

Skiftende skydekke

En Skate-rapport om endringsevne i
bruken av skytjenester.

En rapport fra arbeidsgruppe nedsatt av Skate 10.12.2025
Rapport levert 30.06.2026



Innhold

1 Sammendrag.....	4
2 Innledning.....	5
2.1 Leseveiledning.....	7
2.2 Skytjenester – avgrensninger	7
2.3 Tilgjengelig tid som valgt tilnærming.....	9
3 Perspektiver for skytjenester og portabilitet når man har dårlig tid: kort tid for endring.....	10
3.1 Strategisk tilnærming	10
3.2 Tekniske valg	13
4 Perspektiver for skytjenester og portabilitet når man har god tid: Endring på lang og mellomlang sikt.....	15
4.1 Middels lang tid for endring.....	15
4.2 Lang tid for endring.....	20
5 Exitkostnader	26
5.1 Konseptuell modell for exit-vurdering	26
5.2 Dagens leverandøravhengighet	27
5.3 Exit-kostnader	28
5.4 Eksterne kostnads- og risikodrivere.....	32
5.5 Exitgevinster	34
5.6 Gjennomføringsevne	35
5.7 Beslutningsalternativer	36
5.8 Samlet vurdering	37
6 Juridisk – veiledning til kommende EU-regelverk.....	39
6.1 Innledning	39
6.2 Dataforordningen (Data Act)	40
6.3 Fri flyt av andre opplysninger enn personopplysninger i EU (FFD)	42
6.4 Digital omnibus VII	43
6.5 AI Act (KI-forordningen)	43
6.6 Cloud and AI Development Act (CADA)	44
7 Behov for videre tiltak	49
7.1 Kunstig intelligens	49
7.2 Digital suverenitet.....	49

7.3 Utrede avhengighet til SaaS kontorstøtteverktøy	50
7.4 Etablere styringsmekanismer for å sikre gjennomføring av tiltak lokalt.....	50
7.5 Endre rådene til offentlig forvaltning i digitaliseringsrundskrivet	51
7.6 Offentlige fellesavtaler om skytjenester som legger til rette for endringsevne.....	51
7.7 Bruk av åpne standarder, arkitekturprinsipper, arkitektur og standardiseringsrådet og IT-standardiseringsforskriften.....	51
8 Vedlegg.....	52

1 Sammendrag

Arbeidsgruppen anbefaler tiltak for å redusere risikoen for uønsket leverandørbinding, samt å sikre reell råderett over egne data, tjenester og teknologiske veivalg.

Anbefalingene er hovedsakelig å ta mer kontroll over de tekniske miljøene ved å i større grad benytte åpne standarder og åpen kildekode på viktige områder. Virksomheten bør bygge en arkitektur, en kontraktsportefølje og en organisasjon som ikke blir unødig avhengig av én leverandør eller ett bestemt teknologisk økosystem. Dette gjøres ved å legge til rette for hybrid- eller multisky. Formålet er å sikre at et fremtidig skifte er praktisk, teknisk, økonomisk og juridisk mulig. Dette forutsetter at flyttbarhet og portabilitet behandles som strategiske styringshensyn, ikke som rene tekniske detaljer.

Arbeidsgruppen anbefaler at offentlige virksomheter har beredskapsplaner for tap av tilgang til skytjenester. Dette krever oversikt over avhengigheter innad i og mellom forskjellige skytjenesteleveranser. For å sikre virksomhetens evne til kritikalitetsstyring under press, er det nødvendig å ha vurdert hva som er akseptabel minimumsleveranse på forhånd.

Offentlige virksomheter må ha en exit-strategi for skytjenester. Redusert leverandøravhengighet kan ha stor strategisk verdi. Denne verdien må veies opp mot faktiske overgangskostnader, operasjonell risiko og virksomhetens evne til å gjennomføre endringen. Avhengighet har en kostnad, selv om den ofte er mindre synlig. Innlåsing, svak konkurranse, begrenset forhandlingsmakt, økte lisenskostnader, redusert kontroll over data og sårbarhet for eksterne beslutninger kan over tid gi betydelige strategiske ulemper.

Exit-kostnader bør ikke brukes som argument for passivitet, men som grunnlag for bedre beslutninger. Dersom offentlig sektor ønsker å redusere avhengigheten til dominerende teknogileverandører, må dette gjøres planmessig, trinnvis og med god forståelse for de økonomiske, tekniske, juridiske og organisatoriske konsekvensene.

En god exit-strategi bør derfor som minimum inneholde:

1. en samlet oversikt over eksisterende leverandøravhengigheter
2. en vurdering av hvilke tjenester som er mest kritiske
3. en kartlegging av alternative løsninger
4. en realistisk beregning av direkte og indirekte exit-kostnader
5. en vurdering av eksterne kostnads- og risikodrivere, særlig regelverksendringer fra EU
6. en vurdering av mulige exit-gevinster på kort og lang sikt
7. en vurdering av virksomhetens gjennomføringsevne
8. en vurdering av sikkerhet, personvern og etterlevelse
9. en plan for migrering, opplæring og parallell drift
10. tydelige beslutningspunkter for videreføring, justering eller stans

11. en plan for finansiering, gevinstrealisering og langsiktig forvaltning

En exit-strategi uten kostnadsforståelse kan bli urealistisk. En kostnadsforståelse uten strategisk retning kan føre til at dagens avhengighet videreføres. Det offentlige bør derfor kombinere langsiktig mål om større digital handlefrihet med nøkterne vurderinger av hva overgangen faktisk krever, hvilke gevinster som kan realiseres, hvordan kostnader og gevinster fordeles mellom ulike nivåer i offentlig sektor, og hvordan endringer i regelverk, marked, sikkerhet og geopolitikk kan påvirke både kostnader, risiko og muligheter over tid.

2 Innledning

I norsk offentlig sektor har det de siste ti årene vært en sterk bevegelse i retning av å ta i bruk skytjenester. I lys av den usikre internasjonale politiske situasjonen har det imidlertid blitt stilt spørsmål ved norsk offentlig sektors endringsevne i bruken av skytjenester. Blant annet har Datatilsynet uttrykt bekymring for at offentlige virksomheter ikke er forberedt på en eventuell exit fra store IT-leverandører. Norsk offentlig sektor er i dag tett koblet til noen få leverandører som har sterke incentiver til å skape innlåsingeffekter, er underlagt andre lands jurisdiksjon, og kan påvirkes av interesser som ikke er forenlig med våre egne. Offentlige virksomheter bør ikke være avhengige av enkeltaktører for å levere tjenestene sine.

Manglende eller svært begrensede muligheter for flytting av tjenester mellom ulike skytjenester, såkalt interoperabilitet, representerer et stort hinder for å bytte skytjenesteleverandør. Store avhengigheter til enkeltleverandører kan vise seg nærmest umulig å bryte opp på kort sikt. Til nå har det vært lav oppmerksomhet om virksomhetenes evne og/eller mulighet for å flytte mellom skytjenester. Offentlige virksomheter bør derfor i større grad arbeide ut fra prinsipper om *endringsevne*, for å ivareta langsiktig kontinuitet i tjenestetilbudet og sikre reell konkurranse blant skytjenesteleverandørene.

Arbeidsgruppen ble nedsatt av SKATE¹ i desember 2025. Gruppen har bestått av:

Frode Alne Bolin (Digdir)	Prosjektleder
Edvin Tengs Leirvåg (Digdir)	Juridisk kompetanse
Erling Solberg (Skatteetaten)	Juridisk kompetanse
Thorstein Sjursen (Skatteetaten)	Juridisk kompetanse
Suhail Mushtaq (KS)	Strategisk kompetanse
Tore Andre Mikalsen (Norsk Helsenett)	Teknisk kompetanse

¹ <https://www.digdir.no/skate/skate/1259>

Eirik Mikkelsen (Digdir)	Teknisk kompetanse
Magnus Dahl Mortensen (Larvik kommune)	Teknisk kompetanse
Torkjell Dahl (Ringerike kommune)	Teknisk kompetanse

Arbeidsgruppen har hatt en referansegruppe, som har bestått av representanter fra NSM, Politiet, Lånekassen, KS, SIKT, SSB, Helsedirektoratet, Kartverket, NAV og Oslo kommune.

Arbeidsgruppens mandat og leveranser tar utgangspunkt i hvordan virksomheter kan planlegge for å møte utfordringene beskrevet over. Siden arbeidsgruppen ble etablert, har det vært økende oppmerksomhet om digital suverenitet, forstått som nasjonal kontroll på det digitale området. Det ligger imidlertid utenfor arbeidsgruppens mandat å mene noe om behovet for nasjonal kontroll med skytjenester i streng forstand. Ønsket om nasjonal kontroll er ofte begrunnet i sikkerhetshensyn, og slike vurderinger ligger først og fremst til Justis- og beredskapsdepartementet og deres underliggende virksomheter.

På disse premissene har Skate bedt arbeidsgruppen om å levere følgende:

- 1) Ferdigstille prinsipper for dataportabilitet mellom skytjenester
- 2) Rapportere om relevant utvikling i EU
- 3) Ferdigstille prinsipper for å vurdere exit-kostnader fra skytjenester
- 4) Ferdigstille veiledning til kommende EU-regulering på området
- 5) Vurdere om det er behov for tiltak som ikke allerede er dekket opp på området

Punktene 1, 2 og 3 er gitt leveransefrist Q2 (30. juni), mens punktene 4 og 5 er gitt leveransefrist Q3 (30. september).

Arbeidsgruppen har vurdert at det vil være mest hensiktsmessig å svare ut alle bestillingspunktene i ett samlet dokument med leveranse 30. juni.

Situasjonen har tilspisset seg siden mandatet først ble foreslått i SKATE. Ved opprettelsen av arbeidsgruppen var faktorene regulatorisk risiko, Europas fokus på suverenitet og risiko for geopolitisk innflytelse nevnt som begrunnelse for å bedre muligheter for endring mellom skytjenesteleverandører. Siden har fokuset i større grad blitt flyttet mot konsentrasjonsrisiko hos enkelte store leverandører² og nasjonal suverenitet³. Arbeidsgruppen konstaterer at verden er inne i en urolig periode, der spesielt folkeretten virker svekket. Arbeidsgruppen erfarer at det er mange som arbeider med spørsmål om mulig endring av skytjenesteleverandører. Dette er naturlig, da det offentlige er forventet å lyse ut tjenesteavtaler. Uten evne til å flytte mellom skyleverandører vil virksomhetene ikke kunne benytte seg av markedet.

Som allerede påpekt, er våren 2026 preget av store endringer internasjonalt, både politisk og teknologisk. Utviklingen skjer raskt, og tar stadig uventede retninger. Det er

² [Risiko 2026 - Nasjonal sikkerhetsmyndighet](#)

³ Representantforslag 8:119 S [Sak - stortinget.no](#)

derfor viktig å understreke at de anbefalingene som gis i denne rapporten, er i tråd med skytjenestelandskapet slik det fremstår i første halvdel av 2026.

2.1 Leseveiledning

Denne rapporten har en bred målgruppe, og både beslutningstakere, byråkrater, jurister, IT-strateger og teknologer (på både nasjonalt og lokalt nivå) vil kunne ha nytte av analyser og anbefalinger. Noen deler av dokumentet vil være særlig interessante for enkelte grupper, og tilsvarende vanskelig tilgjengelig for andre. Derfor følger her en leseveiledning for dokumentet:

1) Sammendrag og 2) Innledning er beregnet å kunne gi utbytte til alle grupper av lesere.

Kapittel 3) og 4) er knyttet opp mot ulike scenarioer, der man har underkapitler som ser på strategiske og tekniske valg:

- Kapitlene om de strategiske valgene er relativt overordnede, og kan særlig være relevante for beslutningstakere og IT-strateger.
- Kapitlene om tekniske valg er detaljerte og er i hovedsak relevant for teknologer.

Kapittel 5) om exit-kostnader og -gevinster vil særlig være interessant for beslutningstakere.

Kapittelet 6) Juridisk – veiledning til kommende EU-regelverk, vil særlig være relevant for jurister, beslutningstakere og byråkrater.

Kapittel 7) Behov for videre tiltak er et sentralt kapittel for dem som skal vurdere videre arbeid med tematikken skytjenester, nasjonalsuverenitet og kontroll overdata, da særlig politikere og ansatte i embetsverket.

2.2 Skytjenester – avgrensninger

Begrepet "skytjenester" står sentralt i dette dokumentet. Arbeidsgruppen ser at det er stort spenn i forståelsen av begrepet, og vil derfor tydeliggjøre hva dokumentet favner og ikke favner. Dette er også nødvendig av hensyn til arbeidsgruppens kapasitet og tidsrammer. Arbeidsgruppen har i sitt arbeid forholdt seg til definisjonene av begreper om skytjenester som er fastsatt i ISO/IEC 22123.

Plassering av skytjenestene (allmenn, hybrid eller privat) vil ikke ha innvirkning på prinsippene som beskrives og vil derfor ikke omtales nærmere.

Sikkerhet og krav til sertifiseringer i skytjenester kan være viktig for enkeltkunder, men faller utenfor leveransen.

2.2.1 Skytjenester som er omfattet

Infrastructure as a Service, **laas**.

- En skytjenestekategori der skyleverandøren tilbyr grunnleggende infrastrukturkapasitet, som virtuelle maskiner, lagring, nettverk og andre databehandlingsressurser.
- Kunden har kontroll over operativsystemer, lagring, applikasjoner, mellomvare og virtuelle nettverkskonfigurasjoner, men ikke den underliggende fysiske infrastrukturen.
- Brukes til å bygge, teste og drifte applikasjoner og systemer med god kontroll over den virtuelle infrastrukturen.

Platform as a Service, **PaaS**

- En skytjenestekategori der skyleverandøren tilbyr en plattform for utvikling og drift av applikasjoner, inkludert runtime-miljø, utviklingsverktøy, biblioteker og tilhørende tjenester.
- Kunden har kontroll over applikasjoner og applikasjonskonfigurasjon, men ikke over operativsystem, runtime eller underliggende infrastruktur (f.eks. nettverk, servere og lagring).
- Brukes til utvikling, testing og drift av applikasjoner uten å måtte administrere infrastruktur eller plattformkomponenter.

Software as a Service, **SaaS**

- En skytjenestekategori der skyleverandøren tilbyr ferdige programvare-applikasjoner som leveres over nettverk og brukes via nettleser eller andre klientgrensesnitt.
- Kunden bruker applikasjonen uten kontroll over underliggende infrastruktur, plattform eller applikasjonsarkitektur, men kan gjøre begrenset konfigurasjon gjennom brukerinnstillinger og applikasjonsspesifikke valg.
- Brukes til å levere fullstendige applikasjoner til sluttbrukere, der leverandøren håndterer drift, vedlikehold, oppdateringer og sikkerhet.

2.2.2 Skytjenester som ikke er omfattet

Noen skytjeneste-typer er helt utelatt eller får begrenset omtale av hensyn til tids- og kapasitetsbegrensninger. Arbeidsgruppen anbefaler at disse vurderes nærmere på et senere tidspunkt, se punkt 6, nedenfor.

Skytjenester for kontorstøtte

- Skybaserte kontorstøtteapplikasjoner som leveres som SaaS (Software as a Service). Applikasjonene brukes direkte via nettleser eller dedikerte klienter, uten lokal installasjon.

Skytjenester for klientoperativsystem

- Et operativsystem som kjører på en lokal enhet, men er optimert for å koble seg til og bruke skytjenester. Operativsystemet kan være såkalt tynt (thin client) eller fullverdig, men er avhengig av skyinfrastruktur for lagring, applikasjoner og databehandling.

Skytjenester for IoT

- Internet of Things, en skytjenestekategori for et bredt spekter av enheter som sensorer, wearables og smart hjemmeutstyr, med fokus på skalerbarhet, datainnsamling, lagring og grunnleggende analyse for forbruker- eller virksomhetsapplikasjoner. Favner også varianter som Industrial-IoT og Medical-IoT.

Skytjenester for OT

- Operational Technology, en skytjenestekategori for industrielle miljøer. Integrerer operasjonell maskinvare med programvare som overvåker og kontrollerer fysiske prosesser, enheter og infrastrukturindustrielle kontrollsystemer og prosesser.

2.3 Tilgjengelig tid som valgt tilnærming

Arbeidsgruppens fremstilling tar utgangspunkt i to forskjellige scenarioer for endring. Forskjellen mellom dem er hvor lang tid som er tilgjengelig for å utføre endringene.

Perspektiver for skytjenester og portabilitet når man har dårlig tid: kort tid for endring

I dette perspektivet vil behovet for konkrete endringer aktualisere seg innenfor et tidsrom på 0 – 6 måneder. Dette perspektivet kan i praksis betraktes som krisehåndtering.

Dette scenariet gir ikke rom for kontraktstilpasninger, samt lite rom for juridiske avklaringer og tilrettelegging av tekniske løsninger for å understøtte skytjenesteportabilitet.

Perspektiver for skytjenester og portabilitet når man har god tid: Lang og mellomlang tid for endring

I dette perspektivet vil behovet for konkrete endringer aktualisere seg innenfor et tidsrom på mellom 6 måneder og 10 år.

For å få frem nyansene er dette perspektivet todelt:

Lang tid for endring:

Behovet for konkrete endringer aktualiserer seg innenfor et tidsrom på 3 - 10 år.

Dette scenariet gir stort rom for kontraktstilpasninger, juridiske avklaringer og tilrettelegging av tekniske løsninger for å understøtte skytjeneste portabilitet.

Middels lang tid for endring:

Behovet for konkrete endringer aktualiserer seg innenfor et tidsrom på 6 måneder - 3 år. Dette scenario gir lite rom for kontraktstilpasninger, men noe rom for juridiske avklaringer og tilrettelegging av tekniske løsninger for å understøtte skytjeneste portabilitet.

