Fafo

Johan Røed Steen

Skytjenester for offentlig sektor

Avveininger og internasjonale erfaringer

Fafo-rapport
2022:22

Johan Røed Steen

Skytjenester for offentlig sektor

Avveininger og internasjonale erfaringer

Fafo-rapport 2022:22

Fafo-rapport 2022:22

ISBN 978-82-324-0655-5
ISSN 2387-6859

Innhold

Forord

Skybaserte digitale tjenester kan gi en rekke fordeler for offentlige virksomheter, blant annet at de kan leveres og skaleres etter behov, gir økt fleksibilitet og krever mindre investeringer i lokale IKT-ressurser. Bruk av skytjenester i offentlig sektor er samtidig assosiert med nye former for risiko, blant annet knyttet til personvern, tillit til myndighetene og juridisk risiko i form av at norske data lagres utenlands og/eller behandles av leverandører underlagt andre lands jurisdiksjon. Norske myndigheter har så langt hovedsakelig satset på kjøp av skytjenester i markedet, som domineres av noen få store aktører. Flere land har valgt å opprette statlig kontrollerte skytjenester, og en norsk statlig skyløsning er under utredning ved rapportens utgivelse.

Denne rapporten gjennomgår prinsipielle problemstillinger rundt organiseringen av skytjenester for offentlig sektor, og kartlegger erfaringer fra andre land med vekt på strategier og begrunnelser for valg av ulike løsninger.

Vi vil rette en stor takk til alle som har satt av tid og bidratt gjennom å delta i intervjuene rapporten bygger på. En takk også til Torstein Brechan og Hallvard Berge i NTL og Christian Danielsen i Fagforbundet som har fulgt prosjektet og bidratt med innspill. Takk til Åsmund Arup Seip som har kvalitetssikret rapporten, og Fafos informasjonsavdeling som på kort tid har ferdigstilt rapporten.

Oslo, oktober 2022
Johan Røed Steen

Sammendrag

Denne rapporten handler om bruk av skytjenester i offentlig sektor og diskuterer problemstillinger knyttet til digital suverenitet og muligheten for en offentlig eid nasjonal skytjeneste.

Skytjenester spiller en økende rolle i utviklingen av IKT og digitale tjenester i offentlig sektor, og understøtter allerede en rekke viktige offentlige tjenester. Offentlige virksomheter behandler stadig mer data i skyen. Bruk av skytjenester i offentlig sektor er samtidig assosiert med nye former for risiko, blant annet knyttet til fremtidig avhengighet av leverandører, datasikkerhet, personvern og juridisk, som aktualiserer behovet for digital suverenitet og kontroll med hvor data lagres og behandles.

Norske myndigheter har så langt hovedsakelig benyttet private tilbydere av skytjenester. Flere andre europeiske land har derimot valgt å opprette statlig kontrollerte skytjenester, og denne tilnærmingen har blitt stadig mer aktuell også i Norge. Myndighetene har utredet muligheten for en nasjonal sikker sky siden 2016, og det pågår i 2022 en konseptvalgutredning (KVU) om en statlig skytjeneste for skjermingsverdig informasjon.

Rapporten bygger på en gjennomgang av offentlige dokumenter, strategier og samfunnsvitenskapelig faglitteratur om bruk og organisering av skytjenester i offentlig sektor, supplert med intervjuer med utvalgte beslutningstakere. Problemstillingene i prosjektet har vært 1) Hvilke vurderinger norske myndigheter har gjort når det gjelder eierskap til og organisering av skytjenester for offentlig sektor, og hvordan dagens strategi begrunnes; 2) Hvilke prinsipielle avveininger og problemstillinger nasjonale myndigheter står ovenfor ved valg av eierskapsmodeller og organisering av skyløsninger og; 3) Hvilke erfaringer med nasjonale skytjenester og datasentre som er gjort i andre europeiske land og hvordan strategiske veivalg begrunnes.

Bruk av skytjenester i offentlig sektor

Skytjenestene åpner for at mer og mer IKT kan leveres som tjenester og over nett, der det tidligere har vært vanlig at offentlige virksomheter har kjøpt inn datautstyr og programvare, og driftet dette selv. Offentlige virksomheter tar i økende grad i bruk skytjenester, i tråd med politiske signaler. Syv av ti statlige virksomheter spurt i en undersøkelse for KMD (A2, 2021) oppgir at de benytter en eller flere skyløsninger. Seks av ti har i stor grad har satt ut drift og forvaltning av IKT-infrastruktur. Offentlige virksomheter forventer også videre vekst i bruken av skytjenester. Lagring av data utenfor Norge er utbredt, særlig for hyllevare- og kontorstøtteløsninger. Difi (2017) fant i sin utredning av kundegrunnlaget for en nasjonal sikker skytjeneste at i snitt ca. 60 prosent av virksomhetene som lagrer skjermingsverdig informasjon elektronisk ønsker å ta i bruk sikre skytjenester, gitt at de er godkjent av NSM. Det ser ut være betydelig etterspørsel etter en slik skyløsning, fra et bredt spekter av offentlige virksomheter i både statlig og kommunal sektor, og behovet gjelder en rekke ulike tjenester og data.

Nasjonal strategi for skytjenester

Den norske strategien for bruk av skytjenester baserer seg i stor grad på markedet, med oppfordring til bruk av allmenne skytjenester. Den nasjonale strategien for skytjenester og digitaliseringsskrivet legger de viktigste føringene. Offentlige virksomheter pålegges å vurdere skytjenester, og anbefales å velge dem når det er kostnadseffektivt og hensiktsmessig. Strategien er gjennomgående positiv til allmenne skytjenester. Samtidig vises det til at offentlig sektor har et spesielt behov for kontroll. Kontrollbehovet skal ivaretas gjennom den nylig lanserte offentlige markedsplassen for skytjenester, som samordner standardkontrakter, sertifiseringer, og prekvalifisering av leverandører. Løsningen er inspirert av Storbritannia, som tidlig etablerte en egen markedsplass for skytjenester og har satset på å benytte private tilbydere. Det er lite i regjeringens digitaliseringsstrategi eller strategi for bruk av skytjenester som viser at det er gjort vurderinger av digital autonomi eller av behov for å sikre digital kompetanse i offentlig sektor. Samtidig har en alternativ tilnærming med datasentre og skytjenester under statlig kontroll vært vurdert over en periode og synes å bli mer aktuell.

Utredning av nasjonal skytjeneste

Som oppfølging av arbeidet rundt den nasjonale skytjenestestrategien har NSM og digitaliseringsdirektoratet vurdert handlingsrommet for en sikker skytjeneste og mulig innretning av denne. NSMs første rapport fra 2016 ble fulgt opp i 2017 med vurderinger av hvilken type informasjon som bør omfattes av en slik løsning, potensielt kundegrunnlag og aktuelle markedsaktører, samt handlingsrom i henhold til anskaffelsesregelverket. Utredningsarbeidet førte ikke umiddelbart ny politikk, men regjeringen har signalisert en mer aktiv tilnærming og i tråd med vedtak i Stortinget har Justisdepartementet i samarbeid med KMD og FD igangsatt en konsekvensutredning (KVU) for etablering av en nasjonal skytjeneste for ugradert, skjermingsverdig informasjon, som skal leveres i desember 2022.

Utredningsarbeidet har tatt utgangspunkt i at en eventuell nasjonal skyløsning vil komme i tillegg til og ikke som en erstatning for den gjeldende strategien og markedsplassen for skytjenester. En nasjonal sikker sky skal innrettes mot ugradert skjermingsverdig informasjon, som ikke egner seg til behandling i allmenne skytjenester. En nasjonal skyløsning skal med andre ord ikke konkurrere med markedsrettede løsninger men være et alternativ ved behandling av informasjon som ikke er egnet for slike skytjenester.

Digital suverenitet

Overgang til skytjenester kan gi betydelige gevinster for offentlige virksomheter, i form av økonomiske innsparinger, skalering, trygghet, energieffektivitet, fleksibilitet og innovasjon. Bruk av skytjenester i offentlig sektor er samtidig assosiert med nye risikofaktorer, blant annet knyttet til fremtidig avhengighet av leverandører, datasikkerhet, personvern og juridisk risiko i forbindelse med at data lagres utenlands eller behandles av leverandører underlagt andre lands jurisdiksjon. Dette har aktualisert spørsmål rundt behovet for *digital suverenitet,* altså ideen om at staten bør hevde sin suverenitet også i det digitale domenet. I forbindelse med skytjenester brukes digital suverenitet gjerne om nasjonal kontroll og eksklusiv jurisdiksjon over data og kontroll med hvor data lagres og behandles, hvem som har tilgang og eierskap, og tillit til at data behandles på en måte som ivaretar nasjonale interesser og innbyggernes personvern og rettigheter.

Strategier for skytjenester i offentlig sektor er ikke kun et spørsmål om teknologi og økonomi, det er også et politisk veivalg. En rekke hensyn må veies mot hverandre i utforming av strategi og valg av løsninger. Sentrale problemstillinger inkluderer hensyn til personvern og personvernreglement, behovet for nasjonal kontroll og lokasjonskrav til datalagring og behandling, datasikkerhet, leverandøravhengighet og innløsingseffekter, behov for og bygging av teknologisk kompetanse, og hvordan bruka av skytjenester kan påvirke borgernes tillit til myndighetene. Om det sees som en kjerneoppgave for staten å hevde sin suverenitet også i det digitale domenet vil slike hensyn veie tungt.

