverænitets- og kritikalitetsmatrix på side 18 til at kortlægge dette.
Et kernespørgsmål kunne være: *Hvor er vi teknisk sårbare?*

Definér jeres vigtigste forretningsmål, strategiske principper og hvor I ikke må fejle, som jeres teknologi skal understøtte. Dette sikrer at jeres suverænitetsplaner ikke bliver ren ideologi eller teknik, men skaber forretningsmæssig værdi og handlekraft.
Et kernespørgsmål kunne være: *Hvad er vigtigst for os at opnå?*

Analysér og vurdér ydre faktorer som potentielt eller reelt kan påvirke jer, jeres løsning og jeres kunder. Dette er alt fra bl.a. markedet, kundekrav, lovgivning, nedbrud, vilkår og kontrakter. Her kan I finde nogle eksempler på side 5. Kan kortlægges med en konsekvensvurdering.
Et kernespørgsmål kunne være: *Hvad kan ramme os udefra?*

HVOR STARTER MAN?
FØRSTE TRIN: AFKLARING

Første skridt:

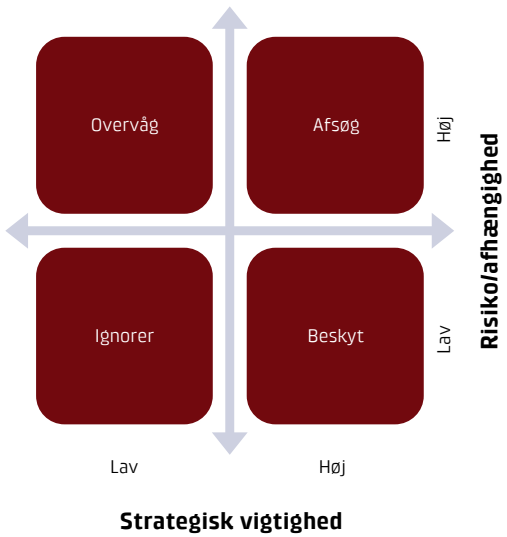
Afklaring

Som et led i at besvare de tre kernespørgsmål på forrige side, kan man bruge følgende to metoder til at evaluere hhv. Teknologi, med suverænitets- og kritikalitetsmatrix og Eksterne faktorer med Konsekvensvurdering.

SUVERÆNITETS- OG KRITIKALITETSMATRIX

Kritikalitetsmatrixen er en måde at få overblik over komponenterne i jeres løsning, og afdække hvilke I skal finde alternativer til, hvilke I skal beskytte, og hvilke afhængigheder I accepterer.

Kortlæg hver komponent ift. hvor strategisk vigtige de er for jer, både teknisk og forretningsmæssigt, og hvor stor risiko eller afhængighed I har til leverandøren af komponenten eller systemet i sig selv.
Det giver bl.a. et overblik over, hvilke komponenter I skal for at finde alternativer til, hvilke I skal hjemtage eller sikre og dermed beskytte, hvilke der vil være en fordel at undersøge alternativer til og hvilke I kan ignorere.

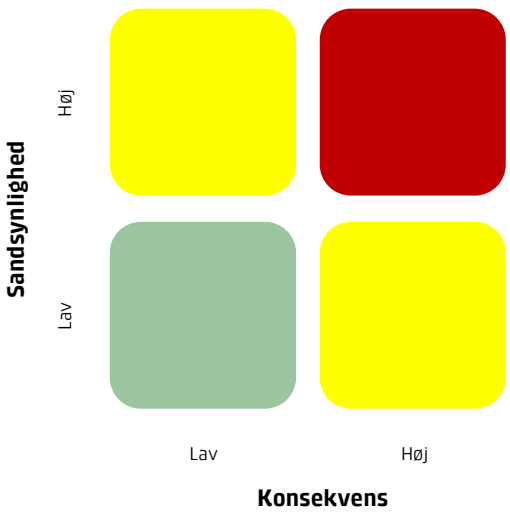


KONSEKVENSVURDERING

Brug konsekvensvurderingen til at prioritere eksterne faktorer efter sandsynlighed og forretningsmæssig effekt.