3 Perspektiver for skytjenester og portabilitet når man har dårlig tid: kort tid for endring

I dette scenarioet er situasjonen at virksomheten så raskt som mulig må flytte fra skytjenesten. Forholdene tilsier at virksomheten må over på ny tjeneste i løpet av 0-6 måneder. Dette omfatter både tilfeller der virksomheten selv bestemmer at behovet for flytting er akutt, og der tjenesten av andre årsaker midlertidig eller permanent bortfaller. Scenarioet innebærer at det er svært begrenset eller ingen tid til forberedelser.

3.1 Strategisk tilnærming

I dette scenarioet må virksomhetens strategiske tilnærming ta utgangspunkt i at bortfall av skytjenester kan være både en teknisk hendelse eller krise av lokalt omfang, men også en bred operativ og samfunnsmessig krise. Dersom tilgangen til skytjenester faller bort som følge av geopolitisk ustabilitet, sanksjoner, leverandørsvikt eller sikkerhetspolitiske kriser, vil virksomheten kunne stå overfor en situasjon der normale forutsetninger for drift, leverandørstøtte og markedskapasitet ikke lenger gjelder.

Målet må være å sikre virksomhetens overlevelsessevne. Det innebærer ikke å opprettholde full funksjonalitet eller normal tjenestekvalitet, men å sikre at de mest kritiske delene av samfunnsoppdraget kan videreføres. Strategien bør bygge på en erkjennelse av at tid, kompetanse, infrastruktur og leverandørkapasitet vil være knapphetsressurser i en krisesituasjon.

Virksomheten må også legge til grunn at den ikke nødvendigvis vil være alene om å stå i et slikt scenario. Dersom flere offentlige og private virksomheter samtidig får behov for nød-migrasjon, alternativ drift eller bistand fra de samme underleverandørene, vil kapasiteten i markedet raskt bli utilstrekkelig. Dette gjelder både datasenterkapasitet, maskinvare, nettverk, sikkerhetsressurser, migrasjonskompetanse og juridisk/kontraktsmessig støtte. Kapasitet hos underleverandører og partnere må derfor inngå som en sentral del av den strategiske vurderingen.

Følgende prinsipper bør ligge til grunn for virksomhetens strategiske arbeid i dette scenarioet:

3.1.1 Kritikalitetsstyring: Prioritering under press

Når tiden er knapp og ressursene er begrensede, kan ikke alle systemer, data og tjenester prioriteres likt. Virksomheten bør derfor legge en verdikjedebasert tilnærming til grunn, der det tydelig identifiseres hvilke funksjoner som er nødvendige for å videreføre samfunnsoppdraget på et minimumsnivå.

Kritikalitetsstyring handler om å skille mellom det som er virksomhetskritisk, det som er viktig, og det som midlertidig kan stanses. Dette må være avklart før krisen oppstår, slik at virksomheten ikke må gjøre grunnleggende prioriteringer under tidspress og usikkerhet.

Identifisering: Virksomheten bør kartlegge hvilke systemer, data og prosesser som understøtter samfunnskritiske og lovpålagte funksjoner. Dette omfatter både primære fagsystemer, nødvendige registre, autentiseringsløsninger, integrasjoner og informasjonsgrunnlag som er avgjørende for å opprettholde liv, helse, sikkerhet, rettigheter eller andre kjerneoppgaver. Kartleggingen bør gi et tydelig bilde av hvilke deler av systemporteføljen som må prioriteres ved alvorlig bortfall av skytjenester.

Differensiering: Ressurser bør styres mot de funksjonene som er nødvendige for å sikre liv, helse, kritiske rettigheter og virksomhetens mest sentrale leveranser. Støttefunksjoner, analysekapasitet, avanserte digitale tjenester og sekundære prosesser må kunne aksepteres nedstengt, redusert eller satt i ventemodus. En slik differensiering gjør det mulig å bruke begrenset kapasitet der den gir størst samfunnsmessig effekt.

3.1.2 Minimumsleveranse framfor full funksjonalitet

I en krisesituasjon er full funksjonalitet ikke et realistisk mål. Strategien bør derfor skifte fokus fra normal drift og sømløs brukeropplevelse, til minimumsleveranse og kontinuitet i kjerneoppgaver. Det avgjørende er at virksomheten kan opprettholde et forsvarlig tjenestenivå innenfor de mest kritiske områdene, selv om store deler av den ordinære digitale støtten faller bort.

Dette krever at virksomheten på forhånd har definert hva som er et akseptabelt minimumsnivå for drift. Minimumsleveranse må være konkret nok til å kunne styre tekniske, organisatoriske og ledelsesmessige prioriteringer i en krise.

Minimum Viable Operations: Virksomheten bør definere det absolutte minimumsnivået for drift, datatilgang, saksbehandling, kommunikasjon og beslutningsstøtte. Dette kan innebære at enkelte tjenester kjøres i sterkt forenklet form, at data oppdateres sjeldnere, eller at manuelle prosesser erstatter automatiserte arbeidsflyter. Minimumsnivået bør knyttes til konkrete funksjoner og verdikjeder, ikke bare til enkeltstående systemer.

Aksept for tap: Ledelsen bør på forhånd ha avklart hvilke funksjoner, tjenester og kvalitetskrav som kan tapes midlertidig uten at virksomhetens samfunnsoppdrag bryter sammen. Dette innebærer en eksplisitt aksept for at avansert funksjonalitet, automatisering, analyse, rapportering og brukerkomfort kan falle bort, til fordel for enklere, mer robuste og eventuelt manuelle løsninger. En slik aksept må være forankret før krisen oppstår, slik at organisasjonen kan handle raskt og samlet.

3.1.3 Avhengighetsforståelse: Kartlegging av økosystemet

En offentlig skytjeneste er sjelden en isolert teknisk løsning. Den inngår som regel i et komplekst økosystem av underleverandører, tredjepartstjenester, integrasjoner, sikkerhetsmekanismer, autentiseringsløsninger, dataplattformer og driftsprosesser. I en krisesituasjon kan svikt i ett ledd få konsekvenser for hele tjenestekjeden.

Virksomheten bør derfor ha en dypere forståelse av hele leveranseøkosystemet, ikke bare hovedleverandøren. Dette er særlig viktig dersom mange virksomheter samtidig er avhengige av de samme underleverandørene eller teknologikomponentene. Manglende

oversikt kan føre til at virksomheten overvurderer egen beredskap eller planlegger for alternativer som i praksis ikke er tilgjengelige.

Dyp innsikt: Virksomheten bør kartlegge kritiske tredjepartskomponenter som SaaS-tillegg, API-er, identitets- og tilgangsstyring, sikkerhetsverktøy, nettverkskomponenter, driftsleverandører og integrasjonstjenester. Kartleggingen bør vise hvilke komponenter som er nødvendige for minimumsdrift, hvilke som har alternative leverandører, og hvilke som representerer enkeltpunkter for svikt. Slik innsikt gir bedre grunnlag for realistisk beredskapsplanlegging.

Relasjonell beredskap: Virksomheten bør identifisere hvilke partnere, underleverandører og myndighetsaktører som er nødvendige for å gjennomføre nødmigrasjon, alternativ drift eller gjenoppbygging. Det bør etableres kontaktveier, eskaleringsrutiner og avtaleverk som tar høyde for krisescenarioer. Relasjonell beredskap handler ikke bare om å vite hvem som skal kontaktes, men om å sikre at samarbeid kan fungere når markedet er presset og flere aktører konkurrerer om de samme ressursene.

3.1.4 Kapasitetsrealisme: Planlegging for knapphet

Virksomheten bør planlegge ut fra en realistisk forståelse av at kapasitet vil være knapp i en alvorlig krisesituasjon. Dersom mange virksomheter samtidig må flytte tjenester, etablere alternativ drift eller sikre tilgang til lokal infrastruktur, vil markedet raskt kunne bli overbelastet. Det kan derfor ikke legges til grunn at nødvendige ressurser vil være tilgjengelige når behovet oppstår.

Kapasitetsrealisme innebærer at virksomheten må vurdere hvilke ressurser som må sikres på forhånd, hvilke som kan deles med andre, og hvilke som ikke realistisk kan skaffes i en krise. Dette gjelder både teknisk infrastruktur, personell, leverandørstøtte, lokaler, nettverk, sikkerhetskapasitet og beslutningsstøtte.

Infrastruktur: Virksomheten bør ikke legge til grunn at det finnes ledig maskinvare, datasenterplass, nettverkskapasitet eller lagringsressurser i det åpne markedet ved en nasjonal eller sektorovergripende krise. Dersom alternativ drift krever konkret fysisk eller logisk kapasitet, må dette vurderes og eventuelt sikres på forhånd gjennom avtaler, reserverte miljøer, rammeavtaler eller sektorvise beredskapsløsninger. Uten slik forhåndsavklaring kan en nødplan vise seg å være urealistisk.

Kompetanse: Ekspertisen som kreves for å flytte komplekse arbeidslaster, gjenopprette tjenester, rekonfigurere sikkerhetsmodeller og etablere alternativ drift, vil være en begrenset ressurs. Virksomheten bør derfor sikre et minimum av intern kompetanse på kritiske systemer, dataflyter og gjenoppbyggingsprosesser. I tillegg bør det vurderes beredskapsavtaler med utvalgte partnere som gir tydelig prioritet, responstid og tilgang til relevant kompetanse i en krisesituasjon. Dette reduserer risikoen for at virksomheten blir stående i kø når behovet for bistand er størst.

3.2 Tekniske valg

Scenarioet 'Kort tid for endring' gir lite rom for tilrettelegging av tekniske løsninger og standarder for å understøtte skytjenesteportabilitet. Dette er et scenario der man trenger rask flytting av skytjeneste, uten nødvendigvis å ha tilrettelagt for portabilitet på forhånd. All forutgående tilrettelegging, som beskrevet i scenarioene for lang og mellomlang tid, vil imidlertid være til stor hjelp.

Tiltakene i dette kapittelet er primært ment som et teknisk førstehjelpsskrin i en akutt situasjon. Hvis man må flytte systemer på under seks måneder, er det sjelden tid til å skrive om store mengder kode eller gjøre store nyinnkjøp – man må løse problemet med de verktøyene man har.

Beskrivelser av tekniske valg i dette kapittelet kan derfor benyttes i to perspektiver:

- I en normalsituasjon fungerer punktene godt som et utgangspunkt for øvelse eller testing av portabilitet. Målet er ikke nødvendigvis at man skal ha alt ferdig oppsatt i dag, men at man har tenkt gjennom problemstillingene. Selv en ren «papirøvelse» rundt et møtebord gir et enormt forsprang den dagen noe skjer. De punktene som lar seg teste uten å forstyrre produksjonsmiljøet, bør testes.
- Står man midt i en oppstått krise når dette leses, fungerer punktene mer som en sjekkliste for hva fagmiljøene bør prioritere å redde eller etablere aller først.

3.2.1 Teknisk tilrettelegging for effektiv portering

3.2.1.1 IaaS

Overordnet anbefaling for IaaS-området er å finne raskeste mulighet for reetablering av tilsvarende skytjeneste eller andre løsninger på minimumsnivå.

Følgende tilnærminger kan understøtte dette:

- **Identifiser kritiske data:** Prioritere umiddelbar uthenting av databaser og filområder.
- **Etabler "Landing Zone":** Opprette et minimalt driftsmiljø hos en alternativ leverandør i Norge eller Europa eller omdisponere eventuelle onprem ressurser.
- **Gjenopprett fra backup:** Benytte de siste sikkerhetskopiene lagret uavhengig av primærleverandøren.
- **DNS-ompeking:** Klargjøre endring av DNS-oppføringer med lav TTL (Time to Live) for rask ompeking til det nye miljøet.
- **Bulk-eksport av secrets:** Hente ut alle passord, API-nøkler og tilkoblingsstrenger fra leverandørens "Secret Manager", til en sikker offline-lokasjon. Dette må løses med skript, da de fleste skyleverandører - av sikkerhetsmessige årsaker - ikke tilbyr dette "ut-av-boksen".
- **Manuelt sertifikatskifte:** Dersom leverandøren kontrollerer virksomhetens SSL-/TLS-sertifikater, må man umiddelbart utstede nye sertifikater via en uavhengig part, for å kunne gjenopprette kryptert trafikk i mottaksmiljøet.

- **Nødomruting via BGP:** Ved bruk av Bring Your Own IP (BYOIP), utføre teknisk ompeking av trafikk på ruting-nivå, for å flytte innkommende trafikk til det nye miljøet umiddelbart.
- **Snapshotkonvertering:** Bruk verktøy for å konvertere disksnapshot fra proprietære formater til åpne formater (som RAW eller QCOW2), for umiddelbar import i det nye miljøet. Få skyleverandører tilbyr nedlasting av snapshots som enkelt kan konverteres, ta derfor først backup til uavhengig leverandør eller koble disker til en virtuell maskin i skymiljøet for å kloner disse.

3.2.1.2 PaaS

Overordnet anbefaling for PaaS-området er å finne raskeste mulighet for reetablering av tilsvarende skytjeneste eller andre løsninger på minimumsnivå.

Følgende tilnærminger kan understøtte dette:

- **Containerflytting/-gjenoppbygging:** Distribuerer eksisterende container-images til alternative kjøremiljøer som støtter standardiserte orkestreringsverktøy.
- **Sikre krypteringsnøkler:** Hente ut nøkler og sertifikater umiddelbart fra leverandørens hvelv, slik at data kan dekrypteres i det nye miljøet.
- **Råeksport:** Utføre en "database dump", fremfor å prøve komplisert synkronisering under tidspress (ved svært lite tid til rådighet, for å sikre dataene mot tap/sletting).
- **Ompeking av API-endepunkt:** Oppdatere konfigurasjonsfiler eller miljøvariabler for å peke mot de nye IP-adressene eller vertsnavnene i mottaksmiljøet.
- **Nødproxy:** Ved behov, sette opp en midlertidig proxy-tjeneste for å rute trafikk mellom den gamle og den nye lokasjonen, mens migreringen pågår.
- **Injeksjon av miljøvariabler:** Bruke skript for å injisere nye tilkoblingsstrenger og miljøkonfigurasjoner i orkestreringen, slik at tjenester finner nye databaseendepunkter etter oppstart.
- **Automatisert gjenoppbygging av tilgangsstyring (RBAC):** Benytt skript for å gjenskape rollestyrte tilgangskontroller i det nye mottaksmiljøet, og løsninger basert på åpne standarder for identitetssynkronisering (eks. SCIM eller OIDC) for identiteter. Dette for å kunne gjenskape identiteter og tilganger under tidspress, samt unngå manuelle feiloppsett.

3.2.1.3 SaaS

Overordnet anbefaling for SaaS-området er å finne best mulig reetablering av tilsvarende skytjeneste. Anbefalingene omfatter ikke kontorstøtterelatert SaaS.

Følgende tilnærminger kan understøtte dette:

- **API-uthenting:** Bruke tilgjengelige API-grensesnitt for å dumpe ut rådata i formater som JSON eller CSV.

- **Manuelle reserveløsninger:** Klargjøre enkle verktøy (f.eks. regneark eller lokale databaser) for å kunne lese de eksporterte dataene og opprettholde kritisk drift og saksbehandling.
- **Identiteter:** Aktivere/ta i bruk alternative autentiseringskilder hvis den primære påloggingsløsningen blir utilgjengelig.
- **Integritetssjekk:** Utføre (automatisert) sammenligning av sjekksummer ("hashes") på de viktigste datasettene før og etter flytting, for å sikre at ingen data ble korrupte under transporten.
- **Minimumstest:** Verifisere kritiske verdikjeder - f.eks. pålogging og lagring av nye data - før systemet åpnes for brukere.
- **Datavask:** Ha ferdige skript (f.eks. Python eller ETL-verktøy) klare for å transformere dataeksport til formatet som kreves av en ny løsning.
- **Nødprioritering av metadata:** Ved flytting av data mellom SaaS-løsninger under tidspress, må tekniske prosedyrer prioritere eksport av metadata (relasjoner, historikk og tilgangsrettigheter), da disse kan være like kritiske for tjenestegenoppbygging som rådata alene. Relasjonsdata må eksporteres i et flatt, menneske- og maskinlesbart format (eks. CSV- eller JSON-fil). Dette sikrer at dataene forblir sporbare også i enkle reserveløsninger.

4 Perspektiver for skytjenester og portabilitet når man har god tid: Endring på lang og mellomlang sikt

4.1 Middels lang tid for endring

Scenarioet beskriver en situasjon der behovet for konkrete endringer aktualiserer seg innenfor et tidsrom på 6 måneder - 3 år. Behovet kan være foranlediget av situasjoner som for eksempel endrede regulatoriske rammer enten nasjonalt eller på EU-nivå, og endrede prioriteringer eller føringer fra ledelse eller politisk hold. Felles for situasjonene er at behovet for endring ikke oppstår akutt, men blir synlig på litt lengre sikt, og at det derfor er noe tid til å vurdere alternativer og kartlegge konsekvenser på en grundig måte.

4.1.1 Strategisk tilnærming

I det mellomlangsiktige perspektivet bør virksomhetens strategiske fokus være en aktiv styrking av egen endringskapasitet. Det innebærer at virksomheten ikke bare skal ha planer for en eventuell utfasing av eksisterende skytjenester, men gradvis bygge de tekniske, organisatoriske og kontraktsmessige forutsetningene som gjør en slik utfasing praktisk gjennomførbar.

Formålet er å etablere broene mellom dagens driftsmodell og mulige fremtidige alternativer. Dette skal skje uten at daglig drift svekkes eller at virksomheten påtar seg unødvendig kompleksitet. Den mellomlangsiktige strategien bør derfor handle om å

redusere avhengigheter, teste realistiske alternativer og utvikle kompetanse som gjør virksomheten i stand til å gjennomføre endringer kontrollert dersom behovet oppstår.