Internasjonale erfaringer

Et ønske om digital autonomi og datasuverenitet, i betydningen at myndighetene kan ha fullstendig kontroll over egne data i skyen gjennom eksklusiv jurisdiksjon over disse i tillegg til vanlige sikkerhetstiltak, ligger til grunn for at en rekke land har valgt strategier delvis basert på statlige løsninger. Rapporten ser nærmere på Tyskland, Nederland, Danmark og felleseuropeiske initiativer. Tyskland har valgt å etablere sin egen «private» statlige sky og har i stor grad valgt å organisere og drifte IKT-tjenestene sine selv. Den tyske strategien setter digital suverenitet og nasjonal kontroll høyt. Begrunnelsen for å drive skytjenester i statlig regi er ikke bare sikkerhet og kontroll over data, men også at offentlig sektor skal kunne være fleksibel i møte med nye utviklingstrekk og en attraktiv arbeidsplass for de flinkeste IT-folkene. Den tyske strategien tar også utgangspunkt i at statens aktive rolle og drift av skytjenester i egen regi kan gi økonomiske og praktiske fordeler. Nederlandske myndigheter har også opprettet statlige skytjenester og vektlegger bruk av software med åpen kildekode for å hindre innlåsingseffekter. Den nederlandske tilnærmingen har fellestrekk med den tyske, men åpner i større grad også for private tilbydere. Statlige datasentre og egne skytjenester for statsforvaltningen ble opprettet da det ble vurdert at markedet ikke kunne levere, verken med tanke på kostnadsbesparelser eller krav til personvern og datasikkerhet. Med et mer modent marked har myndighetene gradvis åpnet for en multi-sky tilnærming der også allmenne skytjenester brukes for data med lavere beskyttelsesbehov. Danmark har hatt en tilnærming som likner mer på den norske og har i stor grad brukt private tilbydere, men det jobbes nå med å videreutvikle og skalere opp den statlige skytjenesten GovCloud. Dette er en skytjenesteløsning for statsforvaltningen som ble opprettet for å møte interesse for skytjenester fra statlige virksomheter. Omfanget er foreløpig begrenset, men løsningen eksemplifiserer at en statlig skytjeneste kan opprettes med relativt beskjedne oppstartskostnader og utvides etter behov. På europeisk nivå har Tyskland og Frankrike tatt initiativ til Gaia-X prosjektet, som tar sikte på å bygge en sikker og suveren europeisk datainfrastruktur gjennom offentlig-privat samarbeid og europeiske tjenesteleverandører, med mål om å utfordre de amerikanske skyleverandørene. EU-kommisjonen har også lansert et initiativ for å bygge felles skytjenester som henviser både til Gaia-X og integrasjon mellom eksisterende nasjonale skyløsninger. Foreløpig er disse europeiske initiativene likevel nærmere idéstadiet enn et reelt alternativ til de amerikanske skygigantene.

1 Bakgrunn

Bruken av skytjenester er i kraftig vekst, i offentlig sektor som i privat næringsliv. Skybaserte digitale tjenester kan leveres og skaleres etter behov og gir tilgang til ny teknologi raskt. Det kan gi offentlige virksomheter fordeler i form av skalering, trygghet, energieffektivitet, fleksibilitet og innovasjon. Samtidig er bruk av skytjenester i offentlig sektor assosiert med risiko og nye utfordringer, blant annet knyttet til datasikkerhet, personvern og juridisk risiko i form av at data lagres utenlands og/eller behandles av leverandører underlagt andre lands jurisdiksjon. Problemstillingene ble aktualisert for mange norske virksomheter gjennom EU-domstolens Schrems II-avgjørelse som slo fast at europeiske borgere har et for svakt vern mot amerikansk overvåkning. Mer overordnet aktualiseres spørsmål rundt behovet for *digital suverenitet* og kontroll med hvor data lagres og behandles, hvem som har tilgang og eierskap, og tillit til at data behandles på en måte som ivaretar nasjonale interesser og innbyggernes personvern og rettigheter.

Regjeringen oppfordrer offentlige virksomheter til å ta i bruk skytjenester, blant annet i den nasjonale strategien for bruk av skytjenester (Kommunal- og moderniseringsdepartementet, 2016) og i digitaliseringsstrategien for offentlig sektor (Meld. St. 27, 2015–2016). Digitaliseringsrundskrivet krever videre at offentlige virksomheter skal vurdere skytjenester på linje med andre løsninger, og anbefaler at disse velges dersom det ikke foreligger spesielle hindringer, og skytjenester gir den mest hensiktsmessige og kostnadseffektive løsningen (Kommunal- og moderniseringsdepartementet, 2022: 1.11).

Nasjonal sikkerhetsmyndighet (NSM) vurderer at skytjenester kan bidra til å redusere sårbarhet spesielt for mindre virksomheter som ikke har kompetanse eller ressurser til digitalt sikkerhetsarbeid selv. Samtidig bringer skytjenester med seg nye sårbarheter og økt risiko på andre områder, herunder behov for nasjonal kontroll i spennet fred, krise, konflikt og krig. NSM er «bekymret for den samlede nasjonale avhengigheten av utenlandske skytjenesteleverandører» (2020a, s. 33) og viser til at dette medfører både en juridisk risiko ved at norske tjenester leveres fra utlandet og en konsentrasjonsrisiko i at et fåtall utenlandske leverandører bærer kritiske norske samfunnsfunksjoner. Avhengigheten av skytjenester kan utgjøre en betydelig utfordring for samfunnssikkerheten i fremtiden, og NSM peker på at «Skytjenester levert fra og med infrastruktur i Norge vil være en god start» (NSM, 2020a, s. 35).

En skytjeneste for offentlig sektor?

Også i den nasjonale strategien for skytjenester (Kommunal- og moderniseringsdepartementet, 2016) legges det vekt på at offentlige virksomheter kan ha særlige sikkerhets- og kontrollbehov. Strategien viser til at offentlig kontroll kan ivaretas enten gjennom 1) å etablere egne datasentre for offentlig sektor, eller 2) å sikre offentlig kontroll ved hjelp av kontrakter og standardavtaler som ivaretar det offentliges behov. Regjeringen har i praksis valgt sistnevnte tilnærming, med utstrakt bruk av tjenesteutsetting og markedsløsninger for skytjenester, i kombinasjon med økende samordning av IKT-tjenester og infrastruktur. Denne strategien innebærer blant

annet opprettelse av en offentlig markedsplass for skytjenester. Den skal gjøre det enklere for offentlige virksomheter å anskaffe kostnadseffektive IT-tjenester fra kommersielle leverandører med felles håndtering av kontraktsmessige sider ved sikkerhet og personvern. Ut over dette tiltaket har regjeringen så langt ikke lagt til rette for offentlig samarbeid om skytjenester eller etablering av felles datasenter, men heller understreket at det offentlige ikke skal opprette egne tjenester dersom disse kan leveres like godt i markedet (Seip, 2020, s. 84).

En rekke land, blant annet Tyskland, Danmark og Nederland, har opprettet egne statlig kontrollerte skytjenester. En tilnærming med dedikerte skytjenester og datasentre for offentlig sektor, har blitt mer aktuell også i Norge. I Hurdalsplattformen som legger det politiske grunnlaget for dagens regjering, skisseres en mer aktiv statlig rolle på området, der regjeringen vil «vurdere i hvilke tilfeller staten bør ta eierskap til digital infrastruktur, plattformer, plattformutvikling og standardutvikling» og «Utrede opprettelsen av en statlig skyløsning for lagring av offentlige data som helsedata, finansdata og informasjon om innbyggere og infrastruktur» (Regjeringen, 2021, s. 15). Justisdepartementet har i samarbeid med Kommunal- og distriktsdepartementet og Finansdepartementet igangsatt en Konseptvalgutredning (KVU) for etablering av en nasjonal skytjeneste for ugradert, skjermingsverdig informasjon. Nasjonal sikkerhetsmyndighet (NSM) er ansvarlig myndighet og skal etter planen levere KVUen 1. desember 2022.

Problemstillinger

Rapporten bygger på en gjennomgang av offentlige dokumenter, strategier og samfunnsvitenskapelig faglitteratur om bruk og organisering av skytjenester i offentlig sektor, supplert med intervjuer med utvalgte beslutningstakere. Problemstillingene i prosjektet har vært:

1 Hvilke vurderinger har norske myndigheter gjort når det gjelder eierskap til og organisering av skytjenester for offentlig sektor, og hvordan begrunnes dagens strategi?
2 Hvilke prinsipielle avveininger og problemstillinger står nasjonale myndigheter ovenfor ved valg av eierskapsmodeller og organisering av skyløsninger?
3 Hvilke erfaringer med nasjonale skytjenester og datasentre er gjort i andre europeiske land, og hvordan begrunnes strategiske veivalg?