Kortlæg hvert eksempel på side 5 og andre faktorer, som kan påvirke jer, jeres løsning eller jeres kunder. Vurder først hvor sandsynligt det er, at det rammer jer inden for de næste 18 måneder, og derefter hvor alvorlig den forretningsmæssige konsekvens er hvis det sker.
De der lander i den røde firkant er aktuelle farer, som skal håndteres med det samme gennem både beredskabsplan og handleplan. De der lander i de gule firkanter er faktorer som skal overvåges aktivt, og hvor der er en klar plan for hvornår og hvordan I vil reagere. De der ender i den grønne firkant er accepterede risici for nu.

Et eksempel kunne være: En stor prisstigning fra jeres cloud-leverandør. Det har høj sandsynlighed og konsekvensen er høj. Dette placerer den i den røde firkant øverst til højre, og kræver øjeblikkelig afdækning af alternativer.



TEKNOLOGISK INSTITUT

HVOR STARTER MAN?
ANDET TRIN: LÆG PLANER

Andet skridt:

Læg planer

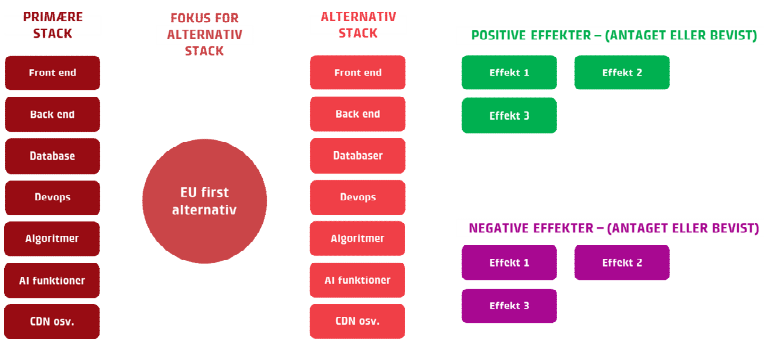
Planlægningsfasen handler om at omsætte jeres Afklaring til konkrete testbare planer. Det handler om at vide: hvilke faktorer vi reagerer på, hvad skal der ske, for at vi reagerer på dem, hvilken påvirkning har det på os når faktoren rammer os på denne måde, hvordan reagerer vi og i hvilken grad. Det handler også om at kende alternativerne, og hvordan det påvirker både jer og kunderne at have som alternativ.

Definér på forhånd, hvordan I reagerer, når bestemte faktorer rammer bestemte systemer. Det kan være at man de første to timer efter et nedbrud på et understøttende system ønsker at afvente opdateringer, men efter seks timer skifter I til et beredskabssystem. Dette sikrer, at I handler baseret på en foruddefineret plan, og ikke i panik, når situationen opstår. Beredskabsplanen skal både gøre jer i stand til at være reaktive, men også være proaktive mod nye segmenter eller øgede dokumentations- og auditkrav.
Et kernespørgsmål kunne være: *Hvornår reagerer vi, hvordan reagerer vi og i hvilken grad?*

Design og afdæk et alternativ til hele jeres stack eller udvalgte kritiske komponenter, som gør jer i stand til at handle på beredskabsplanen. Det kan f.eks. være failover-alternativ, så I undgår nedetid, eller det kan være et EU-first eller open source alternativ, som er klar til, når kunderne efterspørger det. Analysér og test effekterne, både positive og negative, for at skabe et solidt beslutningsgrundlag, og så I kender de afvejninger, I accepterer i suverænitetsspillepladen.
Et kernespørgsmål kunne være: *Hvad betyder en alternativ stack både positivt og negativt for os?*

DESIGN AF ALTERNATIV STACK

Til højre ses en metode til systematisk vurdering af de tekniske-, kompetencemæssige, forretningsmæssige og etiske konsekvenser ved at skifte til en alternativ stack.
Brainstorm derefter alle forventede positive og negative tekniske, kompetencemæssige, forretningsmæssige og etiske effekter ved anvendelse af den alternative stack. Overvej bl.a., hvordan påvirker denne ændring de mennesker, hvis data I behandler? Giver den dem mere eller mindre kontrol, mere eller mindre gennemsigtighed? Det er vigtigt at skelne mellem, hvad der er antagelser, og hvad I har bevist gennem en test eller et proof of concept.



Metoden skaber et balanceret beslutningsgrundlag, bl.a. ved at se om de positive effekter vejer tungere end de negative, eller om de negative effekter er en acceptabel pris at betale for at opnå det strategiske mål.