I denne fasen bør virksomheten legge vekt på tiltak som øker fleksibiliteten over tid. Det betyr at arkitektur, dataforvaltning, leverandørstyring og organisasjonsutvikling må ses i sammenheng. Endringskapasitet skapes ikke gjennom enkeltstående tiltak, men gjennom en samlet utvikling av løsninger, prosesser og kompetanse som gjør virksomheten mindre sårbar for teknologiske eller kommersielle bindinger.

Følgende prinsipper bør styre arbeidet i denne fasen:

4.1.1.1 Etablering av vendbare arkitekturmønstre

Virksomheten bør gradvis bevege seg bort fra dype, proprietære integrasjoner og over til en mer modulær og vendbar arkitektur. Med dette menes en arkitektur der sentrale tjenester, dataflyter og integrasjoner kan flyttes, erstattes eller kobles om, uten at hele systemlandskapet må bygges på nytt.

En slik tilnærming reduserer risikoen for at virksomheten blir teknisk bundet til én bestemt leverandør, og gir bedre forutsetninger for å gjennomføre fremtidige endringer kontrollert. Arkitekturen bør derfor utformes slik at avhengigheter blir synlige, dokumenterte og håndterbare.

Abstraksjon: Mellomvare, API-lag og integrasjonsplattformer bør brukes strategisk for å frikoble applikasjoner fra den underliggende skyinfrastrukturen. Dette gjør det enklere å endre eller erstatte tekniske komponenter, uten at hele applikasjonsporteføljen påvirkes. Abstraksjon bør ikke innføres som et mål i seg selv, men der det gir reell reduksjon av leverandøravhengighet og styrker virksomhetens evne til å flytte tjenester mellom miljøer.

Data-frikobling: Virksomheten bør sikre at data lagres, struktureres og dokumenteres på en måte som understøtter portabilitet. Det innebærer blant annet å unngå unødvendig avhengighet til leverandørspesifikke databasemotorer, proprietære lagringsformater eller lukkede analyseverktøy. Data bør kunne eksporteres, valideres og gjenbrukes i alternative miljøer uten omfattende ombygging. Dette er avgjørende for at virksomheten skal beholde reell råderett over egne data.

4.1.1.2 Aktiv redundans og «reverse cloud»-testing

En teoretisk exit-plan har liten verdi hvis virksomheten ikke har praktisk erfaring med alternativ drift. I det mellomlangsiktige perspektivet bør virksomheten derfor bygge gradvis erfaring med løsninger som kan fungere utenfor dagens primære skyleverandør. Dette kan gjøres gjennom avgrensede piloter, beredskapsøvelser, speiling av data, hybrid drift eller testflytting av mindre kritiske tjenester.

Hensikten er ikke nødvendigvis å etablere full parallell drift, men å skape realistisk kunnskap om hva som faktisk kreves for å flytte, gjenopprette eller drifte tjenester i et annet miljø. Slik erfaring gir bedre beslutningsgrunnlag, avdekker skjulte avhengigheter og gjør virksomheten bedre forberedt på en kontrollert overgang.

Hybrid drift i praksis: Virksomheten bør vurdere om enkelte støttefunksjoner, testmiljøer eller speilede datasett kan kjøres lokalt, i privat sky eller hos alternative leverandører. Dette kan bidra til å opprettholde teknisk kompetanse på flere plattformer og redusere risikoen for at virksomheten kun mestrer én driftsmodell. Hybrid drift bør brukes målrettet der det gir læring, robusthet eller strategisk fleksibilitet, og ikke innføres som generell kompleksitet uten tydelig formål.

Migrasjonsøvelser: Virksomheten bør gjennomføre tekniske piloter der mindre kritiske tjenester faktisk flyttes mellom miljøer. Slike øvelser gir praktisk innsikt i hvor lang tid flytting tar, hvilke data- og integrasjonsavhengigheter som oppstår, hvilke kompetansebehov som melder seg, og hvilke kostnader som er knyttet til migrasjon. Erfaringene bør dokumenteres og brukes til å forbedre arkitektur, kontrakter, beredskapsplaner og fremtidige anskaffelser.

4.1.1.3 Leverandørstyring og utgangsforberedelser

I denne fasen bør virksomheten profesjonalisere leverandørstyringen med særlig vekt på leverandørenes evne og plikt til å støtte en eventuell utfasing. Exit beredskap bør behandles som en del av ordinær kontrakts- og leverandøroppfølging, ikke som et tema som først aktualiseres når virksomheten har besluttet å flytte.

Dette innebærer at virksomheten må ha oversikt over kontraktsmessige rettigheter, tekniske avhengigheter, uttakskostnader, dokumentasjonskrav og leverandørens ansvar ved overgang til ny løsning. Slik kunnskap gir bedre kontroll og reduserer risikoen for uforutsette hindringer, dersom en utfasing blir aktuell.

Kontraktsmessig modning: Virksomheten bør starte arbeidet med å revidere eksisterende avtaler for å sikre tydeligere krav til bistand ved utfasing, datauttrekk, dokumentasjon, overgangsstøtte og håndtering av egress-kostnader. Kontraktene bør også tydeliggjøre hvilke formater, tidsfrister, sikkerhetskrav og støtteforpliktelser som gjelder, dersom data eller tjenester skal flyttes. Dette gir større forutsigbarhet og reduserer risikoen for at virksomheten møter kommersielle eller juridiske barrierer sent i prosessen.

Alternativkartlegging: Virksomheten må holde oversikt over konkrete alternative mottakere av tjenester og data. Dette kan omfatte norske datasentre, private skyløsninger, sektorvise fellesløsninger eller andre offentlige skyleverandører. Formålet er ikke å velge en ny leverandør på forhånd, men å forstå markedets kapasitet, modenhet, sikkerhetsnivå og evne til å overta relevante volumer. Slik kartlegging gjør fremtidige beslutninger mer realistiske og mindre preget av tidspress.

4.1.1.4 Organisasjonsutvikling og brobyggerkompetanse

Endringskapasitet forutsetter at organisasjonen har kompetanse som kan bygge bro mellom dagens skymodell og mulige alternative driftsformer. Dersom virksomheten kun utvikler kompetanse knyttet til én leverandørs plattform, blir risikoen stor for at både tekniske beslutninger og fremtidige handlingsalternativer blir styrt av leverandørens premisser.

Virksomheten bør derfor utvikle en bredere kompetanseprofil, som omfatter offentlig sky, privat sky, lokal infrastruktur, sikkerhetsarkitektur, dataforvaltning, automatisering og leverandørstyring. Dette gjør organisasjonen bedre i stand til å vurdere alternativer, planlegge overgangsløp og gjennomføre tekniske endringer uten å miste styring.

Krystrening: Personell som i dag hovedsakelig arbeider med offentlig sky, bør trenes i arkitekturprinsipper for lokal infrastruktur, privat sky og hybrid drift. Tilsvarende bør personell med erfaring fra tradisjonell infrastruktur få innsikt i moderne skyarkitektur, automatisering og skaleringsprinsipper. Målet er å utvikle en organisasjon som forstår flere driftsmodeller og kan vurdere dem opp mot virksomhetens behov, risiko og strategiske mål.

Prosess-standardisering: Virksomheten bør utvikle standardiserte rutiner for provisjonering, utrulling, overvåking og endringshåndtering som kan fungere på tvers av ulike driftsmiljøer. Bruk av prinsipper som «Infrastructure as Code», automatiserte utrullingsløp og standardiserte konfigurasjoner kan bidra til at tjenester lettere kan flyttes eller gjenopprettes i alternative miljøer. Standardisering bør derfor sees på som et strategisk virkemiddel for fleksibilitet, ikke bare som et effektiviseringstiltak.

4.1.2 Tekniske valg

Scenarioet 'middels lang tid for endring' gir noe rom for tilrettelegging av tekniske løsninger og standarder for å understøtte skytjenesteportabilitet.

For å sikre portabilitet bør virksomheten aktivt tilrettelegge for å:

- Unngå unødvendig bruk av proprietære skylåste tjenester der det finnes portable alternativer som er basert på åpen kildekode
- Standardisere på åpne formater og dokumenterte grensesnitt
- Bruke infrastruktur- og konfigurasjonsbeskrivelser som kan gjenbrukes på tvers av plattformer
- Sikre at identitets- og tilgangsförvaltning ikke er ensidig bundet til én skyplattform
- Etablere løsninger for logging, nøkkelhåndtering, backup og overvåking som kan flyttes eller gjenskapes

4.1.2.1 Teknisk tilrettelegging for skytjenesteportabilitet

IaaS

Overordnet anbefaling for IaaS-området er å redusere konsentrasjonsrisiko ved å legge til rette for hybrid- eller multisky, hvor driften av løsningene vil være taktisk separert i Norge/Skandinavia/Europa.

Følgende tilnærminger kan understøtte dette:

- **Hybridtilkobling:** Etablere sikre forbindelser (f.eks. VPN/IPsec) mellom nåværende sky og alternative lokasjoner i Norge/Europa.
- **Uavhengige støttetjenester:** Etablere løsninger for backup, logging og overvåking som er flyttbare eller kan gjenskapes uavhengig av plattformen.

- **Standardisert objektlagring:** Benytte lagringsløsninger som støtter åpne API-standarder for å forenkle synkronisering av data mellom ulike leverandører.
- **Uavhengig loggaggregasjon:** Sørge for at logger sendes til en nøytral lokasjon (i Norge/Europa) i sanntid, slik at historiske data er tilgjengelige selv om primærskyen blir utilgjengelig.
- **Båndbreddeanalyse:** Kartlegge faktiske overføringstider og eventuelle kostnader ("egress fees") for kritiske datasett, for å sikre at en flytting er praktisk gjennomførbar innenfor tidskravet.
- **Kontinuerlig datasynkronisering:** Etablere løpende asynkron replikering av store datasett til en uavhengig lokasjon i Norge/Europa, for å nøytralisere "data-tyngdekraft" ved behov for flytting. Innføre hyppig integritetsvalidering av de replikerte dataene, for å verifisere at måldataene faktisk er lesbare uten opprinnelig applikasjonslogikk.
- **Latencytesting:** Gjennomføre målinger av forsinkelse mellom nåværende sky og potensielle mottaksmiljøer, for å vite hvilke applikasjoner som tåler splittet drift.

PaaS

Overordnet anbefaling for PaaS-området er å redusere konsentrasjonsrisiko, ved å implementere eller legge til rette for hybrid- eller multisky der minst ett ben er i Norge/Skandinavia/Europa.

Følgende tilnærminger kan understøtte dette:

- **Abstraksjonslag for databaser:** Identifisere og planlegge utfasing av proprietære funksjoner til fordel for portable alternativer som støtter standardisert SQL (ISO/IEC 9075). Dette for å redusere terskelen for migrering mellom ulike databaseplattformer
- **Logghåndtering:** Sentralisere logging via åpne protokoller som Syslog eller standardiserte telemetrimformater, for å bevare sporbarhet på tvers av plattformer.
- **Gjenbrukbar konfigurasjon:** Bruke konfigurasjonsbeskrivelser som kan tolkes og gjenbrukes på tvers av ulike skyplattformer.
- **Standardisert telemetri:** Implementere overvåking basert på OpenTelemetry. Dette sikrer at logger, metrikker og sporingsdata (traces) kan sendes til et nytt miljø uten at applikasjonskoden må skrives om.
- **"Dry-run" av Infrastructure as Code (IaC):** Kjøre regelmessige tester der IaC-skript rulles ut i et tomt testmiljø hos en annen leverandør, for å avdekke skjulte tekniske avhengigheter. KI kan gi effektivt bistand til å tilpasse IaC til ulike leverandører.
- **Validering av API-bakoverkompatibilitet:** Ved versjonsoppdateringer av plattformen, kreve teknisk dokumentasjon som eksplisitt spesifiserer endringer i

API-grensesnitt, for å sikre at automatiserte integrasjoner forblir funksjonelle i en migreringsfase.

SaaS

Overordnet anbefaling for SaaS-området er å redusere konsentrasjonsrisiko ved å legge til rette for reserveløsning i Norge/Skandinavia/Europa. Anbefalingene tar ikke stilling til kontorstøtte-relatert SaaS.

Følgende tilnærminger kan understøtte dette:

- **Teknisk reserveløsning:** Legge til rette for reserveløsninger for kritiske tjenester i Norge eller Europa, for å redusere risiko.
- **Eksportrutiner:** Etablere automatiserte rutiner for periodisk eksport av virksomhetsdata, til en uavhengig lagringslokasjon i Norge eller Europa.
- **Eksport- og integrasjonstesting:** Gjennomføre faktiske tester av dataportabilitet, og bruke SCIM (System for Cross-domain Identity Management) for synkronisering av identiteter for å sikre at virksomheten faktisk kan flytte.
- **Inkrementell dataeksport:** Etablere tekniske rutiner for løpende eksport av endringer i datasett (Change Data Capture - CDC), fremfor å basere seg på tunge full-eksporter som kan feile ved båndbreddebegrensninger.
- **SLA for eksportgrensesnitt:** Spesifisere tekniske krav til oppetid og ytelse (SLA) som gjelder spesifikt for leverandørens grensesnitt for datauttrekk, slik at virksomheten er garantert stabil tilgang til egne data også ved avvikling.

4.2 Lang tid for endring

Med typisk 3–10 år mellom leverandøranskaffelser er tidsbildet for offentlige skytjenester langsiktig. Virksomheten må ha en strategi for fremtidig leverandørskifte, selv om den operative situasjonen er stabil. På teknisk side kan teknologilandskapet endre seg betydelig i tidsrommet, noe som gjør at det ikke er hensiktsmessig å foreta detaljerte tekniske valg for portering av tjenester og data. Likevel må plattformtjenester og infrastruktursystemer forbli fleksible nok til å muliggjøre konkurranse mellom flere leverandører når en anskaffelse skal gjennomføres i fremtiden.

I dette scenarioet inntreffer ingen uforutsette hendelser: daglig drift er stabil, leverandøren oppfyller avtalte SSA-er (SLA), og regulatoriske rammer endres ikke på en måte som påvirker løsningen. Den strategiske styringen må fokusere på å bevare valgfrihet og reell konkurranse ved neste planlagte anskaffelse. Kontraktene og tilhørende tiltak er utelukkende rettet mot denne kommende konkurransen: sikring av endringsevne, dokumentert dataportabilitet og rett til overgangsbistand, samtidig som markedet overvåkes og kravsettet modnes — uten å aktivere opsjoner eller beredskapsmekanismer før selve anskaffelsen.

4.2.1 Strategisk tilnærming

Over tid bør målet med virksomhetens skystrategi være å redusere risikoen for uønsket leverandørbinding, og å sikre reell råderett over egne data, tjenester og teknologiske veivalg i markedet. Siden offentlige skytjenester normalt anskaffes og forvaltes over lange tidshorisonter, må virksomheten ha en strategisk tilnærming som ikke bare ivaretar dagens operative behov, men også bevarer fremtidig handlingsrom.

En langsiktig strategisk tilnærming innebærer at virksomheten bygger en arkitektur, en kontraktsportefølje og en organisasjon som ikke blir unødig avhengig av én leverandør eller ett bestemt teknologisk økosystem. Formålet er ikke nødvendigvis å legge til rette for hyppige leverandørskifter, men å sikre at et fremtidig skifte er praktisk, teknisk, økonomisk og juridisk mulig dersom virksomhetens behov, markedet eller rammebetingelsene endrer seg. **Dette forutsetter at flyttbarhet og portabilitet behandles som strategiske styringshensyn, ikke som rene tekniske detaljer.**

Virksomheten bør derfor bruke sitt handlingsrom aktivt i dialog med markedet, både gjennom kravstilling, kontraktsforhandlinger, arkitekturvalg og løpende modernisering.

Følgende strategiske prinsipper bør ligge til grunn for det langsiktige arbeidet:

4.2.1.1 Kommersielt handlingsrom og kontraktsforhandlinger

Virksomheten bør utvikle og vedlikeholde en reell evne til utfasing som strategisk virkemiddel i møte med skyleverandører. Dette innebærer at virksomheten må kunne dokumentere hvordan data, tjenester og sentrale avhengigheter kan overføres eller avvikles ved behov. En slik evne gir ikke bare operativ trygghet, men styrker også virksomhetens posisjon i kommersielle prosesser.

Forhandlingsmakt: Ved å ha troverdige exit-planer, oversikt over avhengigheter og en teknisk arkitektur som tillater flytting, stiller virksomheten vesentlig sterkere i kontraktsforhandlinger. Dette gjelder både ved reforhandling av eksisterende avtaler og ved nye anskaffelser. Når leverandøren vet at virksomheten har et reelt alternativ, økes virksomhetens mulighet til å påvirke pris, tjenestenivå, sikkerhetskrav, personvernkrav og vilkår for videreutvikling.

Strategisk innkjøp: Virksomheten bør bruke kontraktsrevisjoner og nye anskaffelser til å sikre bedre vilkår for datauttrekk, portabilitet, dokumentasjon og støtte ved eventuell migrasjon. Dette bør inngå som en fast del av anskaffelsesstrategien, ikke som et tilleggskrav sent i prosessen. Avtalevilkår som i praksis binder virksomheten til én løsning gjennom proprietære formater, høye uttakskostnader, manglende overgangsstøtte eller begrenset tilgang til dokumentasjon, må ikke aksepteres.

4.2.1.2 Kontinuerlig modernisering og teknisk gjeld

Langsiktig strategisk handlefrihet krever at virksomheten arbeider aktivt med å identifisere og redusere teknisk gjeld som kan begrense fremtidig fleksibilitet. Over tid kan systemer, integrasjoner og plattformvalg utvikle seg til bindinger som gjør det svært

krevende å endre leverandør, modernisere tjenester eller gjennomføre nye anskaffelser med reell konkurranse.