Gangen i rapporten

Kapittel 2 omhandler utviklingen i bruk av skytjenester i offentlig sektor i Norge, myndighetenes begrunnelse for satsingen på skytjenester og hva vi vet om virksomhetenes behov for et statlig alternativ til de kommersielle skytjenesteleverandørene.

Kapittel 3 omhandler den nasjonale strategien for skytjenester samt tidligere og pågående utredningsarbeid norske myndigheter har gjort med tanke på muligheten for å opprette en nasjonal skyløsning.

Kapittel 4 diskuterer generelle problemstillinger knyttet til bruk og organisering av skytjenester i offentlig sektor og hvilke avveininger myndighetene må foreta i sine valg av løsninger, i lys av begrepet *digital suverenitet* og litteraturen på området.

Kapittel 5 kartlegger erfaringer med skytjenester for offentlig sektor i tre andre europeiske land; Tyskland, Nederland og Danmark, samt initiativer på europeisk nivå.

Kapittel 6 drøfter veivalget norske myndigheter står ovenfor ved valg av skyløsninger, i lys av omverdensanalysen.

2 Til himmels? Bruk av skytjenester i offentlig sektor

Skytjenester er i vekst, i offentlig som i privat sektor. Syv av ti statlige virksomheter spurt i en undersøkelse gjennomført for KMD (A2, 2021, s. 46) oppgir at de benytter en eller flere skyløsninger, og seks av ti har i stor grad satt ut drift og forvaltning av IKT-infrastruktur. Tradisjonelle IT-løsninger og det lokale datarommet er altså i mange virksomheter på vei til å bli erstattet eller integrert med lagring, regnekraft og programvare levert fra skyen. Skytjenestene åpner for at mer og mer IKT kan leveres som tjenester og over nett, der det tidligere har vært vanlig at offentlige virksomheter har kjøpt inn datautstyr og programvare, og driftet dette selv. Prosessen kan beskrives som en overgang fra varebasert til tjenestebasert innkjøp av IKT. Motivene er ofte økonomiske, knyttet til at virksomhetene ikke betaler for mer enn de bruker til enhver tid og får mer transparente kostnader. En viktig praktisk forskjell på skytjenester og mer tradisjonell tjenesteutsetting er forretningsmodellen, der kunden bare betaler for den kapasiteten som brukes. Dette kan gi kostnadseffektive, sikre, fleksible og skalerbare IT-tjenester. Dette er særlig attraktivt for virksomheter som har behov for stor kapasitet i en begrenset periode. Skytjenester gir også tilgang til de nyeste teknologiske løsningene og kan øke innovasjonsevnen ved å gjøre det lettere å videreutvikle eksisterende løsninger og sette opp nye. Stabil drift med høy oppetid, tilrettelegging for økt endringstakt, kostnadskontroll, skalerbar ytelse og ny funksjonalitet er attraktive kvaliteter.

Microsoft, fulgt av Amazon og Google, er de mest benyttede leverandørene. Dette medfører samtidig at lagring av data utenfor Norge er utbredt, og mange virksomheter har ikke full oversikt over hvor deres data befinner seg. Denne utviklingen gir utfordringer med tanke på at kritiske norske samfunnsfunksjoner allerede er avhengige av utenlandske leverandører. Utviklingen ser ut til å fortsette, ikke minst fordi overgang til skytjenester er forbundet med en rekke fordeler for virksomhetene.

I dette kapittelet ser vi først nærmere på hva skytjenester er, hva de kan brukes til og hvordan de leveres, i form av ulike tjeneste- og leveransemodeller. Deretter ser vi på hvordan norske myndigheter begrunner satsingen på skytjenester, hvilke fordeler de kan gi virksomhetene, og drøfter kort i hvilken grad fordelene ved skytjenester som ligges til grunn i strategien kan oppnås gjennom en nasjonal sky. Avslutningsvis ser vi på omfanget av skytjenester i offentlig sektor og hva vi vet om etterspørselen etter et statlig alternativ til de kommersielle skytjenesteleverandørene.

2.1 Om skytjenester

Skytjenester eller «cloud computing» brukes som en samlebetegnelse på skalerbare datatjenester som leveres over nett. Det kan omfatte alt fra regnekraft (dataprosessering) og datalagring til operativsystemer og programvare. Skytjenester inngår i det bredere begreper IKT (informasjons- og kommunikasjonsteknologi), og skytjenestene er som oftest tatt i bruk og vevet sammen med andre former for IKT, som nettbrett- og mobiltjenester, nettverk og datalagring.

Regjeringen har i den nasjonale skytjenestestrategi (Kommunal- og moderniseringsdepartementet, 2016) valgt å følge definisjon av skytjenester fra den amerikanske standardiseringsorganisasjonen NIST (National Institute of Standards and Technology):

> Skytjenester (cloud computing) er leveransemodeller som muliggjør nettverksbasert tilgang til et sett konfigurerbare dataressurser (herunder nettverk, servere, lagring, applikasjoner og andre tjenester) som er tilgjengelig over alt, blir levert og prises etter behov (on demand), skalerer dynamisk etter kapasitetsbehov, og som raskt kan avsettes og klargjøres med minimal administrasjon eller involvering fra tilbyderen. (NIST 2011, s.2, oversatt i NSM 2016, s.9)

Leverandøren kan fordele dataressursene sine dynamisk etter de ulike kundenes behov, og tjenestene kunden trenger kan skaleres opp eller ned etter hva kunden har bruk for, slik at ressursene i praksis oppleves tilnærmet uendelige. Ressursbruken blir målt, kontrollert og rapportert, og er gjennomsiktig for både kunden og leverandøren av tjenesten.

Skytjenester var tilgjengelig allerede på 1990-tallet, men de moderne allmenne nettskyene og skytjenestene ble introdusert fra 2006 da Amazon etablerte sitt datterselskap Amazon Web Service (AWS). I 2008 lanserte Google sin App Engine, som er en skybasert plattform for utvikling og drift av nettjenester, og i 2010 lanserte Microsoft sin skytjeneste Azure. Microsoft, Amazon og Google er i dag de ledende tilbyderne internasjonalt og tilbyr et svært bredt spekter av skytjenester.

Tjenestemodeller

Det er vanlig å skille mellom tre hovedkategorier av tjenestemodeller for sky, inndelt etter hvor mye av tjenesten leverandøren har ansvaret for (Watts & Reza, 2019):

- Infrastruktur som tjeneste (Infrastructure as a Service, IaaS) gir kunden tilgang til grunnleggende virtualiserte dataressurser man normalt vil ha i sitt eget datasenter som lagring, nettverk og prosessortid hvor kunden kan installere, konfigurere og ha kontroll på operativsystem, lagring og annen installert programvare. Programvaren som tilbyr tilgang til dataressursene kalles en hypervisor. Annen programvare som virtuell maskin, operativsystem og applikasjoner ligger dermed hos kunden. Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine er eksempler på tjenester som kan levere infrastruktur. Når kunden kjøper infrastruktur som tjeneste, leverer tjenesteleverandøren vanligvis bare nettforbindelse, lagring, servere og virtualisering. Dette kalles av og til også maskinvare som tjeneste (Hardware as a service, Haas).
- Plattform som tjeneste (Platform as a Service, PaaS) gir kunden mulighet til å installere og konfigurere programvare og applikasjoner hos skyleverandøren. Sluttbruker gis da en plattform hvor de kan installere, konfigurere og vedlikeholde sine tjenester, uten å trenge dyptgående kunnskap om å bygge eller forvalte infrastrukturen som skal til. Skyleverandøren tar seg av drift og vedlikehold av servere og nettverk, lagring, virtualisering, operativsystem og hjelpeprogrammer, men ikke selve programvaren som håndterer data. Eksempel på PaaS kan være en komplett utviklingsplattform med database og web-server. Google App Engine og Microsoft Azure er eksempler på Paas.
- Programvare som tjeneste (Software as a Service, SaaS) gir kunden tilgang til en programvare/applikasjon som er klar til bruk. Ved kjøp av programvare som

tjeneste er det vanligvis leverandøren som har ansvar for alt, oppretting av nettforbindelse, lagring, servere, virtualisering, operativsystemet, hjelpeprogrammer (middleware), oppetid og at programmet blir oppdatert og feil rettet. Sluttbruker trenger da ikke å beskjeftige seg med å installere, konfigurere, oppdatere og vedlikeholde programvaren lokalt. Programvaren kan kjøres gjennom nettleser eller en annen type nettbasert klient. Databasetjenester, e-post, tekstbehandler, regneark, regnskap og lønn, CRM og ERP-systemer m.m. kan tilbys som SaaS. Microsoft 365 og Googles G suite (Gmail m.m.) er eksempler på SaaS.

Det finnes også flere tjenestemodeller, som gjerne er en kombinasjon av de tre ovennevnte modellene. Skyleverandører har gjerne produkter innen flere av kategoriene, slik at kundene kan velge det som passer deres virksomhet og kjøpe tjenester på ulike nivåer. Felles for leveransemodellene er at de for kunden er selvbetjente og API-drevet.

