Anbefalingsnotat fra Tekna, Forbrukerrådet og NITO

Tekna, Forbrukerrådet og NITO arrangerte 13. mai et rundebord om hvordan vi kan operasjonalisere og styrke den nasjonale digitale suvereniteten. Rundebordet samlet sentrale aktører fra offentlig og privat sektor, fagbevegelse og akademia med ekspertise på IKT, digitalisering og offentlige anskaffelser for å identifisere konkrete og realistiske tiltak. På bakgrunn av rundebordet, anbefaler vi Digitaliserings- og forvaltningsdepartementet å iverksette en rekke tiltak.

Samlet viser innspillene fra rundebordet at digital suverenitet ikke handler om én teknologi, én leverandør eller én anskaffelse. Det handler om offentlig sektors evne til å beholde styring og kontroll over egne digitale tjenester, data og infrastruktur, innkjøpsmakt, kompetanse, kontrakter, arkitektur og demokratisk kontroll.

Digital suverenitet betyr ikke at alt må bygges eller driftes av det offentlige selv, men at virksomhetene må ha reell handlefrihet og unngå uheldig leverandørlåsing. Offentlig sektor trenger reell exit-evne; data, dokumentasjon, integrasjoner og drift må kunne flyttes til en annen løsning eller leverandør uten urimelige kostnader, langvarig nedetid eller tap av kontroll.

En strategi for åpen kildekode er et viktig signal. Samtidig bør departementet raskt modernisere Digitaliseringsrundskrivet, gi Direktoratet for forvaltning og økonomistyring (DFØ) i oppdrag å oppdatere maler og veiledere, og sørge for at åpne standarder, portabilitet, interoperabilitet, leverandørdiversitet og reell exit-evne får faktisk betydning i offentlige anskaffelser. Slik kan staten bruke innkjøpsmakten mer strategisk, styrke konkurransen og redusere den digitale sårbarheten over tid.

Tydelige styringssignaler på dette feltet vil også bidra til mer konkurranse, større leverandørmangfold og økt innovasjon. Når offentlige løsninger bygger på åpne standarder og åpen kildekode, kan flere aktører bidra til videreutvikling, og privat sektor kan gjenbruke løsninger som er utviklet eller vedlikeholdt for offentlige midler. Over tid kan dette redusere leverandørmakt og gi offentlig sektor større handlingsrom i møte med de dominerende teknologiplattformene.

Tekna, Forbrukerrådet og NITO vil løfte frem følgende anbefalinger til Digitaliserings- og forvaltningsdepartementet:

1. **Moderniser Digitaliseringsrundskrivet, slik at statlige virksomheter får tydeligere føringer for hvordan de skal vurdere drift,** nyanskaffelser, tjenesteutsetting og videreutvikling av digitale tjenester. Rundskrivet bør presisere at virksomhetene skal vurdere flere modeller, herunder egen drift, drift hos annen offentlig aktør, offentlig kontrollert infrastruktur, åpne løsninger, tjenesteutsetting, skytjenester og kombinasjoner av disse. Rundskrivet bør også ta høyde for de andre anbefalingene i dette dokumentet.
2. **Sørg for at åpen kildekode,** åpne standarder, portabilitet, interoperabilitet, modularitet, leverandørdiversitet og exit-evne får reell betydning i relevante anskaffelser, både som konkrete krav og tildelingskriterier.
3. **Gjør exit-plan, exit-kostnader og dataeksport til standardkrav** i store anskaffelser, slik at virksomhetene vet hvordan data, integrasjoner, dokumentasjon og funksjonalitet kan flyttes eller videreføres ved behov
4. **Krev at åpne og gjenbrukbare løsninger** vurderes før nye IT-anskaffelser, inkludert om eksisterende offentlig finansiert kode, fellestjenester eller åpne løsninger kan videreutvikles for å dekke behovet
5. **Etabler et nasjonalt register over offentlig åpen kildekode,** slik at løsninger kan gjenbrukes, videreutvikles og forvaltes mer systematisk på tvers av offentlig sektor
6. **Gi DFØ i oppdrag å oppdatere maler, veiledere, rammeavtaler og evalueringsmodeller**, slik at virksomhetene får praktiske verktøy for å stille, vekte og følge opp krav til åpne standarder, portabilitet, interportabilitet og exit-evne.

Bakgrunn for tiltakene:

Modernisering av Digitaliseringsrundskrivet

Digitaliseringsrundskrivet bør gi tydeligere føringer for hvordan statlige virksomheter vurderer drift, nyanskaffelser av digitale tjenester, sky, tjenesteutsetting og offentlig kontrollert infrastruktur.