Utskifting av arv: Eldre systemer som er tett sammenvevd med spesifikk infrastruktur, leverandørspesifikke tjenester eller proprietære integrasjoner, bør vurderes særskilt i virksomhetens langsiktige moderniseringsplaner. Der slike systemer utgjør en barriere for fremtidig fleksibilitet, bør de moderniseres, isoleres eller fases ut til fordel for mer standardiserte og flyttbare løsninger. Dette bør skje som del av ordinær porteføljestyling, ikke først når en migrasjon blir nødvendig.

Innebygd flyttbarhet: Nye systemer bør vurderes ut fra hvor godt de understøtter portabilitet, åpne grensesnitt, dokumentert dataflyt og mulighet for fremtidig leverandørskifte. Skybasert utvikling bør ikke forstås som en ensidig tilpasning til én leverandørs økosystem. Å være «Cloud native» må innebære at løsningene er moderne, skalerbare og automatiserbare uten å skape unødvendig avhengighet til proprietære tjenester eller formater.

4.2.1.3 Kompetanse som strategisk aktivum

For å unngå å bli priggitt leverandørenes premisser, bør virksomheten eie den overordnede systemforståelsen selv. Leverandører kan levere teknologi, drift og spesialistkompetanse, men virksomheten må selv ha tilstrekkelig innsikt til å forstå egne avhengigheter, stille presise krav og vurdere konsekvensene av tekniske og kommersielle valg.

Bestillerkompetanse: Virksomheten bør ha tilstrekkelig intern kompetanse til å forstå hvordan egne tjenester er bygget opp, hvilke data som behandles, hvilke integrasjoner som er kritiske, og hvilke avhengigheter som finnes mot leverandørens plattform. Dette er nødvendig for å kunne styre anskaffelser, kontraktsoppfølging, migrasjonsvurderinger og sikkerhetsmessige avklaringer, uten å være fullt ut avhengig av leverandørens egne konsulenter eller andre korttidsansatte.

Arkitekturkontroll: Kontrollen over den logiske arkitekturen bør ligge hos virksomheten, selv om selve driften eller deler av utviklingen settes ut. Virksomheten bør selv eie målarkitekturen, prinsippene for integrasjon, kravene til dataflyt og vurderingene av hvilke avhengigheter som er akseptable. Dette gir bedre grunnlag for å styre leverandører, redusere risiko for innlåsing, og sikre at teknologiske valg understøtter virksomhetens langsiktige behov.

4.2.2 Tekniske valg

Scenarioet med lang tid for endring gir godt rom for teknisk tilrettelegging og kontraktstilpasninger, for å understøtte skytjenesteportabilitet.

For å sikre portabilitet bør virksomheten aktivt tilrettelegge for å:

- Unngå unødvendig bruk av proprietære skylåste tjenester, der det finnes portable alternativer som er basert på åpen kildekode

- Standardisere på åpne formater og dokumenterte grensesnitt
- Bruke infrastruktur- og konfigurasjonsbeskrivelser som kan gjenbrukes på tvers av plattformer
- Sikre at identitets- og tilgangsforvaltning ikke er ensidig bundet til én skyplattform
- Etablere løsninger for logging, nøkkelhåndtering, backup og overvåking som kan flyttes eller gjenskapes

4.2.2.1 Teknisk tilrettelegging for skytjenesteportabilitet

IaaS

Overordnet anbefaling for IaaS-området er å redusere konsentrasjonsrisiko ved å legge til rette for hybrid- eller multisky, hvor driften av løsningene vil være taktisk separert i Norge/Skandinavia/Europa.

Følgende tilnærminger kan understøtte dette:

- **Deklarativ infrastruktur:** All infrastruktur må defineres som kode (IaC) i plattformnøytrale formater, slik at miljøet kan gjenskapes uavhengig av leverandørens egne verktøy. Med plattformnøytrale formater menes åpne spesifikasjoner (f.eks. deklarativer YAML/JSON-strukturer som tolkes av uavhengige motorer). Dette sikrer at man unngår avhengighet av leverandørspesifikke utrullingsskript. Ved å anvende KI kan deklarativer infrastrukturdefinisjoner analyseres, normaliseres og konverteres til ekvivalente implementasjoner på tvers av ulike skyplattformer, noe som forenkler migrasjon og styrker interoperabilitet.
- **Standardisert virtualisering:** Basere arkitekturen på åpne hypervisor-standarder og formater, som muliggjør flytting av virtuelle maskiner mellom ulike datasentre.
- **Hybrid- og multiskyberedskap:** Implementere eller legge til rette for løsninger der minst ett teknisk "ben" er plassert i Norge eller Europa for å redusere konsentrasjonsrisiko.
- **Nøytral nettverksarkitektur:** Benytte standardiserte rutingprotokoller og IPv6 for å unngå avhengighet av leverandørspesifikke nettverksfunksjoner.
- **Plattformnøytral hemmelighets- og nøkkelstyring (Secrets & Key Management):** Bruke en leverandøruavhengig hvelvtjeneste. Denne må omfatte kryptografiske nøkler (f.eks. BYOK), applikasjonshemmeligheter (passord, API-tokens, secrets) og sertifikater, slik at tillitskjeder og tilgangsmekanismer kan porteres uavhengig av skyplattform.
- **Automatisert sertifikatbehandling:** Bruke ACME-protokollen for automatisert utstedelse og fornyelse av sikkerhetssertifikater, slik at man unngår avhengighet av leverandørspesifikke sertifikatautoriteter.

- **Nettverksidentitet - Bring Your Own IP (BYOIP):** Stille tekniske krav om støtte for å annonsere egne IP-adresseområder via BGP (Border Gateway Protocol), slik at man kan flytte infrastruktur uten å rekonfigurere eksterne endepunkter.
- **Leverandøruavhengig SDN-kontroll:** Bruke programvaredefinerte nettverk (SDN) som styres via åpne protokoller, slik at nettverkssegmentering og sikkerhetsregler kan speiles direkte til en ny leverandør.
- **Krav til selvbetjente "exit-verktøy":** Stille tekniske krav om at leverandøren skal tilby dokumenterte, selvbetjente mekanismer (f.eks. API-er eller CLI-verktøy) for fullstendig eksport av virtuelle maskiner og lagringsvolumer, uten behov for manuell bistand fra leverandøren.
- **Maskinlesbar ressurstaksonomi (tagging):** Implementere et teknisk krav om at alle ressurser skal støtte metadatatagging som identifiserer systemtilhørighet, slik at automatiserte migreringsverktøy kan identifisere og flytte komplette tjenestekjeder som en enhet.

PaaS

Overordnet anbefaling for PaaS-området er å redusere konsentrasjonsrisiko ved å legge til rette for hybrid- eller multisky, hvor driften av løsningene vil være taktisk separert i Norge/Skandinavia/Europa.

Følgende tilnærminger kan understøtte dette:

- **Container-standardisering:** Applikasjoner bør pakkes i enheter basert på OCI (Open Container Initiative)-standards for å frikoble programvaren fra den underliggende skyplattformen.
- **Standardisert meldingsutveksling:** Bruke åpne protokoller som AMQP eller MQTT for kommunikasjon mellom komponenter, for å unngå proprietær låsing.
- **Plattformuavhengig identitet:** Implementere autentisering via OIDC (OpenID Connect) og SAML 2.0, for å frikoble brukertilganger fra leverandørens katalogtjeneste og sikre at identitetsforvaltning ikke er ensidig bundet til én leverandør.
- **Plattformuavhengig API-gateway:** Unngå dyp integrasjon med leverandørspesifikke API-gateways. Benytte løsninger som kan kjøres i containere og støtter OpenAPI-spesifikasjoner, for å sikre at trafikkstyring, autentisering og "rate limiting" er flyttbare. Selve konfigurasjonen (rutingregler, sikkerhetspolicyer) må lagres i et standardisert format (f.eks. som deklarativer policyer), slik at hele integrasjonsmønsteret kan flyttes uten manuell rekonfigurering.
- **Service Mesh for intern kommunikasjon:** Vurdere bruk av et "Service Mesh" basert på åpne standarder for å håndtere tjenesteopptagelse ("service discovery") og kryptering mellom komponenter, slik at tjenester kan finne hverandre uavhengig av hvilket nettverk de befinner seg i.

- **Standardisert ressurstagging:** Innføre en streng teknisk taksonomi for tagging av ressurser, slik at automatiserte verktøy kan identifisere hvilke komponenter som hører sammen og må flyttes som en enhet.
- **Standardisert Telemetri og Tracing:** All applikasjonsovervåking, logging og sporing bør instrumenteres ved bruk av åpne telemetristandarder (OpenTelemetry). Dette sikrer at applikasjonskoden er portabel, slik at man kan flytte tjenesten til et nytt mottaksmiljø uten å måtte skrive om koden for å tilpasse den til en ny leverandørs overvåkingsverktøy.
- **Tjenester basert på åpen kildekode:** Ved å velge PaaS-tjenester som er basert på åpen kildekode som tilbys på tvers av flere leverandører, forenkles både migrering og multisky. Vanlige eksempler på dette er PostgreSQL for database og Kubernetes og CNCF-økosystemet for container-plattform.
- **Åpne modeller og standardiserte grensesnitt for KI:** Der det er mulig bør man benytte store språkmodeller (LLM) som er åpne og kan tilgjengeliggjøres på tvers av ulike leverandører. Standardiserte eller de-facto grensesnitt for språkmodeller via API bør benyttes. I en ideell situasjon tilgjengeliggjøres APIer for språkmodeller bak en felles KI-gateway, slik at man kan endre leverandører uten å endre alle konsumenter. De samme grunnleggende prinsippene relatert til åpen kildekode og standardiserte grensesnitt gjelder med andre ord også for KI.

SaaS

Overordnet anbefaling for SaaS-området er å redusere konsentrasjonsrisiko ved å legge til rette for reserveløsning i Norge/Skandinavia/Europa. Anbefalingene tar ikke stilling til kontorstøtterelatert SaaS.

Følgende tilnærminger kan understøtte dette:

- **Strukturerte dataformater og eierskap:** Sikre teknisk rett og evne til å hente ut data i åpne, maskinlesbare formater som JSON, XML eller CSV. Kreve at data lagres og kan eksporteres i åpne formater.
- **Standardiserte grensesnitt:** Prioritere tjenester med integrasjoner via RESTful API med OpenAPI-dokumentasjon, for å forenkle fremtidige bytter.
- **Teknisk dokumentasjon i åpne formater:** Spesifisere at all systemarkitektur, databaseskjemaer og API-dokumentasjon skal leveres og oppdateres i åpne, redigerbare formater (som Markdown eller HTML), slik at teknisk innsikt er portabel ved leverandørbytte.
- **Standardisert brukerprovisjonering:** Ved anskaffelse av SaaS-tjenester bør det kreves støtte for identitetsstyring basert på åpne standarder for brukersynkronisering (eks. SCIM). Dette sikrer at virksomheten automatisk kan trekke tilbake eller flytte tilganger for samtlige brukere simultant, i stedet for å måtte håndtere identiteter manuelt i leverandørens lukkede portal.

5 Exitkostnader

Dersom målet er å redusere offentlig sektors avhengighet av etablerte globale teknologileverandører må vurderingen sees som noe større enn et rent spørsmål om teknologibytte. En exit fra slike leverandører handler ikke bare om å avslutte en kontrakt eller flytte data fra én plattform til en annen. Det handler om å endre digitale økosystemer, arbeidsprosesser, kompetanse, styring, sikkerhet, anskaffelser og organisatoriske rammer.

Dette kapittelet presenterer en konseptuell modell for exit-vurdering. Modellen synliggjør hvordan dagens leverandøravhengighet må vurderes opp mot exit-kostnader, eksterne kostnads- og risikodrivere, virksomhetens gjennomføringsevne og mulige exit-gevinster. Formålet er ikke å etablere en mekanisk beregningsmodell, men å gi et strukturert beslutningsgrunnlag.

En slik tilnærming er nødvendig fordi både det å bli værende og det å gå ut innebærer kostnader og risiko. Dagens løsninger kan fremstå som stabile og effektive, men kan samtidig innebære innlåsing, økende lisenskostnader, redusert forhandlingsmakt, jurisdiksjonsutfordringer og avhengighet av eksterne kommersielle beslutninger.

En exit kan på sin side gi økt kontroll, bedre konkurranse og større digital handlefrihet, men også høye overgangskostnader, produktivitetstap, økt kompleksitet og gjennomføringsrisiko.

Exit-strategien bør derfor ikke bare bygge på spørsmålet: Hva koster det å forlate dagens leverandør? Den bør også stille spørsmålet: Hva koster det å bli værende dersom avhengigheten, regelverkskravene, sikkerhetsrisikoen og markedsmakten øker over tid?

5.1 Konseptuell modell for exit-vurdering

Den konseptuelle modellen består av seks hovedkomponenter:

- 1) Dagens leverandøravhengighet
- 2) Exit-kostnader
- 3) Eksterne kostnads- og risikodrivere
- 4) Exit-gevinster
- 5) Gjennomføringsevne
- 6) Beslutningsalternativer

Modellen viser at exit ikke bør behandles som et isolert IT-prosjekt. Den bør behandles som en strategisk styringsbeslutning der økonomi, teknologi, sikkerhet, regelverk, organisasjon og samfunnsoppdrag må sees i sammenheng.

En forenklet vurderingslogikk kan uttrykkes slik:

overgangsrisiko ((1) + (2))

+/- Eksterne kostnads- og risikodrivere (3)

– langsiktige exit-gevinster (4)

+/- virksomhetens gjennomføringsevne (5)

= samlet exit-vurdering.

Dette er ikke ment som en presis økonomisk formel. Poenget er å synliggjøre at beslutningen må bygge på en samlet vurdering av både kostnader, risikoer, gevinster og gjennomføringsevne.

5.2 Dagens leverandøravhengighet

Før virksomheten kan vurdere en exit, må den forstå dagens avhengighet. Leverandøravhengighet handler ikke bare om hvilke produkter eller lisenser virksomheten kjøper. Den handler også om hvordan systemer, data, arbeidsprosesser, brukere, sikkerhetsmekanismer og samarbeidsformer er bygget opp rundt bestemte plattformer.

Mange offentlige virksomheter har over tid bygget opp et komplekst digitalt miljø. Ulike systemer, applikasjoner og arbeidsprosesser er koblet sammen gjennom felles identitetsløsninger, e-post, kalender, dokumentlagring, samhandlingsverktøy, sikkerhetsløsninger, analyseverktøy, skylagring og automatiseringer. Slike avhengigheter kan være formelle og dokumenterte, men de kan også være uformelle og utviklet gjennom praktisk bruk over tid.

Avhengigheten kan deles inn i fire hovedtyper:

Teknisk avhengighet oppstår når data, integrasjoner, identitetsløsninger, sikkerhetsoppsett, dokumentflyt, API-er, automatiseringer, fagsystemer og samhandlingsverktøy er tett koblet til én leverandørs økosystem. Jo flere slike koblinger som finnes, desto mer krevende blir det å bytte plattform.

Økonomisk avhengighet kan oppstå gjennom lisensmodeller, volumrabatter, bindingstid, rammeavtaler, pakkeløsninger og rabatter som forutsetter samlet bruk av flere tjenester. Slike modeller kan gjøre det økonomisk krevende å redusere bruken av én del av økosystemet, uten samtidig å påvirke kostnaden for andre deler.

Juridisk avhengighet kan være knyttet til kontrakter, databehandleravtaler, underleverandører, jurisdiksjon, revisjonsrettigheter, ansvarsforhold og krav til etterlevelse. Dersom virksomheten ikke har tilstrekkelig innsyn eller kontroll, kan den få utfordringer med å dokumentere at løsningen oppfyller offentlige krav til personvern, sikkerhet og forsvarlig forvaltning.

Organisatorisk avhengighet oppstår når ansatte, ledere, IT-personell og støttefunksjoner har bygget arbeidsvaner, kompetanse, rutiner og interne prosesser rundt bestemte verktøy. Selv om det finnes tekniske alternativer, kan organisatorisk avhengighet gjøre overgangen krevende, fordi nye løsninger krever endret atferd og ny kompetanse.

Jo sterkere avhengigheten er, desto høyere vil som regel exit-kostnadene være. Samtidig kan sterk avhengighet også bety at gevinsten ved å redusere avhengigheten er større. Modellen må derfor fange opp begge sider: høy avhengighet kan både gjøre exit dyrere og gjøre exit mer strategisk relevant.

5.3 Exit-kostnader

Når dagens avhengighet er kartlagt, må virksomheten vurdere hvilke kostnader en reduksjon eller utfasing av leverandøravhengigheten vil utløse. Disse kostnadene bør behandles samlet som exit-kostnader. Begrepet omfatter ikke bare selve avslutningen av én leverandørrelasjon, men hele omstillingen fra etablerte digitale økosystemer til alternative løsninger, driftsmodeller, kompetansemiljøer og arbeidsprosesser.

For offentlig sektor er dette særlig viktig, fordi digitale løsninger ikke bare er administrative støtteverktøy. De er tett integrert i saksbehandling, kommunikasjon, dokumentforvaltning, sikkerhet, beredskap, innbyggerdialog, samhandling mellom forvaltningsnivåer og daglig produksjon av offentlige tjenester. En overgang bort fra de dominerende plattformene må derfor forstås som en større organisatorisk og teknologisk endring, ikke som et isolert IT-prosjekt.

Exit-kostnader vil variere mellom virksomheter, sektorer og tjenesteområder. En kommune, et helseforetak, en etat, en skoleeier og et departement vil ha ulike behov, krav og risikoprofiler. Likevel finnes det noen hovedkategorier av kostnader som bør inngå i enhver vurdering.