Leveransemodeller

Tjenestemodellene for sky kan leveres på ulike måter. Det er vanlig å skille mellom ulike modeller for leveranse, etter hvem som har tilgang til skyen:

- Privat sky (private cloud)[1] er skytjenester som kun er tilgjengelig for én virksomhet. En privat sky kan være eid, driftet og vedlikeholdt av virksomheten selv, en ekstern aktør eller i en kombinasjon. Gruppesky (community cloud) brukes om private skytjenester som er tilgjengelig for en gruppe virksomheter innenfor samme sektor eller virksomheter som deler samme behov, som sikkerhetskrav. Her vil et lukket system med maskin- og programvare typisk være avsatt til den enkelte kunden eller kundegruppa. Dette kan være en forutsetning for høy sikkerhet og valgfrihet for kunden. Privat sky gir ikke de samme stordriftsfordelene som i en allmenn sky.
- Allmenn sky (public cloud) er skytjenester som er delt med andre, eventuelt tilgjengelig for alle på det åpne markedet. Ofte tilbys standardiserte løsninger som er like for alle kunder. De største leverandørene er Google, Amazon og Microsoft. En allmenn sky kan være eid, driftet og vedlikeholdt av private eller offentlige virksomheter, eller i kombinasjon.
- Hybrid sky («hybrid cloud») er en kombinasjon av privat, gruppe eller allmenn sky som er integrert og samhandler på tvers gjennom standardiserte eller proprietære protokoller. Uttrykket brukes også om kombinasjoner av lokale IT-systemer og skytjenester.

Det er også vanlig at en kunde benytter flere skytjenester, gjerne både allmenne og private, til ulike formål uten at disse er koblet samme i en hybrid sky, såkalt multicloud. Store offentlige virksomheter benytter gjerne flere skytjenester med ulike leveransemodeller, i tillegg til egne lokale systemer. I en undersøkelse blant statlige virksomheter (A2, 2021) fremgår det at en større andel bruker allmenne skytjenester, enn private og hybride skyløsninger. 29 prosent oppgir at de i stor grad eller kun bruker allmenne skyløsninger, mot under halvparten av dette for private og hybride løsninger.

[1] Privat og allmenn/offentlig sky henviser i denne sammenhengen til tilgang og må ikke forveksles med skillet mellom privat og offentlig sektor. Skytjenester som benyttes eksklusivt av én offentlig virksomhet omtales dermed som «privat sky» uavhengig av om det benyttes leverandører i privat sektor eller ikke.

Skytjenester innebærer i praksis en form for tjenesteutsetting, men de ovennevnte tjeneste- og leveransemodellene kan alle benyttes uavhengig av hvorvidt en virksomhet i hovedsak drifter sin egen IKT med bruk av interne ressurser, benytter private leverandører for IT-drift og forvaltning eller benytter statlige eller kommunale leverandører av IT-driftstjenester, eksempelvis departementenes servicesenter, Politiets IKT-tjenester eller Statsforvalterens fellestjenester. Bestilling og leveranse av skytjenester kan dermed enten gjøres av virksomheten selv direkte til skyleverandør som Microsoft, Google eller Amazon Web Services, eller med en tjenesteleverandør som mellomledd. Det er virksomhetene som kun benytter private leverandører som i størst grad benytter allmenne skyløsninger (A2, 2021, s. 49).

I den nasjonale strategien for skytjenester (KMD, 2016) trekkes allmenne skytjenester frem som et godt alternativ for systemer som ikke er virksomhetskritiske eller inneholder informasjon som må lagres lokalt, og for sikkerhetskopier. En del informasjon som av ulike årsaker ikke bør behandles i den allmenne skyen, eksempelvis data som ikke er lovlig å lagre i utlandet, særlig virksomhetskritisk informasjon eller systemer som ikke tåler forsinkelse eller risiko for bortfall av tjenesten.

Nasjonale skyløsninger som brukes eksklusivt av offentlig forvaltning, eksempelvis skytjenestene som eies og drives av staten i Tyskland, Nederland, Danmark, er å regne som gruppeskyer. NSM anbefalte i sin utredning av muligheten for en statlig driftet skytjeneste med høyt sikkerhetsnivå at denne bør utformes som en gruppesky (NSM, 2016, s. 11).

2.2 Hvordan begrunnes overgangen til skytjenester i offentlig sektor

Norges nasjonale skytjenestestrategi (KMD, 2016) begrunner ønsket om overgang til skytjenester med følgende fordeler: Økonomiske innsparinger, skalering, trygghet, energieffektivitet, fleksibilitet og innovasjon. Strategien omhandler «først og fremst problemstillingar knytte til bruk av *allmenne skytenester*» (KMD, s. 9). Disse fordelene vil likevel gjelde – noen i større og andre mindre grad – også for en nasjonal sky som eies og/eller driftes av offentlige myndigheter.

Skalering

En grunnleggende fordel med skytjenester er skalering og stordriftsfordeler. Allmenne skytjenester har en kapasitet for lagring og prosessering av data som i praksis kan oppleves som ubegrenset fra kundens side. Virksomheten trenger dermed ikke bekymre seg for om for at tjenesten overbelastes ved uventet høy trafikk eller periodiske topper. Dersom en tjeneste utvides til nye brukergrupper eller med nye funksjoner kan nødvendig kapasitet skaffes nærmest umiddelbart. Skalering henger også tett sammen med økonomi, da utgangspunktet for at skytjenester kan være kostnadseffektive er betydelige stordriftsfordeler. De ledende leverandørene av allmenne skytjenester oppnår dette gjennom gigantiske datasentre, globale nettverk og store utviklings- og sikkerhetsmiljøer. Slike stordriftsfordeler vil nødvendigvis være mindre for privat sky/gruppesky med lokasjonskrav, men kan fortsatt være betydelige sammenliknet med virksomhetsintern IT-drift. En nasjonal sky vil eksempelvis kunne gi mange av de samme fordelene for kunden med tanke på kapasitet, skalering og energieffektivitet, samtidig som det kan gi kostnadsbesparelser sammenliknet med virksomhetsinterne løsninger.

Økonomi

Økonomiske innsparinger blir gjerne trukket frem som den største fordelen med bruk av skytjenester. Dette har vært hovedmotivasjonen i mange av landene som har etablert en strategi der innkjøp av skytjenester i markedet spiller en viktig rolle, eksempelvis for Storbritannias «cloud first» politikk. Det samme gjelder til dels også for Norges strategi for skytjenester, som anbefaler offentlige virksomheter å velge skytjenester blant annet av økonomiske hensyn:

> Skytenester skal vurderast på linje med andre løysingar [… og når] skytenester gir den mest hensiktsmessige og kostnadseffektive løysinga […] bør ein velje å bruke skytenester. (KMD, 2016, s. 25)

Den norske skytjenestestrategien legger stor vekt på at bruk av skytjenester kan gi innsparinger ved at det brukes mindre på lokal infrastruktur, vedlikehold, administrasjon og programvarelisenser. Betaling for bruk som medfører at man slipper å betale for mer datakraft, lagring og programvarelisenser «enn ein treng til kvar tid» (KMD, 2016, s. 9). Kostnadene blir dermed også mer transparente. I stortingsmelding nr. 27 (2015-2016) heter det tilsvarende at

> Skytjenestenes skalerbarhet og 'betal for det du bruker-prinsippet' kan være gode løsninger for kjøpere av IKT som ser etter kostnadseffektive løsninger.

Det vil likevel langt fra alltid være lønnsomt for offentlige virksomheter å benytte allmenne skytjenester. Eksempelvis viste flere av kommunene og de statlige virksomhetene Fafo intervjuet om sourcingstragier (Seip, 2020) til at allmenne skytjenester kunne være dyrt, særlig for lagring og nedlasting av store datamengder, ved behov for lisenser til et stort antall brukere eller ved at abonnementsmodeller som gjør prinsippet om betaling etter bruk til en sannhet med modifikasjoner. Besparelser oppnås særlig for tjenester som krever mye datakraft i korte, avgrensede perioder, eller for mindre virksomheter som ønsker tilgang til den nyeste teknologien uten å ha ressurser til å kontinuerlig oppgradere og videreutvikle egen infrastruktur, programvare og kompetanse.

En nasjonal sikker sky vil med sannsynlighet ha et noe høyere kostnadsnivå enn selvkost hos de ledende internasjonale skyleverandørene, da stordriftsfordelene som gjør skytjenestene fra amerikanske «hyperscalere» som Amazon, Google og Microsoft attraktive nødvendigvis vil være mindre. En vil dermed vanskelig kunne se kostnadsbesparelser sammenliknet med disse i alle tilfeller. Samtidig kan finansierings- og faktureringsmodeller tilpasses bedre til offentlige virksomheters behov, og det er ikke gitt at kostnadsnivået for brukerne eller skattebetalerne alltid vil være høyere.