Et eksempel kunne være at skifte Office-pakken ud med en selv-hostet løsning som NextCloud eller LibreOffice. De positive effekter man kunne forvente er fuld kontrol over dataplacering (bevist) og styrket position ift. GDPR-compliance (antaget). De forventede negative effekter er markant øgede drifts- og vedligeholdelsesbyrder for IT-afdelingen (bevist), at man skal lære at bruge en ny brugerflade, som kræver tilvænning (bevist), samt risiko for kompatibilitetsproblemer med eksterne partnere (antaget).

HVOR STARTER MAN?
TREDJE TRIN: IMPLEMENTERING

Tredje skridt:

Implementering

Med visionen på plads og planen klar handler det nu om at føre den ud i livet, i det tempo og omfang, der passer jeres forretning. Nogle virksomheder skifter ét system ad gangen over flere år. Andre tager hele stacken på seks måneder. Begge tilgange er rigtige, hvis de fører jer tættere på det, I vil opnå. Her er seks måder at gribe det an på.

Det vigtigste er at komme i gang. Mange virksomheder bruger måneder på at planlægge det perfekte skifte, uden at komme i gang. I behøver ikke alle svar, før I tager det første skridt. Start med noget overskueligt. Det kunne være et enkelt system, en afgrænset del af stacken eller et pilotprojekt med et motiveret team. Lær af det og byg videre på det. Implementeringen er ikke én stor beslutning, men en serie af valg: Hvilket system skifter I først? Hvilken leverandør vælger I? Hvilke processer ændrer I? Efter hvert skridt skal I stoppe op og spørge "Virker det? og "Hvad kan vi gøre bedre for f.eks. at øge vores strategiske handlekraft, møde kundekrav i højere grad eller reducere vores afhængigheder?"

LØBENDE FORBEDRING UDEN AT FORSTYRRE DRIFTEN

I udskifter løbende enkelte komponenter i jeres stack med mere suveræne alternativer, når det giver teknisk eller forretningsmæssigt mening. Det er en tilgang med lav risiko, der minimerer forstyrrelserne af den daglige drift og fordeler investeringen over tid. Den trækker dog også skiftet ud over en lang periode.

DEN PARALLELLE OPTION SOM TILBUD

I bygger og vedligeholder aktivt en alternativ stack, og giver det som en mulighed til kunderne i salgsprocessen. Denne model giver fuld fleksibilitet, da det er muligt at imødekomme kundernes individuelle krav. Dette kræver dog vedligehold og opdatering af flere komponenter parallelt.

EN DOKUMENTERET BEREDSKABSPLAN TIL NÅR KATASTROFEN RAMMER

I har en fuld dokumenteret og testet plan, men I bygger først den alternative løsning, når krisen faktisk indtræffer. Dette er den billigste forsikring med minimal forstyrrelse af den daglige drift. Dog vil kunden opleve en længere etableringstid, end hvis alternativet er idriftsat.

NÅR KUNDEN FINANSIERER JERES SKIFTE

I lader den første store implementering af jeres alternative stack blive finansieret af en ny strategisk kunde, som stiller specifikke suverænitets-, compliancekrav eller andre typer krav.
Dette kan ske gennem et projekt eller et længerevarende strategisk samarbejde. Ulempen er, at det kræver en kunde, der har tid, vil finansiere udviklingen og er villige til at påtage sig risikoen ved at være først.

UDSKIFTNING AF MOTOREN, MENS FLYET ER I LUFTEN

I bygger det nye suveræne alternativ ved siden af den gamle stack, og omdirigerer gradvist trafikken til den nye løsning, indtil det gamle system kan slukkes, uden at det rammer nogen. Dette gøres for at opgradere kritiske kernesystemer med så lidt risiko som muligt.

NYE LØSNINGER BYGGES PÅ EN ALTERNATIV STACK

I lader jeres eksisterende løsninger køre videre på den eksisterende stack, men beslutter at alle nye løsninger skal bygges på den alternative stack. Dette fokuserer investeringen på fremtidens stack, og gør at I ikke skal betale for at omskrive teknisk gæld. Dog vil det betyde, at nuværende succesfulde løsninger ikke nødvendigvis kommer over på den alternative stack.

TEKNOLOGISK INSTITUT

REFERENCER, VÆRKTØJER OG ANDEN INSPIRATION

OPSUMMERING

At opnå digital suveræn råderet er ikke et mål, men en kapabilitet I opbygger og vedligeholder. Ved at gennemgå afklaring, planlægning og implementering cyklisk, sikrer I, at jeres teknologi understøtter jeres strategi og imødekommer kundekrav, og ikke er styret af jeres leverandører eller afhængigheder som I ikke er bevidste om.