5.3.1 Kartlegging og planlegging

Før en overgang kan gjennomføres, må virksomheten få en grundig oversikt over hvilke tjenester, data, integrasjoner, lisenser, brukerkontoer, sikkerhetsoppsett, kontrakter, arbeidsprosesser og avhengigheter som er knyttet til dagens leverandører.

Kartleggingen må omfatte både tekniske, organisatoriske og juridiske forhold.

Det må blant annet avklares hvilke data som behandles hvor, hvilke systemer som er kritiske for drift, hvilke brukere som er avhengige av hvilke funksjoner, hvilke integrasjoner som finnes mot interne og eksterne systemer, og hvilke kontraktsmessige forpliktelser som gjelder.

Det må i kartleggingen gjøres en alternativ analyse som gir virksomheten oversikt over tilgjengelige løsninger i markedet. Analysen bør se på alternative leverandører og teknologi med tanke på tidsperioden siden oppstart av tjenestene. Denne analysen er viktig for å vurdere hvilke løsninger som kan erstattes raskt, hvilke som krever lengre overgang, og hvilke som eventuelt bør beholdes inntil videre.

Dette arbeidet krever tid, kompetanse og ofte eksternt bistand. Kostnadene kan knyttes til interne ressurser, konsulenter, juridiske vurderinger, risikoanalyser, tekniske analyser, arkitekturgjennomganger, anskaffelsesforberedelser og utarbeidelse av beslutningsgrunnlag. Uten grundig kartlegging øker risikoen for feilinvesteringer, ufullstendige migreringer, uforutsette driftsproblemer og kostnadsoverskridelser.

5.3.2 Migrering, integrasjon og teknisk tilpasning

Migrering er en av de mest synlige kostnadskategoriene ved en exit-prosess. Data, dokumenter, e-post, kalenderinformasjon, brukerkontoer, arkiver, applikasjoner, tilgangsgrupper, arbeidsflyter og samhandlingsrom må flyttes fra eksisterende løsninger til nye plattformer. Samtidig må virksomheten sikre at data bevarer kvalitet, struktur, metadata, tilgangsstyring, sporbarhet og rettslig verdi etter flytting.

Migrering handler derfor ikke bare om å kopiere data fra ett system til et annet. Det omfatter planlegging, testing, kvalitetssikring, feilretting og ofte tilpasning av datamodeller. I offentlig sektor kan dette være særlig krevende fordi dokumentasjon, arkivkrav, personvern, innsynsrett, sikkerhetskrav og journalføringsplikt kan stille strenge krav til hvordan informasjon håndteres.

Mange offentlige virksomheter har også bygget interne systemer rundt Microsoft-, Google- eller Amazon-plattformer. Dette kan gjelde alt fra enkel dokumentdeling og e-post til avanserte integrasjoner mellom fagsystemer, identitetsforvaltning, sikkerhetslogger, datavarehus, automatiserte arbeidsflyter, møteverktøy, rapportering og saksbehandling.

Ved overgang til nye løsninger kan det derfor bli nødvendig å bygge om integrasjoner, API-koblinger, automatiseringer, tilgangsstyring, sikkerhetsoppsett og tekniske grensesnitt. I noen tilfeller finnes det standardiserte alternativer. I andre tilfeller må det utvikles spesialtilpasninger, eller virksomheten må endre arbeidsprosessene fordi den nye løsningen ikke støtter samme funksjonalitet.

5.3.3 Kompetanse, opplæring og produktivitetstap

En overgang til nye løsninger forutsetter at ansatte, ledere, IT-personell, brukerstøtte, systemeiere og sikkerhetsmiljøer bygger ny kompetanse. Kostnadene omfatter kurs, veiledning, intern opplæring, dokumentasjon, brukerstøtte, superbrukerordninger, lederopplæring og praktisk innføring i nye arbeidsprosesser.

For sluttbrukerne kan overgangen innebære nye grensesnitt, nye måter å dele dokumenter på, nye rutiner for møter, endret bruk av e-post og kalender, nye sikkerhetsrutiner, andre krav til lagring og nye verktøy for samhandling. Selv små endringer kan gi betydelig samlet effekt når de gjelder mange ansatte.

Selv godt planlagte overganger kan føre til midlertidig lavere effektivitet, feil, nedetid, forsinkelser, økt behov for brukerstøtte og større belastning på IT-avdelingen. Slike indirekte kostnader kan være betydelige, men undervurderes ofte fordi de ikke alltid fremkommer som egne budsjettposter.

Produktivitetstapet kan bli særlig merkbart dersom virksomheten går bort fra etablerte og godt integrerte økosystemer der ansatte allerede er vant til arbeidsflyter, dokumentdeling, sikker innlogging, kalender, e-post, lagring, møter og integrerte verktøy. Nye løsninger kan være funksjonelt gode, men likevel gi lavere effektivitet i en overgangsperiode fordi brukerne må endre arbeidsvaner, lære nye grensesnitt og håndtere mer friksjon i samhandling.

I enkelte tilfeller kan produktivitetstapet bli mer langvarig. Dette gjelder særlig dersom den nye løsningen har svakere funksjonalitet, dårligere integrasjon, lavere brukervennlighet eller mindre støtte for etablerte arbeidsprosesser.

5.3.4 Kontrakter, lisenser og anskaffelser

Eksisterende avtaler kan inneholde bindingstid, oppsigelsesfrister, volumforpliktelser, minimumskjøp, rabatter knyttet til samlet bruk eller kostnader ved tidlig avslutning. En

virksomhet som ønsker å redusere eller avslutte bruken av en etablert leverandør, må derfor vurdere hvilke økonomiske forpliktelser som allerede er inngått.

I tillegg kan det oppstå dobbeltkostnader dersom gammel og ny løsning må driftes samtidig. Dette vil ofte være nødvendig i en overgangsperiode for å redusere risiko. Virksomheten kan da måtte betale for eksisterende lisenser, nye lisenser, migreringsverktøy, testmiljøer, konsulentbistand og ekstra support parallelt.

En exit fra etablerte leverandører vil også ofte kreve nye anskaffelser, leverandørvurderinger, markedsdialog, konkurransegrunnlag, kravspesifikasjoner, kontraktsforhandlinger og etablering av nye drifts- og supportavtaler. Offentlig sektor må samtidig ivareta krav til konkurranse, likebehandling, dokumentasjon, sikkerhet, personvern og økonomisk forsvarlighet. På den andre siden utløper anskaffelser og avtaler normalt etter et antall år eller et budsjett er oppbrukt. En videreføring hos samme leverandør uten konkurranse vil kreve et unntak i FOA. En mulig exit-gevinst vil i dette tilfellet kunne være å være forberedt for en Exit.

Dersom målet er å redusere strategisk leverandøravhengighet, må anskaffelsen utformes slik at nye bindinger ikke bare erstatter gamle. Det kan derfor være behov for å stille krav til standarder, dataportabilitet, interoperabilitet, dokumenterte grensesnitt, reversibilitet, sikkerhet, datalagring, innsyn, kontroll og fremtidig exit-mulighet.

5.3.5 Sikkerhet, etterlevelse og beredskap

Nye løsninger må vurderes opp mot krav til informasjonssikkerhet, personvern, datalagring, logging, tilgangsstyring, beredskap, revisjon og etterlevelse av relevant regelverk. For offentlig sektor kan dette omfatte krav etter blant annet personvernregelverk, sikkerhetslovgivning, arkivregelverk, forvaltningsrettslige krav, anskaffelsesregelverk og interne styringssystemer for informasjonssikkerhet.

Dette kan kreve juridiske vurderinger, risikovurderinger, personvernkonsekvensvurderinger, sikkerhetsarkitektur, tekniske kontroller, databehandleravtaler, revisjonsspor, logging, beredskapsplaner og dokumentasjon. Dersom løsningen skal brukes til behandling av sensitive personopplysninger, gradert informasjon eller samfunnskritiske funksjoner, øker kravene ytterligere.

For skytjenester bør en risikovurdering spesielt ta hensyn til avhengighet og tilgjengelighet. Bruk av skytjenester medfører en svakere kontroll over dataene enn tilsvarende egne løsninger, da du utsetter deler av driften. Sikkerheten for virksomheten som benytter skytjenestene er derfor til en viss grad forankret i avtaler i stedet for monitorering av on-prem løsninger. For de mest kritiske tjenestene bør det derfor vurderes i hvilken grad en virksomhet aksepterer slik avhengighet av eksterne tjenesteleverandører.

Det kan også oppstå kostnader knyttet til å etablere et sikkerhetsnivå som tidligere var innebygd i de etablerte leverandørenes økosystemer. Store plattformer tilbyr ofte omfattende sikkerhetsfunksjoner, sentralisert administrasjon, trusseldeteksjon, tilgangsstyring og kontinuerlig oppdatering. Dersom virksomheten går over til mer fragmenterte eller egenstyrte løsninger, må den sikre at tilsvarende sikkerhetsnivå kan etableres og driftes over tid.

Overgangen kan også øke risikoen for datatap, tjenesteavbrudd, sikkerhetshendelser, manglende funksjonalitet, feilkonfigurasjoner og svikt i samhandling. Det kan derfor bli nødvendig med ekstra beredskap, reservekapasitet, testmiljøer, pilotprosjekter, tilbakeføringsplaner og styrket hendelseshåndtering.

5.3.6 Infrastruktur og drift

Ved overgang til egne, nasjonale, åpne eller alternative løsninger kan det oppstå behov for ny infrastruktur, serverkapasitet, lagring, nettverk, overvåking, backup, support, sikkerhetsverktøy og driftsorganisasjon. Dersom dagens løsning i stor grad er levert som en helhetlig skytjeneste, kan mange driftsoppgaver ha vært skjult i leverandørens tjenestemodell.

Ved overgang til nye løsninger uten samme helhetlige tilnærming må virksomheten avklare hvem som skal ha ansvar for drift, vedlikehold, oppdateringer, hendelseshåndtering, kapasitetsstyring og brukerstøtte. Dette kan gi behov for økt intern bemanning eller nye driftsavtaler med alternative leverandører.

For små og mellomstore offentlige virksomheter kan slike krav være krevende å håndtere alene. Det kan derfor være nødvendig med fellesløsninger, interkommunalt samarbeid, statlige plattformer eller sektorvise driftsmodeller.

Infrastruktur- og driftskostnader må vurderes i et livsløpsperspektiv. Det er ikke tilstrekkelig å sammenligne lisensprisen på dagens løsning med anskaffelseskostnaden for en ny løsning. Virksomheten må også beregne kostnader til drift, videreutvikling, sikkerhet, support, oppgraderinger, kompetanse og beredskap over tid.

5.3.7 Organisatorisk omstilling, arbeidsmiljø og medvirkning

Overgangen fra etablerte leverandører til alternative løsninger vil innebære bredere omstillingskostnader for virksomheten. Dette handler ikke bare om teknologi, men også om endrede arbeidsprosesser, nye roller og ansvarsforhold, organisatorisk tilpasning, endret styring, nye rutiner og behov for intern forankring.

Det kan også påløpe arbeidsmiljøkostnader, særlig dersom overgangen skaper usikkerhet, økt arbeidspress, behov for midlertidige dobbeltløp, endrede arbeidsoppgaver eller redusert effektivitet i en overgangsperiode. Slike forhold kan kreve særskilte tiltak for opplæring, oppfølging, bemanning, støtteapparat og ledelsesforankring.

I tillegg kan det oppstå kostnader knyttet til medvirkning og dialog med tillitsvalgte og fagforeninger. Større teknologiske og organisatoriske endringer vil ofte kreve informasjon, drøftinger, risikovurderinger og forankring i tråd med gjeldende regelverk og avtaleverk. Dette kan innebære tidsbruk, møtevirksomhet, dokumentasjon, juridiske vurderinger og eventuelle tilpasninger av gjennomføringsplanen.

For offentlig sektor er legitimitet og forankring særlig viktig. En teknologisk endring som oppleves som påført uten tilstrekkelig involvering, kan møte motstand og gi svakere gevinstrealisering.

5.3.8 Økosystem- og samhandlingskostnader

Ved å gå bort fra store etablerte aktører må virksomheten også vurdere konsekvensene av å forlate eller redusere avhengigheten av deres digitale økosystemer. Mange løsninger er tett koblet til andre tjenester, leverandører, samarbeidspartnere, innbyggere, kunder, offentlige systemer og interne arbeidsprosesser.

Dette kan skape kostnader dersom nye løsninger ikke samhandler like godt med eksisterende systemer eller med eksterne aktører. Det kan oppstå behov for nye integrasjoner, tilpasninger, standarder, rutiner og tekniske grensesnitt for å sikre fortsatt informasjonsflyt og samarbeid.

I tillegg kan overgangen påvirke brukere og samarbeidspartnere som fortsatt benytter de etablerte plattformene. Det kan føre til økt friksjon i samhandling, behov for ekstra opplæring, alternative arbeidsmåter, parallelle løsninger eller særskilte tiltak for å opprettholde effektiv kommunikasjon og datadeling.

Økosystemkostnader er ofte vanskelige å synliggjøre fordi de oppstår i grenseflatene mellom virksomheter. En ny dokumentdelingsløsning kan for eksempel fungere godt internt, men skape utfordringer i samarbeid med andre offentlige aktører, leverandører eller innbyggere som bruker andre verktøy.

5.3.9 Risikobasert tilnærming og parallell drift

En risikobasert tilnærming vil ofte være nødvendig og fornuftig ved overgang bort fra etablerte aktører. Det innebærer at virksomheten vurderer hvilke systemer, data, brukere og arbeidsprosesser som bør flyttes først, hvilke som bør avvente, og hvilke løsninger som eventuelt bør beholdes av hensyn til sikkerhet, drift, økonomi eller samfunnskritiske funksjoner.

Samtidig kan en slik tilnærming føre til at virksomheten i en periode må leve med både gamle og nye løsninger. Det kan innebære parallell drift, doble lisenser, flere integrasjoner, mer komplekst sikkerhetsarbeid, økt behov for brukerstøtte, flere opplæringsløp og større administrativ belastning.

Virksomheten bør unngå å utilsiktet ende opp med en varig eller langvarig hybridmodell. Dette krever realistisk planlegging og kontroll med overgangen til nye tjenester. Alternativt kan virksomheten ende opp med å betale både for det gamle økosystemet og for det nye alternativet på ubestemt tid, med den økte kompleksiteten, risikoen og behovet for koordinering dette innebærer.

Dette betyr ikke at en risikobasert tilnærming er feil. Tvert imot kan den være nødvendig for å redusere operasjonell risiko. Men den må ikke forstås som en garanti for lavere kostnader. I mange tilfeller kan den innebære at exit-kostnadene forskyves, forlenges eller øker, særlig dersom overgangen ikke har tydelige beslutningspunkter, prioriteringer og sluttmaal.

5.4 Eksterne kostnads- og risikodrivere

Etter at exit-kostnadene er vurdert, bør virksomheten analysere eksterne forhold som kan endre kostnads- og risikobildet. Dette er forhold virksomheten i liten grad

kontrollerer selv, men som kan få stor betydning for både dagens løsninger og alternative løsninger.

De viktigste eksterne driverne er regelverksendringer, markedsutvikling, geopolitikk, sikkerhetstrusler, leverandørvilkår, teknologisk utvikling og standardisering. Slike drivere kan påvirke både kostnaden ved å bli værende og kostnaden ved å gjennomføre en exit.

Dette er en viktig del av modellen fordi exit-kostnader ikke er statiske. De kan øke eller reduseres som følge av forhold utenfor virksomheten. På samme måte er dagens løsning heller ikke risikofri eller uforanderlig. Leverandørenes priser, vilkår, tekniske løsninger, underleverandører, databehandlingsmodeller og juridiske rammer kan endre seg over tid.

5.4.1 Regelverksendringer, særlig fra EU

En egen kostnadskategori som bør inngå i vurderingen er kostnader som følger av endringer i regelverk, særlig fra EU (se til dette kapittel 5). Offentlig sektor opererer i et rettslig landskap som er raskt utvikling, og nye krav til personvern, informasjonssikkerhet, kunstig intelligens, dataforvaltning, digital infrastruktur, interoperabilitet, cybersikkerhet og leverandørstyring vil påvirke både eksisterende løsninger og alternative løsninger.

Slike regelverksendringer kan gi kostnader uavhengig av om virksomheten blir værende hos dagens leverandører eller gjennomfører en exit. Dersom nye EU-regler stiller strengere krav til datadeling, dokumentasjon, risikostyring, sikkerhet, hendelsesrapportering, tredjepartsleverandører, kunstig intelligens eller datalagring, kan virksomheten måtte gjøre tekniske, juridiske og organisatoriske tilpasninger. Dette kan innebære nye kontrollrutiner, endrede avtaler, revisjoner, sikkerhetstiltak, dokumentasjon, opplæring og rapportering.

I en exit-sammenheng kan regelverksendringer få særlig stor betydning. Nye regler kan gjøre dagens løsninger dyrere eller mer krevende å bruke dersom eksisterende leverandørmodell ikke lenger vurderes som tilstrekkelig robust, transparent eller forenlig med nye krav. Samtidig kan nye regler påvirke kostnadene ved alternative løsninger, fordi også disse må tilfredsstille gjeldende og kommende krav til sikkerhet, dokumentasjon, revisjon, databehandling og etterlevelse.

Regelverksendringer kan også skape usikkerhet i selve overgangsperioden. Dersom virksomheten planlegger en flerårig exit-strategi, kan kravbildet endre seg underveis. En løsning som fremstår som tilstrekkelig ved prosjektstart, kan kreve ytterligere tilpasninger før full innføring. Dette kan føre til forsinkelser, omarbeiding, ekstra juridiske vurderinger, nye tekniske krav og økte kostnader.