For data som i dag *ikke* er tillatt eller ønskelig å overføre til allmenne skytjenester vil det dessuten være tilstrekkelig at en nasjonal sky er konkurransedyktig sammenliknet med interne IKT-systemer, eller sekundært med kommersielle private skytjenester dersom disse kan oppfylle nødvendige krav til sikkerhet og personvern. En nasjonal sky vil samtidig være en investering i sikkerhet, personvern og kompetansebygging i Norge. Avhengig av finansieringsmodell vil det også være mulig å gi incentiver til at offentlige virksomheter til å ta i bruk en slik løsning. Erfaringer fra andre land, herunder Nederland og Tyskland, indikerer også at det i noen tilfeller kan gi betydelige besparelser å konsolidere eksisterende IKT-infrastruktur og datasentre i forvaltningen for å oppnå stordriftsfordeler (se kapittel 5).

Energieffektivitet

Skytjenester som kjører på maskinvare lokalisert i store datasentre er en vei til mer energieffektiv og klimavennlig IT-drift. Stordriftsfordeler ved samlokalisering av maskinvare for mange kunder og effektiv kjøling gjør at datasentrene kan levere datakraft med markant mindre strømforbruk. Dette gjelder allmenne skytjenester, men vil også være tilfelle for en nasjonal skyløsning av en viss størrelse. Krav om databehandling i Norge kan potensielt gjøre skytjenester mer klimavennlige, da Norge har svært gode forutsetninger både for effektiv kjøling og tilgang til grønn elektrisitet.

Fleksibilitet

Skytjenester kan gi enkel tilgang til avanserte tjenester og maskinvare via nett, fra ulike klienter som mobil, nettbrett og PC. Tilgjengelighet fra ulike lokasjoner og ved bruk av private enheter kan være verdifullt, eksempelvis ved bruk av hjemmekontor. I mange virksomheter tar ansatte uautorisert i bruk forbrukerrettede skytjenester for å kunne ha en fleksibel arbeidshverdag, noe KMD (2016, s. 11) peker på som en sikkerhetsrisiko siden sluttbrukeravtalene ofte gir leverandørene vide fullmakter med hva de kan gjøre med data fra kundene. Å flytte denne type bruk over på sikre løsninger på en nasjonal skytjeneste vil åpenbart innebære betydelig styrket datasikkerhet og personvern, men også allmenne skytjenester kjøpt inn av virksomheten vil representere en vesentlig forbedring. Den nasjonale skytjenestestrategien peker også på at overgang til skytjenester vil ha konsekvenser for arbeidsoppgavene i offentlige virksomheter som kan miste lokal IT-kompetanse, men samtidig frigjøre ressurser til planlegging og tjenesteutvikling. Lokalt vil effektene være tilsvarende ved overgang til en nasjonal skytjeneste, men dersom en slik løsning baserer seg helt eller delvis på at staten selv drifter systemene vil det samtidig innebære at det offentlige bygger sterke sentrale kompetansemiljøer. Sentraliserte datasentre/driftsenheter kan også overta IT-ansatte ved virksomhetsoverdragelser, noe det finnes eksempler på blant annet fra Nederland.

Innovasjon

Skytjenester kan fremme tjenesteutvikling og innovasjon i offentlig sektor ved å redusere kostnader og andre utfordringer knyttet til utvikling, lansering og skalering av nye applikasjoner og tjenester. Skytjenester kan også gi enkel tilgang til avanserte utviklerverktøy, moderne infrastruktur og testmiljøer, og gjøre det enklere å starte opp pilotprosjekter og teste nye løsninger. Behovet for å investere tungt i egen maskinvare og programvarelisenser blir mindre. Ved lansering av en ny nettbasert tjeneste kan skybasert infrastruktur raskt skaleres opp eller ned etter behov, noe som reduserer risikoen ved infrastrukturinvesteringer. I sum vil dette gjøre innovasjon og utvikling enklere, særlig når det gjelder innbyggerrettede og nettbasert tjenester. KMD trekker frem at dette særlig gjelder kommunene, som ofte har begrensede ressurser til tjenesteutvikling.

Spredning av innovasjoner er tilsvarende viktig; ofte vil et passende verktøy, applikasjon eller tjeneste allerede være utviklet. På den annen side er det ikke gitt at slike løsninger møter kravene til datasikkerhet og personvern, og tjenestene vil sjelden være skreddersydd til behovene til eksempelvis en mellomstor norsk kommune. Her kan en nasjonal skytjeneste ha et stort fortrinn, dersom denne settes opp på en måte som gjør at brukerne kan dele, gjenbruke og skalere applikasjoner og løsninger på tvers av ulike offentlige virksomheter. På dette området har den nye tyske skytjenestestrategien (IT-Planungsrat, 2021a) store ambisjoner (se kapittel 5.1): Målet er

at private skyer og gruppeskyer i hele offentlig sektor – nasjonalt, delstatlig og lokalt – skal bygges opp slik at de er kompatible med hverandre og gjør det mulig å gjenbruke, skalere og videreutvikle applikasjoner fra andre offentlige virksomheter. Visjonen er at en hvilken som helst offentlig virksomhet skal kunne gå inn på plattformen, søke etter en passende tjeneste og ta denne i bruk, uten vesentlige tekniske eller lisensmessige hindringer. Slike løsninger kan motvirke utvikling av mange parallelle og inkompatible systemer i offentlig sektor og gi store kostnadsbesparelser og effektivitetsgevinster.

Sikkerhet

Ifølge Nasjonal sikkerhetsmyndighet vil tjenesteutsetting til allmenne skytjenester som Microsoft, Amazon eller Google for de fleste virksomheter ha en positiv innvirkning på datasikkerheten: «Skyløsninger er ofte basert på moderne teknologi med innebygde sikkerhetsmekanismer og leverandørene har kapasitet til nødvendig vedlikehold. Kjøp av slike tjenester kan være bedre enn å utvikle og vedlikeholde de selv 'in house'», heter det i anbefalingen fra NSM (2020b). Utdaterte systemer og «teknisk gjeld» kan fases ut, og virksomheten får tilgang til sikker infrastruktur og profesjonelle sikkerhetsmiljøer. Store datasentre har typisk god fysisk sikring, streng adgangskontroll og sertifiseres etter sikkerhetsnivå. Ved bruk av programvare som tjeneste (SaaS) vil skyleverandøren også sørge for kontinuerlige sikkerhetsoppdateringer og høy oppetid. Sikkerhetskopiering og at data lagres flere steder kan også bidra positivt. Bruk av skytjenester kan bidra til å redusere risiko, spesielt for mindre virksomheter som ikke har kompetanse eller ressurser til digitalt sikkerhetsarbeid selv. NSM er positive til overgang til skytjenester såfremt virksomheten gjør gode vurderinger i forkant av beslutningen (NSM, 2020a, s. 31).

I den norske skytjenestestrategien understrekes det at allmenne skytjenester ikke gir tilstrekkelig sikkerhet for alle formål, og at virksomheter må vurdere om de har informasjon som bør sikres særskilt eller er underlagt sikkerhetsloven og krav om håndtering i Norge. Det vises til at slike vurderinger bør gjøres også av virksomheter som ikke er underlagt sikkerhetsloven og at informasjon som i utgangspunktet ikke er skjermingsverdig likevel kan være det «om han blir lagra i eit felles datasenter eller ei skyteneste der informasjonen til fleire samfunnsfunksjonar er samla. Då vil skadepotensialet ved tap av den samla informasjonen kunne få innverknad på den nasjonale tryggleiken» (KMD, 2016, s. 11). NSM anbefaler at bruk av skytjenester for noen virksomheter bør vurderes opp mot behov for nasjonal kontroll og krisespennet fred, krise, konflikt og krig, slik at det i noen tilfeller bør stilles større krav til robusthet og tilgjengelighet enn det som vanligvis tilbys i kommersielle allmenne skytjenester (NSM, 2020a, s. 33). Strategien sier også at informasjonssystem som behandler gradert og skjermingsverdig informasjon, inkludert informasjon som er omfattet av beslutningsinstruksen, må i utgangspunktet være lokalisert i Norge. Unntak må godkjennes av NSM.

En nasjonal sky vil kunne ha klare sikkerhetsmessige fortrinn sammenliknet med allmenne skytjenester. Datasikkerheten, forstått som konfidensialitet, integritet og tilgjengelighet, vil kunne økes ved at datasentre og annen infrastruktur lokaliseres i Norge, underlegges statlig kontroll og eventuelt driftes helt eller delvis av det offentlige. I tillegg kan det spesifiseres tekniske og fysiske krav tilpasset ønsket sikkerhetsnivå. En nasjonal skyløsning vil også fjerne juridisk risiko knyttet til at datasentre eller leverandører er underlagt andre lands jurisdiksjon og dermed kan bli gjenstand for innsyn fra utenlandske myndigheter, en bekymring som særlig gjelder USAs lovgivning. Hensynet til sikkerhet og personvernhensyn har vært avgjørende for

europeiske land som har valgt å etablere nasjonale skyløsninger, og står helt sentralt i debatten rundt digital suverenitet (se kapittel 4 og 5).

2.3 Omfang og behov

Offentlige virksomheter tar i økende grad i bruk skytjenester. Dette er i tråd med politiske signaler, herunder nasjonal strategi for skytjenester og Digitaliseringsrundskrivet (Kommunal- og moderniseringsdepartementet, 2022), som pålegger at skytjenester vurderes på linje med andre løsninger når virksomhetene etablerer eller oppgraderer eksisterende fagsystemer eller digitale tjenester, eller når de endrer eller fornyer avtaler til drift. Den økte bruken av skytjenester i offentlige virksomheter kan endre virksomhetenes drift og måte å operere på. Det kan ha betydning for sikkerheten, hvilken kompetanse virksomhetene trenger, kostnader ved kjøp av tjenester og beslutninger om hvordan IKT skal styres i virksomheten.