Rundskrivet bør også kreve at statlige virksomheter vurderer åpne og gjenbrukbare løsninger før nye IT-anskaffelser. Virksomhetene bør også stille konkrete krav til åpne standarder, interoperabilitet og modularitet, dokumentere hvordan data kan eksporteres, og beregner exit-kostnader før valg av løsning og leverandør.

Rundskrivet sier i dag at virksomheter som etablerer eller oppgraderer digitale tjenester, fagsystemer eller driftsavtaler, skal vurdere skytjenester på linje med andre løsninger. Flere innspill peker på at virksomheter i praksis kan tolke dette som en føring mot de største globale skyplattformene. Det var neppe intensjonen, men formuleringen bør moderniseres.

Departementet bør presisere at virksomhetene skal vurdere flere modeller: egen drift, drift hos annen offentlig aktør, offentlig kontrollert infrastruktur, tjenesteutsetting, skytjenester eller kombinasjoner. Valget bør bygge på behov, risiko, kontrollkrav, jurisdiksjon, portabilitet, leverandørdiversitet og exit-evne.

Krav til åpne standarder, åpen identitet og reell interoperabilitet

Offentlige anskaffelser bør stille krav til bruk av konkrete åpne standarder for dokumenter, data, API-er, identitet, kalender, meldingsutveksling, arkiv og samhandling.

Kravene må være testbare. Det holder ikke at en leverandør skriver at løsningen «støtter åpne standarder». Oppdragsgiver må vite hvilke standarder løsningen støtter, hvordan støtten dokumenteres, og hvordan den kan testes.

Identitet og tilgangsstyring krever særskilt oppmerksomhet. Når identitetslaget bindes til én leverandørs økosystem, blir hele porteføljen mindre flyttbar. Krav til åpne identitetsstandarder, som OAuth og OpenID Connect, bør derfor inngå i relevante anskaffelser.

Erfaringer fra UiO Share viser at åpne alternativer kan dekke sentrale behov for fildeling, dokumentsamarbeid og kalender. Samtidig blir samhandling mot Microsoft 365 krevende når kalenderdata og dokumentflyt låses i proprietære mekanismer. Svenske eSamverka viser en komplementerende vei: Med åpne protokoller som Matrix kan virksomheter bruke ulike chatløsninger og likevel samhandle.

Suverenitet som teller i evalueringen

For å styrke den digital suverenitet, er de fleste enige om at offentlig sektor bør redusere leverandørlåsing, bruke åpne standarder, sikre portabilitet, interoperabilitet og modularitet, og bygge større digitalt handlingsrom. Utfordringen er at disse prinsippene ofte ikke styrer anskaffelsene i praksis.

Departementet bør gi føringer om at åpen kildekode, åpne standarder, portabilitet, interoperabilitet og exit-evne **skal inngå som reelle tildelingskriterier i relevante anskaffelser.** Det holder ikke å omtale disse hensynene i kravspesifikasjonen dersom de får så lav vekt at pris og funksjonalitet avgjør.

Et innspill fra en større KI-anskaffelse i helsesektoren illustrerer problemet: Funksjonalitet ble vektet 50 prosent og pris 30 prosent, mens sikkerhet samlet ble vektet 7 prosent. Suverenitet inngikk bare som ett underpunkt under sikkerhet. Da får suverenitet liten praktisk betydning for tildelingen, selv om anskaffelsen formelt stiller krav.

Krav til åpne standarder, dokumentert interoperabilitet, dataeksport, leverandørdiversitet og reell exit-evne bør vurderes bredt i offentlige digitale anskaffelser. Vektingen bør samtidig stå i forhold til risiko, avhengighet og samfunnsmessig betydning. For KI, sky, identitet, helse, justis, arkiv, kritiske fagsystemer og beskyttelsesverdige data må slike hensyn veie spesielt tungt.

Leverandørlåsing er likevel ikke bare et problem i de mest kritiske systemene. Også kontorstøtte, samhandlingsløsninger, saksbehandlingsverktøy, analyseplattformer, dokumentflyt, kalender, e-post og andre tilsynelatende mindre kritiske systemer kan skape sterk avhengighet når de blir felles infrastruktur for hele virksomheten. Når slike løsninger samler data, arbeidsprosesser, integrasjoner og identitet i ett lukket økosystem, kan det bli svært krevende å bytte leverandør senere, noe som også kan gå på bekostning av konkurransen i markedet, samt tilliten til både myndighetene og løsningene.