Samtidig kan endringer i regelverk også styrke begrunnelsen for exit. Dersom nye europeiske regler legger større vekt på digital suverenitet, sikkerhet, kontroll, datadeling, interoperabilitet og ansvarlig bruk av teknologi, kan dette gjøre det mer strategisk relevant å redusere avhengigheten av lukkede eller jurisdiksjonsmessig krevende økosystemer. Regelverksendringer er derfor ikke bare en kostnadsdriver. De

kan også være en driver for omstilling og et argument for å bygge mer robuste, åpne og kontrollerbare digitale løsninger.

5.4.2 Marked, geopolitikk og leverandørvilkår

I tillegg til regelverk vil markedsutvikling, geopolitikk og leverandørenes egne kommersielle strategier kunne påvirke både kostnaden ved å bli værende og kostnaden ved å gå ut.

Markedet for digitale plattformer preges av sterke nettverkseffekter, stordriftsfordeler og høy grad av innlåsing. Når mange virksomheter bruker samme plattform, blir det enklere å samarbeide innenfor plattformen, men vanskeligere å bytte ut deler av økosystemet. Dette kan svekke konkurransen over tid og gjøre offentlige virksomheter mer sårbare for prisendringer, produktendringer og endrede avtalevilkår.

Leverandører kan endre lisensmodeller, pakke funksjonalitet på nye måter, fase ut produkter, endre sikkerhetsfunksjoner, justere tilgang til API-er eller flytte funksjonalitet mellom ulike prisnivåer. Slike endringer kan gi økte kostnader eller redusert handlingsrom for offentlige virksomheter, selv uten at virksomheten selv har endret behov.

Geopolitiske forhold kan også påvirke vurderingen. Dersom teknologi, data, skytjenester eller underleverandører er knyttet til andre jurisdiksjoner, kan virksomheten bli eksponert for konflikter mellom regelverk, sanksjoner, eksportkontroll, politiske beslutninger eller endrede sikkerhetsvurderinger. Dette kan være særlig relevant for samfunnskritiske funksjoner, beredskapssektorer og virksomheter som behandler sensitive data.

Disse eksterne driverne viser at en exit-strategi ikke kan være statisk. Den må oppdateres over tid og ta høyde for at både dagens løsninger og alternative løsninger vil utvikle seg.

5.5 Exitgevinster

Selv om dette kapittelet har et tydelig fokus på exit-kostnader, er det viktig å understreke at en exit-strategi også kan gi betydelige gevinster. Når kostnader, eksterne drivere og gjennomføringsevne er vurdert, kan virksomheten analysere mulige exit-gevinster på en mer realistisk måte.

Dersom offentlig sektor reduserer avhengigheten av etablerte globale teknologileverandører, kan det på lengre sikt gi økt strategisk handlefrihet, bedre kontroll over data, sterkere forhandlingsposisjon, større nasjonal og europeisk digital suverenitet og redusert sårbarhet ved geopolitiske, rettslige eller kommersielle endringer.

Exit-gevinster må vurderes som en del av det samlede beslutningsgrunnlaget. Dersom kun kostnadene synliggjøres, kan det skape et skjevt bilde der dagens løsninger fremstår som billigere og mindre risikable enn de faktisk er. Dagens avhengighet har også en kostnad, selv om den ikke alltid fremkommer direkte i budsjettene. Dette kan være kostnader knyttet til innlåsing, svak konkurranse, begrenset forhandlingsmakt, økende

lisenspriser, redusert kontroll over teknologisk utvikling, manglende dataportabilitet og økt eksponering mot eksterne beslutninger utenfor norsk offentlig styring.

En sentral exit-gevinst er redusert leverandøravhengighet. Dersom virksomheten etablerer løsninger basert på åpne standarder, bedre dataportabilitet og mer fleksible arkitekturer, kan den på sikt få større frihet til å bytte leverandør, kombinere ulike løsninger og stille tydeligere krav i fremtidige anskaffelser. Dette kan styrke konkurransen og redusere risikoen for at én leverandør får en dominerende posisjon over tid.

En annen strategisk gevinst er bedre kontroll over data og digital infrastruktur. For offentlig sektor er dette særlig viktig fordi data kan ha stor samfunnsmessig, rettslig og sikkerhetsmessig betydning. Økt kontroll kan gi bedre oversikt over hvor data lagres, hvem som har tilgang, hvilke nasjoner som har jurisdiksjon, hvordan data behandles, hvilke underleverandører som brukes, og hvordan virksomheten kan sikre etterlevelse av nasjonale og europeiske krav.

Exit kan også gi beredskapsmessige gevinster. Dersom offentlige virksomheter blir mindre avhengige av et fåtall globale plattformer, kan det redusere sårbarheten ved tekniske feil, endrede eksportregler, sanksjoner, geopolitiske konflikter, endringer i leverandørvilkår eller rettslige konflikter mellom jurisdiksjoner. Dette kan være særlig relevant for samfunnskritiske funksjoner, beredskapsaktører og sektorer som behandler sensitive eller store mengder personopplysninger.

Det kan også oppstå organisatoriske gevinster. En exit-prosess tvinger virksomheten til å kartlegge systemer, data, arbeidsprosesser, integrasjoner, roller og ansvar. Dette kan avdekke ineffektivitet, overlappende løsninger, utdatert teknologi, svak datakvalitet og mangelfull styring. Selv om kartleggingen i seg selv har en kostnad, kan den gi bedre oversikt og styring av den digitale porteføljen.

Videre kan en exit-strategi bidra til mer innovasjon og utvikling av alternative markeder. Dersom offentlig sektor etterspør løsninger basert på åpne standarder, interoperabilitet og europeiske eller nasjonale driftsmodeller, kan det stimulere til utvikling av nye leverandørmiljøer, mer konkurranse og større teknologisk mangfold.

Exit-gevinster vil likevel ikke oppstå automatisk. De forutsetter tydelige mål, god styring, realistisk gjennomføringsevne og langsiktig finansiering. Dersom overgangen bare innebærer at én lukket leverandør erstattes med en annen, kan gevinsten bli begrenset. Dersom nye løsninger ikke bygger på åpne standarder, dataportabilitet, reell konkurranse og god forvaltningsstyring, kan virksomheten ende opp med ny innlåsing i en annen form.

5.6 Gjennomføringsevne

Før exit-gevinster vurderes fullt ut, bør virksomheten vurdere sin egen gjennomføringsevne. Dette er viktig fordi gevinster ikke realiseres automatisk. De avhenger av om virksomheten faktisk klarer å gjennomføre overgangen på en styrt, sikker og økonomisk forsvarlig måte.

Gjennomføringsevne handler om intern kompetanse, prosjekt- og programstyring, teknisk arkitekturkompetanse, anskaffelseskompetanse, juridisk kapasitet, endringsledelse, brukerstøtte, finansiering, ledelsesforankring og politisk eller administrativ støtte.

For offentlig sektor vil også samarbeid på tvers av virksomheter være viktig. Mange offentlige aktører har like behov, men ulik kapasitet. Dersom hver enkelt virksomhet må utvikle egne exit-strategier, kravspesifikasjoner, tekniske løsninger og driftsmodeller, kan kostnadene bli høye og resultatene fragmenterte. Felles offentlige krav, felles anskaffelser, sektorvise løsninger eller nasjonale støttemiljøer kan derfor styrke gjennomføringsevnen.

Et særskilt forhold er at kostnadene og gevinstene ved exit ikke alltid tilfaller samme nivå eller aktør. Kostnadene vil ofte påløpe den enkelte virksomhet, kommune, etat eller sektor i form av kartlegging, migrering, opplæring, parallell drift, anskaffelser, sikkerhetstiltak og organisatorisk omstilling. Gevinstene kan derimot i stor grad være nasjonale eller sektorovergripende, for eksempel i form av økt digital suverenitet, bedre beredskap, sterkere forhandlingsmakt, mer konkurranse, bedre kontroll over offentlige data og redusert samlet sårbarhet.

Dette skaper en styringsutfordring. Den enkelte virksomhet kan ha svake økonomiske insentiver til å bære betydelige overgangskostnader dersom gevinstene i hovedsak realiseres på samfunns- eller nasjonalt nivå. Mange offentlige virksomheter har i tillegg stramme budsjetter og begrenset kapasitet til å finansiere større teknologiske omstillinger innenfor ordinære driftsrammer.

Dersom reduksjon av leverandøravhengighet vurderes som et nasjonalt mål, bør derfor finansiering, prioritering og koordinering også løftes til nasjonalt nivå. Det kan innebære statlige støtteordninger, felles finansieringsmodeller, nasjonale krav, felles anskaffelser, sektorvise programmer eller etablering av felles offentlige løsninger som gjør det mulig å realisere nasjonale gevinster uten at enkeltvirksomheter alene må bære uforholdsmessige kostnader.

Gjennomføringsevne bør vurderes realistisk. En virksomhet kan ha gode strategiske grunner til å redusere leverandøravhengighet, men likevel mangle kapasitet til å gjøre det raskt. I slike tilfeller kan det være mer forsvarlig å starte med kartlegging, kompetansebygging, åpne standarder, bedre kontraktskrav og selektiv utfasing av mindre kritiske tjenester.

5.7 Beslutningsalternativer

Den konseptuelle modellen bør munne ut i konkrete beslutningsalternativer. Det er viktig fordi exit ikke bare handler om ja eller nei. Offentlig sektor kan velge flere mellomformer, avhengig av risikoprofil, samfunnsoppdrag, datatyper, økonomi, kompetanse og strategiske mål.

Å ikke gjøre noe innebærer at man ikke gjør noen endringer i dagens driftsmodell. Det kan f.eks. være aktuelt dersom exit-kostnadene er høye og at eksisterende leveranser ikke er kritiske, eller vil ha små innvirkninger på driften hvis de blir utilgjengelige.

Videreføring med styrket kontroll innebærer at virksomheten blir værende hos dagens leverandør, men styrker kontraktsoppfølging, sikkerhet, dataklassifisering og exit-forberedelser. Dette kan være aktuelt dersom exit-kostnadene er høye eller dagens løsning vurderes som nødvendig for kritisk drift.

Risikobasert reduksjon av avhengighet innebærer at virksomheten flytter ut enkelte tjenester, data eller brukergrupper der risikoen er lav og gevinsten høy. Dette kan være en god tilnærming dersom full exit er for krevende, men dagens avhengighet likevel vurderes som strategisk uheldig.

Hybridmodell innebærer at virksomheten kombinerer etablerte plattformer med alternative løsninger. Dette kan gi fleksibilitet og redusert risiko, men kan også føre til økt kompleksitet, dobbeltkostnader, flere integrasjoner og mer krevende sikkerhetsstyring. Hybridmodeller bør derfor ha tydelige mål og ikke bare bli et resultat av manglende beslutninger.

Trinnvis exit innebærer at virksomheten gjennomfører en planlagt utfasing over flere år, med tydelige beslutningspunkter, milepæler, risikovurderinger og gevinstmål. Dette gir mulighet for læring, justering og gradvis kompetansebygging, men kan også føre til langvarig parallell drift dersom strategien ikke har tydelige prioriteringer og slutt mål.

Full exit innebærer at virksomheten avslutter bruken av én eller flere etablerte leverandører på definerte områder og etablerer nye løsninger, driftsmodeller og styringsregimer. Dette kan gi stor strategisk gevinst, men vil ofte være det mest krevende alternativet og bør bare gjennomføres der virksomheten har tilstrekkelig oversikt, finansiering, kompetanse, sikkerhetsnivå og organisatorisk gjennomføringsevne. Dette alternativet kan også tvinge seg frem gjennom avtaleutløp/avslutning og påfølgende ny anskaffelse.

Felles offentlig løsning innebærer at flere offentlige virksomheter samarbeider om felles plattformer, åpne standarder, sikkerhetskrav, kompetansemiljøer og leverandør oppfølging. Dette kan redusere kostnader, styrke forhandlingsmakten og bygge offentlig kompetanse, men krever god styring, tydelig ansvarsfordeling og langsiktig finansiering.

5.8 Samlet vurdering

Exit-strategi må forstås som et helhetlig styringsverktøy, ikke som en teknisk migreringsplan. Modellen i dette kapittelet viser at en forsvarlig vurdering må starte med dagens leverandøravhengighet, deretter kartlegge exit-kostnader, vurdere eksterne drivere, analysere gjennomføringsevne, identifisere mulige gevinster og til slutt munne ut i konkrete beslutningsalternativer.

Exit-kostnader oppstår ikke bare i det øyeblikket en kontrakt sies opp eller en teknisk migrering gjennomføres. De oppstår gjennom hele prosessen: i kartlegging, planlegging, anskaffelse, migrering, opplæring, parallell drift, sikkerhetsarbeid, organisasjonsendring, regelverkstilpasning og gevinstrealisering.

For offentlig sektor er det derfor avgjørende at exit-strategier bygger på realistiske kostnadsanslag og ikke på en forenklet antakelse om at alternative løsninger automatisk

vil være billigere. Redusert leverandøravhengighet kan ha stor strategisk verdi, særlig med hensyn til digital suverenitet, beredskap, kontroll, konkurranse og langsiktig handlingsrom. Men denne verdien må veies opp mot faktiske overgangskostnader, regulatorisk usikkerhet, operasjonell risiko og virksomhetens evne til å gjennomføre endringen.

Samtidig må ikke kostnadene alene bli styrende. Dagens avhengighet har også en kostnad, selv om den ofte er mindre synlig. Innlåsing, svak konkurranse, begrenset forhandlingsmakt, økte lisenskostnader, redusert kontroll over data og sårbarhet for eksterne beslutninger kan over tid gi betydelige strategiske ulemper. En helhetlig vurdering må derfor sammenholde exit-kostnader med exit-gevinster.

Et særskilt forhold i offentlig sektor er at kostnadene og gevinstene ved exit ikke alltid tilfaller samme nivå eller aktør. Kostnadene vil ofte påløpe den enkelte virksomhet, kommune, etat eller sektor. Gevinstene kan derimot i stor grad være nasjonale eller sektorovergripende, for eksempel i form av økt digital suverenitet, bedre beredskap, sterkere forhandlingsmakt, mer konkurranse, bedre kontroll over offentlige data og redusert samlet sårbarhet.

Dette skaper en styringsutfordring fordi den enkelte virksomhet kan ha svake økonomiske insentiver til å bære betydelige overgangskostnader dersom gevinstene i hovedsak realiseres på samfunns- eller nasjonalt nivå. Det anbefaler derfor at man foretar en vurdering av hvordan kostnader og gevinster fordeles mellom virksomhetsnivå, sektornivå og nasjonalt nivå.

Mange offentlige virksomheter har i tillegg stramme budsjetter og begrenset kapasitet til å finansiere større teknologiske omstillinger innenfor ordinære driftsrammer. Dersom reduksjon av leverandøravhengighet vurderes som et nasjonalt mål, bør derfor finansiering, prioritering og koordinering løftes til nasjonalt nivå. Det kan innebære statlige støtteordninger, felles finansieringsmodeller, nasjonale krav, felles anskaffelser, sektorvise programmer eller etablering av felles offentlige løsninger.

Det offentlige bør derfor i større grad vurdere å gå sammen om utvikling, anskaffelse og drift av digitale løsninger der behovene er felles på tvers av virksomheter. For mange enkeltvirksomheter vil kostnadene ved å bygge opp nødvendig kompetanse, sikre gode tekniske løsninger og følge opp leverandører være krevende å bære alene. Samtidig vil gevinstene av bedre digitale løsninger ofte være nasjonale, ikke bare lokale. Felles innsats kan derfor gi bedre ressursbruk, sterkere offentlig bestillerkompetanse og mer helhetlig styring. Dette bør særlig vurderes der løsninger bygger på åpne standarder, felles sikkerhetskrav og behov for langsiktig kompetanseutvikling i offentlig sektor.

Det sentrale poenget er at exit-kostnader ikke bør brukes som argument for passivitet, men som grunnlag for bedre beslutninger. Dersom offentlig sektor ønsker å redusere avhengigheten av dominerende teknologileverandører, må dette gjøres planmessig, trinnvis og med full forståelse for de økonomiske, tekniske, juridiske og organisatoriske konsekvensene.

En god exit-strategi bør derfor som minimum inneholde:

1. en samlet oversikt over eksisterende leverandøravhengigheter

2. en vurdering av hvilke tjenester som er mest kritiske
3. en kartlegging av alternative løsninger
4. en realistisk beregning av direkte og indirekte exit-kostnader
5. en vurdering av eksterne kostnads- og risikodrivere, særlig regelverksendringer fra EU
6. en vurdering av mulige exit-gevinster på kort og lang sikt
7. en vurdering av virksomhetens gjennomføringsevne
8. en vurdering av sikkerhet, personvern og etterlevelse
9. en plan for migrering, opplæring og parallell drift
10. tydelige beslutningspunkter for videreføring, justering eller stans
11. en plan for finansiering, gevinstrealisering og langsiktig forvaltning

En exit-strategi uten kostnadsforståelse kan bli urealistisk. En kostnadsforståelse uten strategisk retning kan føre til at dagens avhengighet videreføres. Det offentlige bør derfor kombinere langsiktig mål om større digital handlefrihet med nøkterne vurderinger av hva overgangen faktisk krever, hvilke gevinster som kan realiseres, hvordan kostnader og gevinster fordeles mellom ulike nivåer i offentlig sektor, og hvordan endringer i regelverk, marked, sikkerhet og geopolitikk kan påvirke både kostnader, risiko og muligheter over tid.