Bruk av skytjenester

Difi (2017a) fant i en undersøkelse blant offentlige virksomheter at 80 prosent av de spurte benyttet skytjenester. I en undersøkelse blant statlige virksomheter gjennomført av A2 (2021) for KMD svarer 71 prosent av de 199 spurte statlige virksomhetene at de benytter en eller flere skytjenester. Det stilles ikke krav om at offentlige virksomhetene skal utarbeide egne strategier for bruk av skytjenester, men nesten halvparten at de statlige virksomhetene oppgir at de har.

I staten er det de minste virksomhetene som bruker skytjenester mest; halvparten av virksomhetene med 50 eller færre årsverk svarer at de i stor grad eller kun benytter skytjenester til å drifte og forvalte IKT-tjenester. Blant de store virksomhetene er det mer utbredt med spesialløsninger som ikke er tilrettelagt for å legges i skyen og driftes og forvaltes internt. Hyllevare og kontorstøtteløsninger er tjenestekategorien der skytjenester benyttes i størst grad, fulgt av standardløsninger og IKT-infrastruktur, mens det er noe mindre utbredt for spesialutviklede løsninger. Statsforetakene utmerker seg meg en høy andel som i stor grad benytter skytjenester, mens statlige virksomheter innen forsvar, landbruk, helse og justis og beredskapssektoren i mindre grad oppgir å bruke skytjenester.

Blant statlige virksomheter er allmenne skytjenester for hyllevare og kontorstøtteløsninger, altså programvare som tjeneste, mest utbredt. De minste virksomhetene bruker private skytjenester i størst grad, mens hybride skytjenester er mer utbredt blant store virksomheter. Allmenne skytjenester leveres i all hovedsak av de store, internasjonale teknologigigantene. Av 177 spurte statlige virksomheter som benytter allmenne skytjenester, svarte 160 (90 prosent) at de benytter Microsoft (Azure), mens 32 (18 prosent) svarte Amazon Web Services og 26 (15 prosent) Google Cloud. Private skyløsninger leveres av langt flere ulike tilbydere, herunder flere norske og europeiske selskaper.

Vi har ikke funnet tilsvarende kartlegginger av bruk av skytjenester i kommunal sektor. Det er likevel klart at skytjenester er tatt i bruk i stor skala i norske kommuner og fylkeskommune, og også her ser bruken ut til å være økende. En undersøkelse utført for KS (Føyen Torkildsen, 2015) som ble besvart av 16 kommuner, viste at mange allerede da hadde tatt i bruk skytjenester, særlig innenfor skolesektoren med blant annet Google og Microsoft 365 som leverandører. I undersøkelsen fra Difi (2017a) svarte nesten åtte av ti kommuner at de benyttet skytjenester. Fafos kartlegging av sourcingstrategier i fire kommuner (Seip, 2020) viste at alle hadde tilgang til private eller allmenne skytjenester og flere av informantene forventet økt bruk i tiden

fremover, blant annet gjennom at eldre systemer erstattes av programvare som tjeneste (Saas). For mange kommuner, særlig små og mellomstore, vil allmenne skytjenester kunne gi tilgang til kapasitet og løsninger som ikke er realistisk å drifte i egen regi.

Digitale fellesløsninger og felleskomponenter for offentlig sektor utvikles stadig og flere bruker eller tilbyr skybaserte tjenester. Et eksempel er Fiks-plattformen som utvikles og forvaltes av KS.

> FIKS-plattformen tilbyr kommuner og andre offentlige virksomheter en rekke felleskomponenter og tjenester, både egenutviklede og allerede etablerte nasjonale felleskomponenter. Plattformen skal i hovedsak levere «skybaserte applikasjonstjenester som er helhetlige og modulbaserte og i størst mulig grad sektoruavhengige». (KS, 2020:16) Fiks-plattformen har en rekke tjenester innen deling og transport av data og fagløsninger, eksempelvis finnes det tjenester for smittesporing, bekymringsmelding til barnevernet, kjøretøyregistrering og mye annet som er felles for alle kommunene. Plattformen er basert på en arkitektur med Platform as a Service (PaaS) og mikrotjenester. Fiks-plattformen utvikles og eies av KS, mens driften av plattformen leveres som en tjeneste fra Intility, som kjører plattformen fra et datasenter i Norge. Plattformen kjører Openshift som PaaS til å hoste microtjenestene. (KS, 2020)

Hvor lagres data?

Bruken av private leverandører og allmenne skytjenester medfører at det ikke er uvanlig at offentlige virksomheter lagrer data utenfor Norge. I undersøkelsen blant statlige virksomheter utført av A2 oppgir 26 prosent av virksomhetene at data fra hyllevare og kontorstøtteløsninger, typisk levert som allmenne skytjenester, bare lagres i Norge, mens tilsvarende andel er 38 prosent for standardløsninger, 45 prosent for spesialutviklede løsninger og 53 prosent for IKT-infrastruktur. Nesten én av fire virksomheter lagrer i stor grad data fra hyllevare og kontorstøtteløsninger utenfor Norge, mot under 10 prosent for IKT-infrastruktur, standardløsninger og spesialutviklede løsninger (A2, 2021, s. 47). Majoriteten av data er dermed lagret i Norge. Bruk av allmenne skytjenester levert av utenlandske selskaper kan likevel medføre uklarhet om hvor data og sikkerhetskopier til enhver tid befinner seg, hvorvidt den kan være underlagt andre lands jurisdiksjon og spørsmål knyttet til mulig tilgang til data fra utlandet.

En kartlegging av datasentre i Norge fra 2015 viser til at det er vanskelig å finne små og mellomstore kommuner som ikke samarbeider om IKT-drift, og anslår at norske kommuner og fylkeskommuner til sammen har rundt 100 datasentre. Studiens datagrunnlag for statlige virksomheter gjorde det vanskeligere å estimere antall datasentre for slike virksomheter, det antas mellom 50 og 100. I sum betyr det at det offentlige Norge hadde 150 til 200 datasentre i drift i 2015.

2.4 Forventninger og behov

Fortsatt sterk vekst i bruk av skyløsninger er å forvente. A2s undersøkelse blant statlige virksomheter viser at det forventes fremtidig vekst i bruk av de allmenne skytjenestene. 43 prosent av virksomhetene har i stor eller svært stor grad økt bruk av allmenne skyløsninger for egne systemer, og 32 prosent av leverandørene forventer det samme for systemene de drifter for kundene. Virksomhetene forventer en stor vekst i bruk av allmenne skyløsninger, men også for private og hybride løsninger.

Statsforetakene og virksomheter som benytter private IT-leverandører tror særlig på vekst, men også de store statlige IKT-leverandørene forventer en slik utvikling.

NSM konkluderte i rapporten «Sikker sky» (omtalt nedenfor) med at det er tydelig behov for en offentlig skytjeneste og at denne kunne gitt store gevinster ved å øke effektiviteten og informasjonssikkerheten (NSM, 2017, s. 14). Difi fant i sin relaterte utredning av kundegrunnlaget for en sikker skytjeneste at i om lag 60 prosent av virksomhetene som oppga at de lagrer skjermingsverdig informasjon[2] elektronisk ønsker å ta i bruk sikre skytjenester, under forutsetningen av at en slik skytjeneste var godkjent av NSM (Difi, 2017a, s. 4).

Lagringskapasitet i skyen, samhandlingsrom, epost og kontorstøtte er tjenester flest ser som aktuelle å sette ut i en sikker sky, men også skjemaløsninger, driftsplattform, regnskap eller timeregistrering er aktuelle å sette ut, ifølge undersøkelsen. Den viser med andre ord at det allerede i 2017 var betydelig etterspørsel etter en slik skyløsning, fra et bredt spekter av offentlige virksomheter i både statlig og kommunal sektor, og at virksomhetene ser et slikt behov for en lang rekke ulike tjenester.

Samlet peker de ovennevnte undersøkelsene og utviklingen i bruk av skytjenester mot at offentlige virksomheter i stor grad forventer og ønsker å ta i bruk skytjenester på nye områder, og at dette også gjelder behandling av skjermingsverdig informasjon dersom en nasjonal sikker sky gjør dette mulig. Med utgangspunkt i virksomhetenes behov vil en sikker nasjonal skytjeneste kunne utfylle allmenne skytjenester ved å gjøre det mulig å legge data i skyen som per i dag vurderes uegnet til dette. En slik løsning vil da i hovedsak kunne erstatte virksomhetsintern IT og private skyløsninger. For politiske beslutningstakere vil valget dermed ikke nødvendigvis stå mellom allmenne skytjenester *eller* en nasjonal sky, men handle om ulike modeller for en slik tjeneste, hvilke data og løsninger den skal omfatte og i hvilken grad virksomhetene står fritt til å velge løsninger.