REFERENCER:

Bertelmann Stiftung
- EuroStack – A European Alternative for Digital Sovereignty

Dansk Industri
- VEJEN TIL STYRKET DIGITAL SUVERÆNITET

Dansk Erhverv
- Vil virksomheder skifte væk fra ikke-europæiske cloudleverandører?

Europa-kommissionen:
- The future of European competitiveness
- How the DIGITAL Building Blocks can help bring EuroStacks vision of European digital sovereignty to life

Fællesoffentlige digitaliseringsstrategi 2026-2029
- Sammen griber vi de digitale muligheder

IT-Branchen
- Sådan skal Danmark sikre digital suverænitet – IT-Branchens anbefalinger

grit42' case
- grit42 skiftede fra big tech til open source og sparede penge

Dataetik og digitale rettigheder
- Dataethics.eu
- Dataetisk Råd
- Noyb.eu

ANDEN INSPIRATION:

Find suveræne alternativer til bl.a. browsing, videoplatforme, Generativ AI mm.
- dataethics.eu/tools

Find danske alternativer til jeres stack
- Dansktechstack.dk

Find europæiske alternativer til jeres stack
- European alternatives

EuroStack
- EuroStack

DI Digitals guide til digital suverænitet
- Guide til digital suverænitet

Lex' beskrivelse af digital suverænitet
- Digital suverænitet opslag

PA Consulting
- Digital suverænitet i den offentlige sektor

Find Open stack komponenter
- Openstack.org

Europæisk data space til deling af data på tværs af værdikæder
- GAIA-X

Sikring af data under brug og behandling
- IBM's definition

Liste over selv-hostede alternativer
- GitHubs "Awesome Selfhosted" liste

VÆRKTØJER:
- **Spørgsmål til strategisk handlekraft – side 5**
- **Suverænitetsspillepladen – side 9**
- **Suverænitets- og kritikalitetsmatrix – side 18**
- **Konsekvensvurdering af eksterne faktorer – side 18**
- **Design af alternativ stack – side 19**

MED DENNE GUIDE HAR I SPROGET OG VÆRKTØJERNE

Når bestyrelsen spørger om risiko, når kunden kræver dokumentation, når teamet skal vælge mellem tempo og sikkerhed, så har I nu et fælles sprog for at tage diskussionen. I har også en række værktøjer, som både kan hjælpe jer med at overveje strategisk, hvad jeres prioritet er, hvilke udløsende faktorer I ser som den største risiko, til hvilke afvejninger I står overfor.

KLAR TIL AT TAGE NÆSTE SKRIDT?

For nogle er guiden nok. I tager værktøjerne, samler teamet og går i gang. Men for de fleste hjælper det at have en facilitator, der har gjort det før. En, der stiller de rigtige spørgsmål, udfordrer antagelserne og holder jer på sporet. Digital Lead og Teknologisk Institut hjælper virksomheder med at omsætte guiden til handling.

Kontakt os for en uforpligtende samtale, I finder kontaktoplysninger på bagsiden.