6 Juridisk – veiledning til kommende EU-regelverk

6.1 Innledning

Det er for tiden sterk bevegelse i EU på digital suverenitet-området, og dette kan få store konsekvenser for norsk offentlig sektors bruk av skytjenester. Arbeidsgruppen vil særlig trekke frem det nylig presenterte forslaget til en forordning om skytjenester og AI (CADA, punkt 5.1.3, under). Denne har som uttalt mål å begrense avhengighet og lock-in-effekter, og vil innebære at norske offentlige virksomheter blir forpliktet til å risikovurdere alle sine skytjenesteleveranser fra et digitalsuverenitetsperspektiv. Dersom CADA innføres i sin nåværende form må særlig offentlige virksomheter innen forsvar, nasjonal sikkerhet, politi- og rettsvesen, men også helsesektoren og andre sentrale og kritiske offentlige tjenesteleverandører, være forberedt på at det kan komme krav til å flytte noen av sine skydrevne tjenester til heleuropeiske leverandører. Det gjenstår å se hvor omfattende pliktene etter CADA vil bli da forslaget skal inn i trilogforhandlinger, men alle offentlige virksomheter som i betydelig utstrekning benytter seg av skytjenester i sine leveranser bør være forberedt på at arbeidet med etterlevelse kan bli svært omfattende.

6.2 Dataforordningen (Data Act)

Data Act (dataforordningen) er EUs rammeverk for enklere tilgang til og bruk av data. På skrivende tidspunkt er forordningen ikke vedtatt inkorporert i EØS-avtalen. Forordningen er heller ikke gjennomført i norsk rett. Forordningen har et eget kapittel om bytting mellom databehandlingstjenester. Hensikten er både å gi bedre muligheter til å operere på flere forskjellige skyplattformer med forskjellige komponenter (multi-cloud), samt å fasilitere bytting mellom tjenestetilbydere. Som ledd i dette stilles det noen krav til innhold i kontrakter mellom tilbyder og kunde. I tillegg stilles en rekke tekniske krav til mulighet for portering, eksport av data og tvungne standarder for interoperabilitet mellom tjenester. Sistnevnte vil bestemmes ved gjennomføringsrettsakter gitt av kommisjonen. I skrivende stund har det ikke kommet noen slike, men utredningsarbeidet pågår.

Tilbydere er etter forordningen forpliktet til å fjerne hindringer for flytting mellom databehandlingstjenester, samt eventuelle hindre for sambruk av forskjellige tjenester. Artikkel 23 påbyr tjenesteleverandør å fjerne alle former for tiltak som forhindrer kunder fra å avslutte kontrakten etter bytting, inngå nye avtaler med andre leverandører av samme tjenester, portere data til annen leverandør eller lokal infrastruktur, å oppnå funksjonell likeverdighet ved flytting til nye tjenester, samt på visse vilkår å separere (unbundle) tjenestene.

Artikkel 25 påbyr partene å kontraktfeste vilkår for bytting mellom leverandører, og innebærer en operasjonalisering av artikkel 23. Samtidig virker artikkel 23 selvstendig ved siden av artikkel 25, og den er derfor ikke noen uttømmende liste over hvilke kontraktsvilkår som ikke kan aksepteres innenfor rammen av forordningen. Artikkelen inneholder en lang rekke bestemmelser om hvilke vilkår som må være med i alle kontrakter mellom databehandlingstjenestetilbydere og kundene. Vilkårene handler i stor grad om å forhindre ulike former for praksis som er ment eller er egnet til å vanskeliggjøre bytting mellom tjenesteleverandører.

Kravene er i korthet:

- Kundens og leverandørens rettigheter og plikter relatert til bytting mellom tilbydere skal reguleres i en skriftlig avtale.
- Vilkår som eksplisitt tillater kunden å bytte til en annen tjenesteleverandør eller å portere alle eksporterbare data til en on-prem løsning uten ugrunnet opphold og senest i løpet av en 30-dagers overgangsperiode.
- At leverandøren i overgangsperioden må forholde seg lojalt til kundens behov for kontinuitet
- Gi informasjon om kjente problemer og risiko for kontinuitet som skyldes forhold ved leverandørens tjenester
- Påse at det opprettholdes et høyt sikkerhetsnivå ved overføring av data
- Krav om at leverandør må forholde seg lojalt til kundens exit-strategi, blant annet ved å ikke tilbakeholde informasjon som kan være relevant for kunden
- Kontrakten kan ikke stille vilkår om forhåndsvarsling om bytte eller avslutning av avtalen lenger enn 2 måneder

- Leverandøren må tilby en uttømmende liste over hvilke (typer) av kundens data som kan porteres, og hvilke som ikke kan porteres
- Leverandøren må minimum tilby kunden et vindu på 30 dager for å foreta selve dataporteringen
- Leverandøren må garantere at kundens data blir fullstendig slettet etter kontraktens opphør
- En oversikt over hvilke kostnader leverandøren vil kreve i forbindelse med byttingen

Artikkel 26-28 gir noen bestemmelser om informasjonsplikt og lojalitetsplikt.

Leverandør påbys spesifikt å opplyse åpent om hvilken jurisdiksjon de er underlagt, samt å forklare hvilke tiltak som er iverksatt for å hindre tilgang til disse dataene som ville være i strid med EU-retten eller nasjonal rett.

Kostnader som leverandøren kan pålegge kunden å dekke i forbindelse med bytte (såkalt egresskostnad) skal gradvis fases ut ihht. art. 29, og blir forbudt fra 12. Januar 2027.

Artikkel 30 gir mer detaljerte bestemmelser om de tekniske aspektene ved bytting mellom tjenester. Den praktisk viktigste er nr. 3, som bestemmer at leverandører er forpliktet til å følge de standarder for interoperabilitet som kommisjonen bestemmer. For IaaS bestemmer nr. 1 at leverandører i alle tilfeller skal tilrettelegge for at kunden kan oppnå funksjonell ekvivalens hos ny leverandør. Nr. 2 bestemmer at leverandøren er forpliktet til å tilby et grensesnitt (API) til både kunden og kundens nye leverandør, slik at de kan benytte egen programvare til å foreta porteringen.

Art. 31 gir et viktig unntak, og bestemmer at artikkel 23, samt reglene om kostnader ved bytting og om de tekniske aspektene ved bytting, ikke gjelder for tjenester der mesteparten av funksjonaliteten er spesielt utviklet for kunden.

6.2.1 Dataforordningens praktiske betydning

Reglene i Data Act kan komme til å få stor betydning for styrkeforholdet mellom kunde og leverandør på skytjenesteområdet, men det er ennå langt igjen til effekten vil bli merkbar. Dette handler først og fremst om at forordningen stiller få klare, ufravikelige krav til bestemte løsninger som fremmer endringsevne. Bestemmelsene kan stort sett karakteriseres som regler om lojalitetsplikt i kontraktsforholdet: De er altså ikke noe man som kunde kan slå i bordet med. Bestemmelsen som forbyr såkalte «egress»-kostnader er et godt eksempel: Uspesifiserte kostnader som belastes dersom kunden vil ta med seg dataene vekk fra tilbyders plattform blir ikke lenger tillatt, men dette hindrer ingen fra å bake de faktiske kostnadene leverandøren har inn i prisen for selve tjenesten. Kunder kan ikke forvente at leverandøren tilbyr noe mer enn minimumskravene til støtte ved bytte, med mindre noe annet er spesifisert i kontrakten.

Forordningen er full av detaljerte bestemmelser og begreper som garantert vil bli gjenstand for konflikt i rettslige prosesser. Noen endelige avgjørelser fra EU-domstolen om innholdet i forordningen kan man imidlertid ikke vente å se før om 4-5 år.

Slik tilstanden er nå vil Data Act primært ha betydning som en faktor i kontraktsforhandlinger i skyanskaffelser. For det mellomlange og kortsiktige perspektivets del er de viktigste bestemmelsene her at kontrakter med skytjenesteleverandører må tillate at kunden - vilkårsløst - bestemmer seg for å bytte leverandør.⁴ For det langsiktige perspektivet vil resten av de nevnte bestemmelsene ha større betydning, særlig når kommisjonen begynner implementeringen av standardene for interoperabilitet. Den omfattende informasjonsplikten som tillegges leverandørene kan være nyttig for virksomheter i utarbeidelsen av planer for bytte av skytjenesteleverandører eller exit-strategier.

Det er vanskelig å si noe mer konkret på dette stadiet enn at rammeverket i forordningen i alle fall legger opp til at det skal være mulig å inngå kontrakter som ikke fører til innlåsing hos en leverandør. Forordningen beskytter imidlertid ikke virksomheter mot å inngå dårlige kontrakter eller mot dårlig kontraktsforvaltning. Kommisjonen har publisert utkast til standard kontraktsvilkår for skytjenestekontrakter, og det finnes tillegg en del private initiativer, som CISPE, som jobber med avtaleverk og standarder for blant annet bedre interoperabilitet mellom skytjenester.⁵

6.3 Fri flyt av andre opplysninger enn personopplysninger i EU (FFD)

Forordningens artikkel fire punkt 1 og 2 kan ha direkte betydning for endringsevne i bruken av skytjenester. Artikkelen beskrives slik i høringsnotatet om forordningen: «Artikkel 4 introduserer prinsippet om fri flyt av andre opplysninger enn personopplysninger. Nasjonale lover, forskrifter og administrative krav i medlemslandene som begrenser muligheten til å lagre og behandle data utenfor landets grenser blir forbudt, med mindre de kan begrunnes i hensynet til offentlig sikkerhet ("justified on grounds of public security").»

Forordningen skal sammen med EUs personvernforordning (GDPR) skape et helhetlig og sammenhengende rettslig rammeverk som skal sikre fri flyt av alle opplysninger i hele EU/EØS-området. For endringsevne i bruk av skytjenester vil det si at krav til geografisk plassering av datasenter innenfor EØS/EU området bare begrenset grad er lovlig. FFD

⁴ Denne bestemmelsen ser imidlertid ut til å bli tatt ut igjen gjennom omnibus VII. Se til dette punkt 2.3.3, nedenfor.

⁵ Se [Draft Recommendation on non-binding model contractual terms on data access and use and non-binding standard contractual clauses for cloud computing contracts | Shaping Europe's digital future](#). Utkastet vil bli formelt vedtatt når det foreligger oversettelser til alle medlemslandenes språk.

[Portability of Cloud Services | CISPE](#)

gjelder alle typer elektronisk behandling og lagring av data i vid forstand som ikke er personopplysninger.

Lokaliseringskrav som er lovlige må være berettiget av hensyn til offentlig sikkerhet, slik dette hensynet er definert i EU-retten og særlig TFEU artikkel 52. Tilfeller som kan berettigede unntaket er nærmere beskrevet i fortalens avsnitt (19). Unntaket kan begrunnes i trusler mot både indre og ytre sikkerhet, som er tilstrekkelig alvorlige og som truer grunnleggende samfunnsinteresser. Eksempelene gitt indikerer at terskelen skal ligge høyt. begrunnet i offentlig sikkerhet må være egnet for å oppnå formålet og ikke gå lenger enn det som er nødvendig (proporsjonalitet).

Forbudet mot lokaliseringskrav gjelder for statene og i virksomheter som reguleres av offentlig lovverk som anskaffelsesreglementet. Lokaliseringsforbudet er dermed relevant for offentlige myndigheter.

FFD ble besluttet inntatt i EØS-avtalen 22. september 2023, men med forbehold om opphevelse av konstitusjonelle forbehold. Avgjørelsen i EØS-komiteen er ikke tredd i kraft per juni 2026 og forordningen er så langt ikke inkorporert i norsk rett. Det ble avdekket flere regelverk som ikke var i overensstemmelse med lokaliseringskravet ved høringen i Norge. Et av regelverkene er arkivloven § 9 første ledd bokstav b. Selv om ny arkivlov tredde i kraft 1. januar 2026, gjelder fortsatt lokasjonskravene i den gamle arkivloven. Dette er gjort med delt iverksetting i FOR-2025-12-12-2510. Den nye arkivloven har i § 11 gitt departementet forskriftshjemmel for å lage vilkår for lagring av digitale arkiv utenfor Norge, men det er i juni 2026 ikke varslet slik forskrift.

6.4 Digital omnibus VII

I endringspakken «Omnibus VII» er det foreslått store endringer i Dataforordningen. Endringene innebærer at Data Governance Act, Open Data Directive, samt Free Flow of Non Personal Data Directive opphører som egne rettsakter og skal integreres i dataforordningen. For bestemmelsene i Dataforordningens del er de viktigste foreslåtte endringene at det innføres unntak fra reglene for kostnader ved bytte for kontrakter som inngås for en fastsatt tidsperiode (egresskostnader). Det kan i så fall ilegges “early termination penalties”. Det foreslås også å innføre et unntak for de fleste av bestemmelsene i kapittel 6 for visse typer avtaler inngått før 12. September 2025, samt at det ikke skal være noen plikt til å reforhandle avtalene før de utløper. Begge forslagene er beholdt i det seneste kompromissforslaget fra presidentskapet (26. april).

6.5 AI Act (KI-forordningen)

EU har vedtatt et felles regelverk for kunstig intelligens som skal sikre at KI-systemene som brukes i EU skal være trygge. På norsk kalles dette regelverket KI-forordningen. Formålet er å legge til rette for innovasjon og teknologisk utvikling, samtidig som våre

grunnleggende samfunnsverdier ivaretas. Forordningen bygger på et risikobasert system der kravene som stilles øker i takt med hvilken risiko et system kan utgjøre for menneskers helse, grunnleggende rettigheter eller sikkerhet.

De strengeste forpliktelsene i KI-forordningen gjelder for KI-systemer som klassifiseres som høyrisiko. Denne kategorien er avgrenset til to tilfeller: KI-systemer som er integrert i bestemte produkter regulert av eksisterende EU-regelverk – som medisinsk utstyr, kjøretøy og leketøy – og KI-systemer som brukes på særlig kritiske områder, som rekruttering, utdanning og drift av kritisk infrastruktur. Virksomheter som hverken utvikler, videreformidler eller tar i bruk slike KI-systemer vil ikke være underlagt de strengeste kravene i KI-forordningen. KI-forordningen tar med andre ord ikke sikte på å regulere skytjenester. Det er imidlertid teoretisk mulig at AIA kan påvirke skyleverandører, men dette vil bero på en konkret helhetsvurdering for de enkelte typetilfellene. Eksempelvis oppstiller AIA ansvar for aktører som er involvert i KI-verdikjeden. Det er derfor mulig at en skyleverandør kan få forpliktelser etter art. 25 dersom leverandøren gjør endringer i et KI-system som hostes fra deres skytjeneste på en måte som fanges opp av AIA art. 25 nr. 1 flg..

6.6 Cloud and AI Development Act (CADA)

Forslaget til den nye forordningen «CADA» ble etter flere utsettelse presentert av kommisjonen den 3. juni som del av den såkalte "Tech Sovereignty Package". At kommisjonens forslag overhodet blir presentert er et tegn på at noe vil bli vedtatt, selv om man må regne med at det blir endringer i løpet av trilogforhandlingene. CADA inneholder særlig to virkemidler som kan få konsekvenser for hvordan norske offentlige virksomheter arbeider med anskaffelser av skytjenester: krav til risikovurdering og suverenitet, samt krav til "EU added value"-kvalitetsindikatorer i anskaffelser.

6.6.1 Sikkerhetsnivå og risikovurderinger ved bruk av skytjenester i offentlige virksomheter

CADA del IV, kapittel 1, etablerer et rammeverk for suverenitet i skytjenester. Forordningen forutsetter at medlemslandenes myndigheter, til dels også private selskaper, som er omfattet av tillegg I og II til NIS2-direktivet ("vesentlige" og "viktige" samfunnstjenester) tar hensyn til digital suverenitet ved anskaffelser av skytjenester.

For å ivareta dette etablerer forordningen fire sikkerhetsnivåer ("assurance levels"). Offentlige myndigheter er i henhold til art. 29 forpliktet til å foreta en risikovurdering hvert annet år. Denne skal:

- Identifisere bruk av skytjenester i offentlige virksomheter som bidrar til å opprettholde offentlig orden ("contribute to the preservation of public order")
- Bestemme hvilket av de fire sikkerhetsnivåene som er passende for de forskjellige tjenestene

Risikovurderingen skal ta hensyn til mengden av og sensitiviteten til både persondata og ikke-personlige data som tjenesten behandler, behandlingens kontekst og omfang samt risiko for brudd på grunnleggende rettigheter og friheter. Den skal eksplisitt beskrive

risiko og konsekvenser at tredjeland får tilgang til dataene som behandles i tjenesten, og konsekvensene av et eventuelt brudd i tjenesteleveransen. Det siste gjelder uansett hva avbruddet skyldes, men er også ment å omfatte såkalte "kill-switches". Kommisjonen får i henhold til samme artikkel fullmakt til å utarbeide retningslinjer for hvordan risikovurderingen skal gjennomføres, og har i tillegg rett til å bestemme om medlemslandenes risikovurderinger har plassert de forskjellige tjenestene på et passende sikkerhetsnivå. Det er uklart hvordan denne og andre håndhevingsmekanismer eventuelt vil bli gjennomført i norsk rett, men det vil sannsynligvis måtte etableres et myndighetsorgan med liknende karakteristikk som RME (reguleringsmyndigheten for energi). Forordningen gir også kommisjonen fullmakt til å revidere kriteriene for de forskjellige sikkerhetsnivåene.