[2] Begrepet «skjermingsverdig informasjon» brukes som en samlebetegnelse på informasjon som skal beskyttes for å ivareta nasjonale sikkerhetsinteresser. NSM forklarer det slik: «Informasjon som er skjermingsverdig skal beskyttes med et forsvarlig sikkerhetsnivå (Med forsvarlig sikkerhetsnivå menes kombinasjonen av relevante sikkerhetstiltak). Informasjon som er skjermingsverdig av konfidensialitetshensyn skal sikkerhetsgraderes.»

3 Hvor står vi? Norsk strategi for skytjenester og utredning av statlige alternativer

3.1 Nasjonal strategi

Potensialet for effektivisering ved overgang til skytjenester har blitt vektlagt i en rekke offentlige dokumenter, som del av en bredere satsing på digitalisering av offentlig sektor. I stortingsmelding nr. 27 (2015–2016) presenterte regjeringen Solberg en overordnet politikk for hvordan Norge kan ta i bruk IKT til samfunnets beste. Målet er en «brukerrettet og effektiv» offentlig forvaltning som skal gi mulighet for verdiskapning og deltakelse. Det legges til grunn en klar ambisjon om å øke bruken av skytjenester i det offentlige: «Skytjenester begynner å bli den dominerende måten å levere IKT-tjenester på, særlig til forbrukere og til næringslivet. Offentlig sektor følger etter» (Meld. St. 27, 2015–2016:13). Den nasjonale strategien for skytjenester, der offentlige virksomheter oppfordres til å bruke skytjenester der dette er mulig: «Skytenester skal vurderast på linje med andre løysingar [... og når] skytenester gir den mest hensiktsmessige og kostnadseffektive løysinga [...] bør ein velje å bruke skytenester» (KMD, 2016:25). Strategien er gjennomgående positiv til skytjenester. Samtidig vises det til at offentlig sektor har et spesielt behov, avhengig av hvilken type informasjon som behandles, for kontroll over hvem som forvalter informasjon og hvor dette gjøres. Kontrollmekanismene som anbefales i strategien er bruk av standardkontrakter og sertifiseringer i tillegg til prekvalifisering av leverandører. Dette er fulgt opp i form av etablering av den offentlige markedsplassen for skytjenester, omtalt under. Strategien nevner samtidig muligheten for at sentrale myndigheter kan «inngå avtalar på vegner av offentleg sektor med leverandører av datasenter/skytjenester» som oppfyller de strengeste sikkerhetskravene, samt muligheten for at sentrale styresmakter selv etablerer ett eller flere datasenter som tilfredsstiller disse kravene (KMD, 2016 s. 26). Både muligheten for å opprette nasjonale datasentre/skytjenester i egenregi og muligheten for å kjøpe tilsvarende i markedet avvises derimot kontant med henvisning til en undersøkelse utført av Nexia Management Consulting for KMD (2015). Konklusjonen er at: «det ikkje [er] avdekka behov for at sentrale styresmakter forhandlar fram felles avtalar om datasenterdrift, eller etablerer eit felles datasenter for statleg- eller offentleg sektor. Desse alternativa er derfor ikkje drøfta nærare i strategien.» (KMD, 2016 s. 26) Bakgrunnen for denne avgjørelsen fremstår noe uklar, da den henviste undersøkelsen i hovedsak er deskriptiv og ikke direkte vurderer om eller avviser at sentrale myndigheter bestiller eller selv drifter skytjenester.[3]

[3] Nexia (2015) skriver at «Det ligger utenfor denne studiens mandat å gjøre en grundig og helhetlig analyse av hvordan sentrale myndigheter kan legge til rette for mer IKT-samarbeid, ytterligere datasenterkonsolidering og økt bruk av skytjenester i kommuner, fylkeskommuner og statlige virksomheter», men advarer mot å velge «*enten* en «bottom-up»-tilnærming eller en «topdown»-tilnærming» og anbefaler konsolidering basert på eksisterende samarbeid. Samtidig understrekes det at

Digitaliseringsrundskrivet (KMD, 2022), som oppdateres jevnlig, følger opp skytjenestestrategien og stiller krav til statlige virksomheter som etablerer nye fagsystemer eller digitale tjenester, eller som oppgraderer eksisterende systemer eller avtaler, om at de «skal vurdere» bruk av skytjenester på linje med andre løsninger, og at disse bør velges «Når det ikke foreligger spesielle hindringer for å ta i bruk skytjenester, og slike tjenester gir den mest hensiktsmessige og kostnadseffektive løsningen». Spesielle hindringer kan være særlige krav til sikkerhetsvurderinger, eller at skytjenester ikke vil være kostnadseffektivt.

Markedsplass for skytjenester

I den nasjonale skytjenestestrategien fremgår det at «Regjeringa ønsker å etablere mekanismar som kan hjelpe verksemdene å sikre nødvendig kontroll gjennom gode innkjøp og kontraktar som tilfredsstiller offentlege krav, og oppfølging av dei inngåtte kontraktane» (KMD, 2016 s. 27).

Regjeringen gjentok ambisjonen i Jeløya-plattformen, og arbeidet med å etablere en markedsplass for skytjenester startet i 2018. Løsningen er inspirert av Storbritannia, der det ble etablert en egen markedsplass for skytjenester, Cloud Store – nå G-Cloud og tilhørende Digital Marketplace (Difi, 2018). Målet er å gjøre det enklere for virksomhetene å anskaffe sikre, lovlige og kostnadseffektive skytjenester. Markedsplassen inneholder en voksende samling avtaler som offentlige virksomheter kan bruke. Fellesavtaler skal forenkle gjennomføring og oppfølging av avtalene for virksomhetene og dekker mange ulike skytjenester. Avtalene er frivillige å bruke og kan benyttes av både statlige, kommunale og andre offentlige virksomheter. En del av arbeidet består i å introdusere en kontraktsfestet «referansearkitektur» basert på NSMs grunnprinsipper og NIST sikkerhetsstandarder og øke sikkerhetsnivået ved bruk av kontrakter. Videre skal Markedsplassen gi veiledning om overgang til skytjenester og anskaffelsesprosessen, samt om informasjonssikkerhet og personvern (DFØ, 2022). På sikt skal markedsplassen også inneholde et tjenesteregister der tilbyderne kan registrere sine tjenester. Plattformen åpnet for registrering av leverandører i februar 2022 og skal i første omgang gi en oversikt over programvare i skyen (SaaS). Det skal videre jobbes med utvikling og drift i skyen (IaaS og PaaS) og konsulenttjenester (DFØ, 2021).

3.2 Utredninger av nasjonal skyløsning

Den norske strategien for bruk av skytjenester baserer seg i stor grad på markedet, med oppfordring til bruk av allmenne skytjenester og den offentlige markedsplassen for skytjenester. Samtidig har den alternative tilnærmingen med datasentre og skytjenester under statlig kontroll vært vurdert over en lengre periode. En eventuell nasjonal sky anses av norske myndigheter primært å være aktuelt for skjermingsverdig informasjon som ikke egner seg til behandling i allmenne skytjenester.

Som oppfølging av arbeidet rundt den nasjonale skytjenestestrategien har NSM og digitaliseringsdirektoratet vurdert handlingsrommet for en sikker skytjeneste og mulig innretning av denne. NSMs første rapport fra 2016 ble fulgt opp i 2017 med vurderinger av hvilken type informasjon som bør omfattes av en slik løsning, hvor stort kundegrunnlaget er og aktuelle markedsaktører, samt handlingsrom i henhold til

skytjenester «byr på mange utfordringer, særlig i forhold til sikkerhetsaspekter knyttet til prosessering og lagring av personsensitiv informasjon.» (s.5)

anskaffelsesregelverket[4]. Utredningsarbeidet førte ikke umiddelbart til praktiske endringer, men Støre-regjeringen har signalisert en mer aktiv tilnærming, og i tråd med vedtak i Stortinget har Justisdepartementet i samarbeid med KMD og FD igangsatt en Konseptvalgutredning (KVU) for etablering av en nasjonal skytjeneste for ugradert, skjermingsverdig informasjon, som skal leveres i desember 2022.

Utredningsarbeidet har tatt utgangspunkt i at en eventuell nasjonal skyløsning vil komme i tillegg til og ikke som en erstatning for den gjeldende strategien og markedsplassen for skytjenester. I mandatet for den pågående konseptvalgutredningen forklares det at behovet for en sikker skytjeneste kan deles opp i tre deler; behandling og lagring av 1) lavgradert informasjon, 2) ugradert, skjermingsverdig informasjon og 3) ugradert, annen informasjon. Behandling og lagring av *lavgradert informasjon* i statsforvaltningen anses som løst gjennom etablering av Forsvarsdepartementets tonivå-plattform, herunder Nasjonalt begrenset nett (NBN). Tonivå-plattformen er utviklet for behandling av lavgradert informasjon i statsforvaltningen og er besluttet innført som felles IKT-løsning for Statsministerens kontor, departementene, utenriksstasjonene og Departementenes sikkerhets- og serviceorganisasjon, samt andre statlige virksomheter etter behov. Behandling og lagring av *ugradert, annen informasjon* anses ifølge mandatet «løst gjennom DFØs Markedsplass for skytjenester for offentlig sektor». En nasjonal skyløsning skal med andre ord ikke konkurrere med markedsrettede løsninger, men være et alternativ ved behandling av informasjon som ikke er egnet for slike skytjenester.