ORDLISTE

ORD I GUIDEN	BETYDNING
Arkitektur	Hvordan jeres platform er bygget op og hænger sammen.
API (Application Programming Interface)	Den måde systemer taler sammen på. Et standardiseret interface, der lader jeres applikationer udveksle data med andre tjenester.
Audit	En systematisk gennemgang af, om I gør det, I siger I gør. Handler typisk om sikkerhed, processer eller compliance.
Auditability	Om I kan dokumentere og spore, hvad der er sket i jeres systemer, hvis nogen spørger.
CI/CD (Continuous Integration/Continuous Deployment)	En automatiseret proces i softwareudvikling, der sikrer, at ny kode hurtigt og pålideligt kan bygges, testes og leveres til produktion. En "CI/CD-pipeline" er den tekniske opsætning af denne proces.
Cloud (cloud computing)	Levering af IT (f.eks. servere, lagring, databaser og software) som en tjeneste over netværk, typisk med skalerbarhed og forbrugsbaseret betaling.
CLOUD Act	Amerikansk lov, der giver amerikanske myndigheder ret til at kræve adgang til data hos amerikanske tech-virksomheder – også selvom data ligger i EU. Derfor er "EU-hosting" hos en amerikansk leverandør ikke det samme som EU-kontrol.
Colocation	Driftsmodel, som består af jeres eget hardware, men placeret i et eksternt datacenter, der leverer strøm, køling og fysisk sikkerhed.
Compliance	At leve op til de regler, I er underlagt, f.eks. GDPR, NIS2, branchekrav, kundekontrakter.
Confidential Computing	Teknologi, der krypterer data, selv mens de behandles i hukommelsen. Betyder at cloud-udbyderen teknisk set ikke kan se jeres data.
Container(e)	En måde at pakke en applikation med alt, den har brug for, så den kører ens uanset miljø. Gør det lettere at flytte mellem leverandører og miljøer, og dermed lettere at undgå lock-in.
Dataportabilitet	Evnen til at få jeres data ud – i et brugbart format, uden urimelige omkostninger.
Deploye (deployment)	At få kode ud i produktion. At gøre en applikation eller opdatering live.
Digital Suveræn Råderet	En virksomheds praktiske evne til at træffe bevidste valg om sin teknologi, kende sine afhængigheder og have en beredskabsplan, så den bevarer sin strategiske handlefrihed. Jeres evne til at kende jeres afhængigheder, træffe bevidste teknologivalg og have en beredskabsplan. Det centrale begreb i denne guide.
EU-first	En strategi, hvor man prioriterer at anvende software og infrastruktur, der er ejet, udviklet og hostet af europæiske virksomheder under EU-jurisdiktion.
EU-hosting	At jeres data ligger i datacentre fysisk placeret i EU. Det kan bl.a. være for at øge overholdelsen af GDPR. Det er vigtigt at være opmærksomme på, at det ikke er EU-kontrolleret.
EU-kontrolleret	At leverandøren er ejet og kontrolleret af juridiske enheder i EU. Flere amerikanske tech-giganter og hyperscalere tilbyder EU-hosting, men pga. US-jurisdiktion vil de være underlagt CLOUD Act, og dermed ikke EU-kontrolleret.
Failover	Automatisk eller manuelt skifte til en backup-løsning, når den primære fejler. Det er med henblik på at sikre høj oppetid.
FinOps	En driftsmodel og kultur, der kombinerer finansiel ansvarlighed med DevOps. Målet er at give organisationer fuld kontrol over og indsigt i deres cloud-omkostninger for at kunne optimere forbruget løbende.
Hyperscaler	Betegnelse for de største, globale cloud-leverandører (typisk Amazon Web Services, Microsoft Azure og Google Cloud Platform), kendetegnet ved massiv skalerbarhed, et bredt udbud af services og en global infrastruktur.
Hybrid-cloud	En arkitektur hvor IT-løsninger kører på tværs af både egen infrastruktur (on-premise eller on-location) og eksterne cloud tjenster.