Derfor bør hensynet til portabilitet, interoperabilitet og exit-evne ikke avgrenses til de mest sikkerhetskritiske systemene.

Norge bør også utvikle en norsk tilpasning av et digitalt suverenitetsrammeverk, inspirert av europeiske rammeverk som Cloud Sovereignty Framework og SEAL-nivåer. Et slikt rammeverk kan gi innkjøpere et felles språk for jurisdiksjon, drift, teknologi, åpenhet, sikkerhet, leverandørkjede, rettslig etterlevelse, manglende konkurranse, konsentrasjonsevne for den enkelte virksomhet og offentlig sektor som helhet, og exit-evne.

Exit-evne som standardkrav

Offentlig sektor bør ikke kjøpe større IT-løsninger uten å vite at og hvordan det er mulig å migrere til alternativer ved behov.

Exit-planen må planlegges ved kontraktsinngåelse, ikke når kontrakten skal avsluttes. Virksomhetene bør kreve mulighet for dataeksport i åpne, maskinlesbare formater, migreringsbistand, dokumentasjon av integrasjoner, oversikt over avhengigheter, tilgang til kildekoden, og beregning av exit-kostnader.

Exit må også testes i praksis. En løsning som bare kan forlates på papiret, gir ikke reell handlefrihet. Dette gjelder særlig for sky, KI, identitet, arkiv, kritiske fagsystemer og løsninger som behandler beskyttelsesverdige data.

Vurdering av åpne og gjenbrukbare løsninger før anskaffelsen starter

Moderne digital infrastruktur bygger i stor grad på åpne komponenter. Offentlig sektor bør derfor behandle åpen kildekode som strategisk infrastruktur, ikke som et nisjevalg.

Departementet bør kreve at statlige virksomheter vurderer åpne og gjenbrukbare alternativer før de starter nye IT-anskaffelser.

Vurderingen må komme tidlig. Hvis virksomheten først definerer anskaffelsen som kjøp av en bestemt proprietær pakkeløsning, kan åpne alternativer i praksis være utelukket før konkurransen starter.

Bevisbyrden bør flyttes. Det offentlige bør ikke måtte forklare hvorfor åpne løsninger vurderes. Virksomheten bør heller forklare hvorfor en lukket løsning gir bedre samlet verdi over tid dersom den velger en lukket løsning. Begrunnelsen bør omfatte videreutvikling, gjenbruk, kompetansebygging, portabilitet, leverandøravhengighet, jurisdiksjon og langsiktige kostnader.

Kode, integrasjoner og systemspesifikke tilpasninger som utvikles for offentlige midler, bør som hovedregel leveres med kildekode, dokumentasjon og åpen lisens. Norge bør også etablere et nasjonalt register over offentlig finansiert og offentlig brukt åpen kildekode, etter modell av OpenCoDE i Tyskland og code.gouv.fr i Frankrike.

Offentlig sektor bør ikke bare bruke åpen kildekode, men også bidra til vedlikehold, sikkerhetsarbeid, videreutvikling og finansiering av åpne prosjekter som inngår i åpne løsninger.

Verktøy og kapasitet til å gjennomføre kravene

Krav virker først når virksomhetene får verktøyene de trenger for å bruke dem.

DFØ bør oppdatere veiledning, kontraktsmaler, rammeavtaler og evalueringsmodeller. Virksomhetene trenger konkrete formuleringer for åpne standarder, portabilitet, exit-planer, databruk, kildekode, escrow, change-of-control og migreringsbistand.

DFØ bør også vise hvordan virksomheter kan stille slike krav uten å stenge ute mindre leverandører. Kravene må være relevante og forholdsmessige, men samtidig sterke nok til å endre praksis.

Departementet bør i tillegg koble offentlig IT-kompetanse bedre sammen. Offentlig sektor har sterke fagmiljøer, men bruker dem for fragmentert. Universitetssektoren, Digdir og andre offentlige miljøer kan i enkelte tilfeller levere, drifte eller videreutvikle fellestjenester for flere.

For kritiske fagsystemer, arkiv, identitet og beskyttelsesverdige data må staten stille sterkere krav til offentlig kontroll over arkitektur, kompetanse og drift. Arbeidet med digitalt handlingsrom bør også omfatte den digitale grunnmuren: samtrafikkpunkter, navnetjenere, tidstjenester og sertifikater/root CA.