De fire sikkerhetsnivåene stiller krav av både teknisk og organisatorisk art for leverandører og underleverandører, og er for de høyeste sikkerhetsnivåene svært omfattende. Nivå 1 stiller grunnleggende krav til sikkerhet og kontroll over tjenesten, og krever blant annet at data og infrastruktur til enhver tid må befinne seg i EU. I tillegg må leverandøren via uavhengige kilder bekrefte at de ikke er underlagt en jurisdiksjon som krever at de avslører sikkerhetsbakdører til myndighetene uten å opplyse om dette i offentligheten. Nivå 2 stiller i tillegg til dette blant annet krav til at leverandørens personell må befinne seg i EU, og at leverandøren skal iverksette alle nødvendige tiltak for å forhindre eventuelle tredjeland med jurisdiksjon over dem fra å få tilgang til kundens data. Nivå 2 utelukker ikke at leverandøren kan være underlagt tredjelands myndigheter, og det er noe uklart hvordan kravene til at leverandøren må «forhindre» innblanding fra fremmede myndigheter skal forstås. På nivå 3 er enhver form for kontroll av fremmede myndigheter som hovedregel utelukket, enten den utøves gjennom offentlig myndighet, i kraft av eierskap osv. Leverandørens personell må være EU-borgere. Forordningen oppstiller en unntaksadgang, men denne ser i praksis ut til å være svært snever. På nivå 4 stilles svært strenge krav som også strekker seg til tredjeparters kontroll og innflytelse over programvare som leverandøren benytter seg av. På nåværende tidspunkt er det vanskelig å si noe mer konkret om hvordan de forskjellige kravene til sikkerhetsnivå vil bli forstått, og mye avhenger også av hvilke typer offentlige virksomheter som havner inn under de forskjellige nivåene.

	Control	EU infra-structure	Personnel	AI inference data	Supply chain	Sub-contractors	Vulnerability disclosure restrictions	Cybersecurity	Type of assessment
Level 4	EU established, owned and controlled	Fully located in the Union	Located in the EU and EU citizens. Security cleared (**)	Not transferred outside of the EU and not reused by a third-country entity	Effective control (over the software)	Established in the Union, owned, and controlled	Not needed	High	National authorities based on a 3 rd party-audit
Level 3	EU established, owned and controlled (*)	Fully located in the Union	Located in the EU and EU citizens. Security cleared (**)	Not transferred outside of the EU and not reused by a third-country entity	High degree of control (auditable software)	Established in the Union. If owned by a 3 rd country, absence of interference (*)	No hidden disclosures	Substantial	National authorities based on a 3 rd party-audit
Level 2	EU established & absence of 3 rd country interference	Fully located in the Union	Located in the EU. EU citizens if required by the customer	Not transferred outside of the EU and not reused by a third-country entity	High degree of control (auditable software)	Established in the Union. If owned by a 3 rd country, absence of interference	No hidden disclosures	Substantial	National authorities based on a 3 rd party-audit
Level 1	EU established	Fully located in the Union	Located in the EU	No requirement	No requirement	Full transparency	No hidden disclosures	State-of-the-art cybersecurity standards	Self-assessment

(*) a cloud computing service subject to the control of a third country or a legal entity established in a third-country can still be audited against the audit criteria where the third country has implemented specific safeguards that ensure that there is no risk of unauthorised access to Union data or possible disruption of service quality or continuity.
(**) where appropriate

Figur 1 - Sammenlikning av de forskjellige sikkerhetsnivåene. (Kommisjonens Impact Assessment Report SWD(2026) 502 Final, s. 40)

Dersom kommisjonen eller den offentlige virksomheten selv kommer frem til at en tjeneste benytter en skytjenesteleverandør som ikke oppfyller kravene til sikkerhetsnivået for tjenesten, bestemmer art. 29 at migrering til ny tjeneste må skje innen 12 måneder. Artikkelen bestemmer også at risikovurderingene må vurdere bruken av multi-cloud eller multi-vendor som avbøtende tiltak.

Art. 30 bestemmer at offentlige virksomheter må benytte skytjenester som minst oppfyller kravene til sikkerhetsnivå 1 (det laveste nivået). For offentlige virksomheter som i henhold til NIS2-direktivet leverer vesentlige eller viktige samfunnstjenester, er kravet at skytjenesten må oppfylle kravene til sikkerhetsnivå 2. Både sentral og regional offentlig forvaltning er betegnet som "vesentlig" i NIS2. Det er i skrivende stund uavklart om begrepet regional forvaltning også omfatter kommuner. Dersom kommuner faller utenfor er det imidlertid ikke klart at de helt og holdent vil havne utenfor kravet til å benytte nivå 2-tjenester. Artikkel 29 bruker begrepet «public sector *activities*» – kravet til sikkerhetsnivå er altså ikke knyttet til virksomheten som sådan, men hvilke oppgaver virksomheten har. Norske kommuner har ansvar for viktige samfunnstjenester som åpenbart «bidrar til den offentlige orden» i forordningens forstand, og må regne med at enkelte av disse tjenestene kan måtte plasseres på både nivå 2 og 3.

Kravet til å minst benytte nivå 2-tjenester gjelder også offentlige virksomheter innen nasjonal sikkerhet, grensekontroll, forsvar samt politi- og rettsvesen, uavhengig av hvilken status de har etter NIS2. En passus i art. 29(3) forutsetter også at virksomheter på forsvarsfeltet kun kan benytte skytjenester på nivå 4. Det er noe uklart i hvilken grad forskjellige tjenester og aktiviteter innad i en og samme organisasjon kan benytte skytjenester på ulike nivåer, for eksempel basert på sikkerhetsklassifisering av informasjonen som behandles. Det er tydelig at CADA er ment å treffe forskjellige bruksområder, ikke enkelte offentlige virksomheter som helhet. Enkelte kritiske offentlige virksomheter vil likevel nødvendigvis ende opp med at en stor del av deres

oppgaver faller inn under et høyt sikkerhetsnivå. Dette kan få store konsekvenser for bruken av alminnelige kontorstøtteverktøy, integrerte KI-verktøy, epost osv.. På pressekonferansen etter presentasjonen av CADA uttalte visepresident i Kommisjonen Henna Virkkunen at det ville være "vanskelig" for amerikanske skytjenester å oppnå sikkerhetsnivå 3 i lys av CLOUD Act og FISA, se figur 3, under. Kommisjonens konsekvensutredning (SWD (2026) 502 Final) forventer imidlertid at fordelingen av brukstilfeller på de forskjellige sikkerhetsnivåene vil være hhv. 70% på nivå 1, 20% på nivå 2, 9% på nivå 3 og 1% på nivå 4. Kommisjonen bruker et fiktivt offentlig vannverk som eksempel, se figur 2, under.

Table 6. Illustrative distribution of criticality of IT systems within a fictitious public sector water company

Non-critical use cases (candidate for level 1)	Critical use case (candidate for levels 2-4)
• Procurement • Stock management • Inventory • Helpdesk • Billing system • Accounting system • CRM • Workforce management: ○ Payroll ○ Timesheets ○ Training ○ Holidays ○ Recruitment ○ ... • ...	• Water monitoring system • Incident response system • Early warning system

Figur 2 - Illustrasjon av fordeling mellom sikkerhetsnivåer i en fiktiv offentlig virksomhet (Impact Assessment Report SWD (2026) 502 Final, s. 42)

Types of providers whose services could currently reach sovereignty Levels 1-4

Level 1: US hyperscalers generally all have offerings that would allow them to qualify under Level 1. They offer dedicated EU-based cloud services with strong cybersecurity credentials which rely exclusively on (data) 'regions' located in the EU, including for redundancy.

Level 2: Several US hyperscalers have partnered with EU companies to provide additional sovereignty assurances – these partnerships are often called “sovereign joint ventures”. While the implementation models differ, such partnerships generally rely on majority EU ownership, operation by EU personnel, data centre region limited to a particular Member State, cloud software stack provided by a hyperscaler, with security layer controlled by the EU partner, auditable core software, with some reaching certification under the SecNumCloud scheme. Non-European companies, outside of joint ventures, could also qualify provided they demonstrate the absence of 3rd country interference.

Level 3: EU providers would easily satisfy the control criteria. They would have to pass the necessary cybersecurity controls to achieve the future EUCS certification at assurance level Substantial or High. The other difficulty would be to demonstrate a 'very high' control over their software supply chain, something demonstrated in the recently awarded contract by the Commission for sovereign cloud services.

Level 4: This level differs from level 3 in stricter cybersecurity certification and full control over the software supply chain, something that some emerging EU offerings propose, at least for some type of cloud services.

Figur 3 - Hvilke nåværende skytjenesteleverandører som kan oppfylle de forskjellige sikkerhetsnivåene (Komisjonens Impact Assessment Report SWD (2026) 502 Final, s. 40)

6.6.2 Tvungne kvalitetsindikatorer i offentlige anskaffelser og plikten til å vurdere "open source first"

Art. 32 i CADA bestemmer at anskaffelser som gjelder "innovative" skytjenester og KI-systemer må inkludere kvalitetskrav som vurderer hvordan anskaffelsen vil bidra til å utvikle det europeiske skytjeneste- og KI-økosystemet. Dette kvalitetskravet skal ikke alene være utslagsgivende, men må telle med i tillegg til andre kvalitetskrav og priskrav. Vurderingen skal spesifikt ta hensyn til:

- Hvordan tilbyderen bidrar til å styrke de digitale forsyningskjedene i Europa, for eksempel ved å bruke maskin- eller programvare designet eller produsert i EU.
- Om tilbyderen benytter teknologi som er utviklet i EU.
- Om valg av tilbyderen kan føre til innovasjon og utvikling som styrker det europeiske økosystemet på skytjeneste- og KI-området.
- Om tilbyderen benytter seg av regne- og lagrings- og nettverkskapasitet som benytter maskinvarekomponenter utviklet eller produsert i EU.

I tillegg pålegger 33 myndighetene i hvert medlemsland å operere med et mål om at 25% av alle offentlige anskaffelser av skytjenester og KI skal tilfalle «innovative» små og mellomstore bedrifter.

Artikkel 41 bestemmer at medlemslandene er forpliktet til å oppfordre offentlige virksomheter til å bruke åpne standarder og programvare utgitt med åpen kildekode i sine sky- og KI-tjenesteanskaffelser. I motsetning til bestemmelsene om suverenitet dreier det seg her om en form for soft law, som det er mer uklart om vil ha konkret betydning.

7 Behov for videre tiltak

Prosjektet har blitt bedt om å vurdere om det er behov for tiltak som ikke allerede er dekket opp på området. Dette arbeidet har gitt mye innsikt og mange viktige diskusjoner. I prosjektets arbeid har vi, både ut fra det gitte mandatet og arbeidsgruppens begrensede ressurser, måttet avgrense omfanget av rapporten. Men vi har gjort observasjoner som kan være viktige og interessante for mange deler av offentlig sektor.

Arbeidsgruppen vil her peke på noen tema/områder som det bør jobbes videre med.

7.1 Kunstig intelligens

I kartlegging og avgrensing av arbeidet, ser arbeidsgruppen at kunstig intelligens (KI) har stor innflytelse på skytjenester, både integrert i skytjenesteplattformer og som dedikerte tjenester (AI as a Service). I tiden fremover vil sannsynligvis denne innflytelsen øke betydelig, blant annet fordi teknologiens videreutvikling er selvforsterkende og det vil åpne seg stadig nye bruksområder.

For at norske virksomheter skal hente ut det enorme gevinstpotensialet som ligger i dette uten å gå på kompromiss med norske verdier, etikk og sikkerhet, trengs det proaktiv nasjonal veiledning og arkitektoniske rammer. Uten felles retningslinjer risikerer vi fragmentert utnyttelse av teknologien og fremvekst av usikker skygge-KI.

Arbeidsgruppen ser at det er viktig å designe bruken av KI slik at virksomheter har god mulighet til å bytte ut KI modeller i systemene. De samme prinsippene som kommer frem i denne rapporten om skytjenester vil være aktuelle også for KI. På linje med anbefaling om skytjeneste hybrid- og multisky, bør virksomhetene gjøre tilsvarende grep for KI tjenester for å sikre fleksibilitet og portabilitet. Arbeidsgruppen foreslår at KI Norge får ansvar for å veilede rundt endringsevne i bruk av KI.

7.2 Digital suverenitet

Dersom CADA-forordningen blir vedtatt i samme form som forslaget fra EU-Kommisjonen, skal det gjennomføres risikovurderinger som også ser på digital suverenitet ved bruk av skytjenester i samtlige offentlige virksomheter. Selv om det vil komme veiledning fra EU bør nasjonale myndigheter sørge for å ligge i forkant med veilednings- og informasjonsarbeidet, slik at kravene ikke kommer som en overraskelse

på norske offentlige virksomheter. Dette gjelder særlig for de virksomhetene som leverer tjenester som kan komme til å trenge skytjenester kategorisert på nivå 3 og 4 (se punkt 5.6.1, over). Innføring av CADA vil også ytterligere aktualisere problemet med fremmede lands tilgang til data gjennom skytjenesteleverandører som opererer på tvers av landegrenser. Avtalerettslige og organisatoriske tiltak for sikkerhet og tilgangsstyring til sensitive data er ikke tilstrekkelige når leverandørene opererer i et internasjonalt eller globalt marked. USAs CLOUD Act og saken mellom OVHClouds canadiske datterselskap og canadiske myndigheter trekkes gjerne frem som enkeltteksempler. Faktum er at dette er regelen heller enn unntaket, for den saks skyld også i Europa og Norge. Å forhindre fremmede land fra å få tilgang på data gjennom å kontrollere dataenes fysiske lokalisering, er altså ineffektivt.⁶

Digital suverenitet blir trukket frem som et svar på konsentrasjonsrisiko. Arbeidsgruppen anbefaler at styrende myndigheter tar ansvaret for å gjennomføre vurderinger av konsentrasjonsrisiko. Hver for seg kan ikke offentlige virksomheter forventes å ha den oversikten som kreves for å foreta slike vurderinger.

7.3 Utrede avhengighet til SaaS kontorstøtteverktøy

Risikoen ved norske offentlige virksomheters avhengighet av enkeltleverandører av kontorstøtteverktøy bør utredes. Alle typer kontorstøtteverktøy bør ses på, men arbeidsgruppen vil særlig peke på kommunikasjons- og samhandlingsverktøy som e-post, chat, digitale møter, tekstbehandlingsverktøy og verktøy for dokumentlagring- og samhandling.

7.4 Etablere styringsmekanismer for å sikre gjennomføring av tiltak lokalt

Det må legges til rette for samarbeid på tvers av virksomheter i offentlig sektor. Mange har like behov, men ulik kapasitet. Dersom hver enkelt virksomhet må utvikle egne exit-strategier, kravspesifikasjoner, tekniske løsninger, risiko- og driftsmodeller, kan kostnadene bli høye og resultatene fragmenterte. Felles offentlige krav, felles anskaffelser, felles risikomodeller, sektorvise løsninger, nasjonale fellesløsninger eller nasjonale støttemiljøer kan styrke gjennomføringsevnen.

Som tidligere nevnt vil kostnadene her i stor grad komme lokalt, mens den sikkerhetsmessige gevinsten vil være nasjonal. Derfor bør det vurderes måter å bistå det lokale arbeidet, i form av ressurser, bistand eller midler. Det bør utredes muligheter for fellesløsninger som understøtter kritisk digital infrastruktur.

⁶ Se Pervaiz, Shanzay og Joel, Alex, "Data Localization and Government Access to Data Stored Abroad: Discussion Paper 2" (2023). Joint PIJIP/TLS Research Paper Series. 87.
<https://digitalcommons.wcl.american.edu/research/87>

7.5 Endre rådene til offentlig forvaltning i digitaliseringsrundskrivet

Det har blitt kommunisert til arbeidsgruppen at digitaliseringsdirektivets kapittel om skytjenester (pkt. 1.15) blir oppfattet som en beskjed om å velge «sky først». Ut fra ordlyden er det lett å forstå denne tolkningen. Arbeidsgruppen anbefaler at digitaliseringsrundskrivet endres til å bli mer nøytral med hensyn til å beskrive både fordeler og ulemper ved teknologien.

Konkret mener arbeidsgruppen at det bør tas inn krav om exit-strategi basert på denne rapporten. Videre bør teksten i rundskrivet under overskriftene krav og anbefaling nyanseres ut fra dagens reelle situasjon. Skytjenester kan både være kostnadseffektive og fleksible, men fare for lock-in og kostnadsdrivende avtaler er reelt og bør vurderes.

7.6 Offentlige fellesavtaler om skytjenester som legger til rette for endringsevne

Fellesavtaler for offentlig sektor kan være tilgjengeliggjørende og kostnadseffektive, men virksomheter som skal levere tjenester ut over avtalenes varighet må ha en klar exit-strategi. Arbeidsgruppen anbefaler derfor at det blir obligatorisk på fremtidige fellesavtaler at virksomheter som skal levere tjenester ut over avtaleperioden har implementert en exit-strategi.

7.7 Bruk av åpne standarder, arkitekturprinsipper, arkitektur og standardiseringsrådet og IT-standardiseringsforskriften

Mer aktiv bruk av regulatoriske virkemidler som IT-standardiseringsforskriften og arkitektur og standardiseringsrådet (ASR) kan gjøre det lettere for offentlig forvaltning å gjøre gode valg når det skal velges teknologi for å levere tjenester.

Arbeidsgruppen anbefaler derfor å styrke arbeidet med referansekatalogen for IT-standarder, de overordnende arkitekturprinsippene for digitalisering av offentlig forvaltning (arkitekturprinsippene) og ASR. Herunder ønskes det at forløpet til standarder blir bedre forvaltet med gjennom innlemming, kontinuitetsvurderinger og utfasing. Videre anbefales det at arkitekturprinsippene blir mer detaljerte og enklere å benytte i dagens teknologiske landskap. For eksempel lyder punkt 5.3 i arkitekturprinsippene «Sørg for arkitektur som gir systemer og tjenester evne til endring og vedlikehold over tid.» Dette er i samsvar med arbeidsgruppens anbefalinger, men uten videre detaljering av rådet er det på et så overordnet nivå at det er vanskelig å oversette til praksis.

Gevinsten ved en bedre forvaltning av referansekatalogen, IT-standardiseringsforskriften og arkitekturprinsippene som inkluderer samsvarsvurderinger kan være et mer velfungerende økosystem for skytjenester, da de offentligaktørene vil stille samsvarende krav til leverandør markedet og basere sine krav på åpne ressurser.

8 Vedlegg

1. EU initiativ oppdatert 13.03.2026