ORDLISTE

ORD I GUIDEN	BETYDNING
Infrastructure-as-Code (IaC)	Praksis, hvor man definerer og administrerer sin it-infrastruktur (servere, databaser, netværk) gennem kode i stedet for manuel konfiguration. Gør det lettere at genskabe og flytte miljøer.
Infrastruktur	Den underliggende tekniske platform, som jeres løsning kører på, herunder servere, netværk, lagring, virtualisering og driftsmiljøer.
Interoperabilitet	Evnen for systemer og løsninger til at udveksle data og fungere sammen.
Jurisdiktionsprincip	Hvilket lands lovgivning, der gælder for jeres data. Afgøres af tre ting: hvor data fysisk ligger, hvem der ejer leverandøren, og hvilken jurisdiktion leverandøren er underlagt. Eksempel: Data hos en amerikansk leverandør kan være underlagt amerikansk lov – også selvom data ligger i EU.
Key Management	Hvem der styrer de nøgler, der krypterer jeres data. I kan lade leverandøren styre dem, I kan levere jeres egne nøgler til leverandøren, eller I kan holde nøglerne helt selv – så leverandøren teknisk set ikke kan dekryptere, uanset hvem der spørger.
Lock-in (leverandørafhængighed)	Situation, hvor det er udfordrende eller næsten umuligt at skifte leverandør, bl.a. på grund af tekniske, kontraktuelle eller økonomiske barrierer.
Managed Service	En IT-tjeneste, hvor en ekstern leverandør overtager det fulde driftsansvar (f.eks. for en database eller applikationsplatform). Managed services øger tempo og bekvemmelighed, men skaber ofte et stærkt teknisk lock-in, som kan gøre det komplekst og dyrt at skifte leverandør.
Microservices	Arkitekturprincip, hvor en løsning opdeles i mindre, selvstændige tjenester der kan udvikles, skaleres og udskiftes uafhængigt af hinanden.
Migration	At flytte data, applikationer eller infrastruktur fra ét miljø til et andet, f.eks. fra on-prem til cloud.
Multi-cloud	En arkitektur hvor flere cloud-udbydere kan anvendes parallelt for at reducere afhængighed af én leverandør og øge robustheden.
On-prem (on-premises):	Infrastruktur, der driftes i jeres egen organisation eller eget datacenter. I ejer og driver det.
Off-prem (off-premises):	Infrastruktur, der kører hos en ekstern leverandør. Det meste cloud er off-prem.
Open source	Software, hvor kildekoden er frit tilgængelig. I en suverænitetskontekst er det værdifuldt, da det reducerer leverandør-lock-in, øger transparensen og giver mulighed for at hoste og modificere løsningen selv.
Portabilitet	Hvor let i kan flytte applikation, data eller platform fra ét miljø til et andet uden større omkostninger eller omskrivning.
SBOM (Software Bill of Materials)	En stykliste over alt det, jeres software er bygget af, f.eks. komponenter, biblioteker, afhængigheder. Bruges til at vide, hvad I faktisk kører, og om der er kendte sårbarheder i det.
Self-hosted	At I selv installerer og driver en løsning. Det kan være på egne servere eller hos en hosting-partner I vælger. Nøgleordet her er kontrol over placering både fysisk og jurisdiktion.
SLA (Service Level Agreement)	En kontraktlig aftale mellem en serviceudbyder og en kunde, der definerer det forventede serviceniveau. Inkluderer typisk garantier for oppetid, svartider og konsekvenser, hvis aftalen ikke overholdes.
SPOF (Single Point of Failure)	En del af en løsning, hvor en fejl vil medføre, at det hele vælter. I en suverænitetskontekst kan en enkelt, kritisk leverandør eller cloud-region udgøre et Single Point of Failure.
Stack	Den samlede kombination af teknologier, jeres løsning er bygget på. Fra database til frontend.
Suites	Sammenhængende pakker af softwareløsninger fra samme leverandør, designet til at fungere integreret, f.eks. Microsoft 365 eller Google Workspace. De er meget praktiske, men skaber ofte dyb afhængighed.
TCO (Total Cost of Ownership)	En beregning af de samlede omkostninger ved en IT-løsning over dens levetid. Inkluderer ikke kun direkte omkostninger (hardware, software, abonnement), men også indirekte omkostninger (drift, vedligehold, uddannelse, support, nedetid).

Marts 2026

DELTAGERNE

TypoConsult A/S

Typoconsult er specialister i open source-baserede web- og CMS-løsninger (især TYPO3), og arbejder suverænt mod at give kunderne fleksible løsninger, samt at sikre kundernes løsninger kan køre videre i tilfælde af nedbrud på deres primære stack.

HUGIN EXPERT A/S

HUGIN EXPERT A/S leverer software til model-baseret beslutningsstøtte under usikkerhed. Softwaren benyttes blandt andet til prædiktiv analyse, forudseende vedligeholdelse og fejlfinding, særligt indenfor compliancetunge sektorer, og arbejder suverænt mod at beskytte kundernes data.

Co-Creators CO ApS

Co-Creators CO ApS udvikler digitale platforme med fokus på fleksibilitet, modulær arkitektur og som understøtter samarbejde hos kunderne. Co-Creators fokus på suverænitet er at sikre kundernes data og at kunne levere løsningerne effektivt til kunderne, så de kan samarbejde så friktionsløst som muligt.

HVIS DU VIL VIDE MERE

DIGITAL LEAD
Martin Grønbæk Jensen
mgj@digitallead.dk
+45 9398 4481

TEKNOLOGISK INSTITUT
Michael Anker Guldager
mics@teknologisk.dk
+45 7220 2937

TEKNOLOGISK INSTITUT
Jessica Lønborg Olsen
jlon@teknologisk.dk
+45 7220 3041

DigitalLead.

TEKNOLOGISK INSTITUT