Sikker Sky

I forbindelse med lansering av den nasjonale strategien for skytjenester i 2016 fikk Justis- og beredskapsdepartementet, i samråd med Kommunal- og moderniseringsdepartementet og Forsvarsdepartementet, i oppdrag å «igangsette et arbeid for å vurdere etablering av en statlig driftet skytjeneste med høyt sikkerhetsnivå, slik at også sentrale myndigheter med særskilte sikkerhetsbehov kan utnytte mulighetene til effektivisering som skytjenester gir» (NSM, 2016, s. 1). Justis- og beredskapsdepartementet ga NSM oppdraget med å utrede dette, og alternative driftsløsninger for skytjenester. Rapporten skisserer mulig innretning av en statlig skytjeneste for både lavgradert (begrenset, fortrolig/strengt fortrolig) og ugradert, sensitiv informasjon.

NSM konkluderte med at det er mulig å etablere en sikker skyløsning for sentrale myndigheter, som overholder sikkerhetskravene som sikkerhetsloven med forskrift krever. Modellen som ble anbefalt var en partisjonert løsning der sensitiv informasjon behandles adskilt, men på tilsvarende måte som lavgradert informasjon, med en del felles krav til operasjonsmåte, sikkerhetsarkitektur og risikostyring, og med felles tilgang for sluttbruker. For gradert informasjon vil sikkerhetskravene følge av sikkerhetsloven, herunder krav innen fysisk og systemteknisk sikkerhet, kryptering, internkontroll, personellsikkerhet og anskaffelser. For ugradert, sensitiv informasjon anbefales det å følge en liknende tilnærming i tillegg til etablerte industristandarder og sertifiseringer som ISO 27000- serien.

[4] Utredningsarbeidet resulterte i rapportene Sikker sky (NSM 2016); Sikker sky (fase 2) (NSM 2017); Sikker sky (fase 2 del 2) (Difi, 2017a); og Vurdering av hvorvidt anskaffelsesregelverket (og tilknyttet EØS-lovgivning) legger begrensninger på offentlige virksomheters mulighet til å stille krav til nasjonal lagring og behandling av data. (Difi, 2017b). Rapportene er unntatt offentlighet, Fafo har søkt om og fått innvilget innsyn.

Statlig eller privat drift?

NSM tok også for seg ulike mulige eierskapsmodeller, herunder 1) statlig eid og driftet; 2) statlig eid men privat driftet og; 3) statlig kontrollert, men privat eid og driftet. Alle tre modeller vurderes realiserbare. NSM anbefaler i rapporten en statlig kontrollert, men privat eid og driftet løsning. Dette begrunnes dels med «Regjeringens ønske om økt tjenesteutsetting (blant annet IKT) til private aktører» (NSM, 2016, s. 5), dels med henvisning til vurderinger i rapporten fra Nexia (2015) om at IKT-miljøene i offentlig sektor har begrensede ressurser til å bruke IKT-styringsmodeller og en bekymring om at dette «kan medføre redusert kvalitet på sikkerhetsstyring, utarbeidelse av risiko- og verdivurderinger og oppfølging av inngåtte avtaler» (NSM, 2016, s. 5).

Den anbefalte løsningen vil innebære at staten er bestiller, kravstiller, godkjenner og kontrollør for en skyplattform som eies, forvaltes og driftes av en privat aktør. Mellomløsningen med en statlig eid, men privat driftet skyplattform innebærer at staten har en tilsvarende rolle som bestiller og kravstiller, men i tillegg styrer investeringene, godkjenner alt som skal implementeres på plattformen og eier eller har kontroll på driftsmiljøer og datasentre. En statlig eid og driftet plattform vil innebære at har staten har full kontroll med alle involverte parter i skyplattformen og i leveranse av skytjenestene. Statlige virksomheter vil da være leverandører i tillegg til at staten er kravstiller, bestiller, godkjenner og kontrollør. NSM vurderer at en slik helstatlig løsning har best forutsetninger for å oppfylle sikkerhetskravene. Når løsningen likevel ikke anbefales vises det til mulige utfordringer med kompetanse og teknologi: «En utfordring kan være å få til en forretningsmodell som er konkurransedyktig og sammenlignbar med utviklingen ellers i «sky-markedet». En slik modell kan lett oppfattes som ineffektiv og lite fleksibel med hensyn til bruk av teknologi og løsninger.» (NSM, 2016, s. 15). Uavhengig av eierskapsmodell anbefales en konsolidering av statens IT-tjenester, slik at det «i sentralforvaltningen/departementsfellesskapet bør være ett IKT-miljø som har ansvaret for IKT-løsningene, herunder inkludert «sikker sky»-løsningen» (NSM).

Som andre fase av «sikker sky» ba JD og FD NSM og Difi om å utrede behov og kundegrunnlag for en sikker skytjeneste, hvorvidt anskaffelsesregelverket legger begrensninger for valg av løsning og hvilken informasjon, ut over gradert informasjon, en slik løsning bør omfatte. Difis vurdering av begrensninger i anskaffelsesregelverket og tilknyttet EØS-lovgivning konkluderte, i kontrast til anbefalingen fra NSM, med at regelverket legger sterke begrensninger på offentlige virksomheters mulighet til å stille krav til nasjonal lagring og behandling av data ved bruk av private tilbydere (Difi, 2017b). Det vises til at EØS-avtalens artikkel 36.1 som medfører at det i utgangspunktet ikke kan diskrimineres mellom tjenesteleverandører som er etablert i Norge og andre EØS-medlemsstater. Krav om lagring i Norge eller norsk leverandør vil dermed være diskriminerende og ulovlig. Difi vurderer flere mulig unntak, og viser blant annet til at Sikkerhetsloven åpner for restriksjoner knyttet til sikkerhetsgraderte anskaffelser. Vurderingen konkluderer med at «en løsning som forutsetter nasjonal lagring av «sikker sky» sannsynligvis ikke er lovlig i henhold til anskaffelsesretten dersom løsningen også omfatter ugradert informasjon.» (Difi, 2017b). Det bemerkes avslutningsvis at dette ikke vil være til hinder for en statlig eiet og driftet skyløsning: «Dersom en ytelse leveres i egenregi, foreligger det ingen kontrakt i anskaffelsesrettslig forstand, og anskaffelsesregelverket kommer ikke til anvendelse. Det vil altså være fullt mulig for staten å etablere en «sikker sky», men denne kan, etter dagens regelverk, ikke anskaffes i markedet» (NSM, 2017, s. 14). En slik løsning ble imidlertid ikke vurdert i det videre.

Behov og omfang

NSMs vurdering av kundegrunnlag og aktører konkluderte med at «det er tydelig behov for en offentlig skytjeneste» (NSM, 2016, s. 14). Vurderingen er basert dels på en undersøkelse der NSM spurte Datatilsynet, DSB, Finanstilsynet, Helsedirektoratet, Luftfartstilsynet, Nasjonal kommunikasjonsmyndighet (Nkom), NVE, Petroleumstilsynet og Politidirektoratet om behovet for en sikker skytjeneste og hvilke typer informasjon i deres sektor, eller underlagt deres tilsyn, som kan eller bør inngå i en sikker sky. Respondentene var positive til etablering av en sikker skyløsning og vurderte det slik at denne kunne erstatte tungvinte arbeidsprosesser, informasjonsdeling som gjøres på papir av sikkerhetshensyn, og erstatte virksomhetsinterne IT-systemer som er krevende å vedlikeholde.

NSM vurderte også hvilken informasjon en sikker sky bør inneholde, med utgangspunkt i at løsningen bør tilpasses sensitiv informasjon, forstått som ugradert informasjon som i sin karakter og omfang har et høyt beskyttelsesbehov. Dette kan være informasjon som bør være tilgjengelig dersom en kritisk situasjon skulle oppstå, som har behov for å deles sikkert, som omfatter sensitive prosjekter eller arbeidsprosesser eller som ved sammenstilling blir sensitiv. E-postforsendelser av informasjon unntatt offentlighet av hensyn til personvern, og intern saksforberedelse nevnes særskilt.

Informasjonen de spurte virksomhetene vurderte som sensitive og egnet til behandling i en sikker sky varierte mye, men inkluderte blant annet personopplysninger, operative rutiner, planverk (inkludert beredskapsplaner og beredskapstiltak), tegninger, kartdata, bygnings- og infrastrukturdata, tillatelser (f.eks. for eksplosiver), rapporter og underlag, erfaringsdata, og undersøkelser og granskninger. NSM viser til «flere eksempler på arbeidsprosesser der en sikker skyløsning ville gitt store gevinster» (NSM, 2016, s. 12) og at de tror at det finnes flere eksempler i andre sektorer. En sikker sky vurderes å øke effektiviteten og informasjonssikkerheten gjennom bedre tilgjengelighet, integritet og konfidensialitet. NSM mener at datamengdene som behandles i disse eksemplene ikke er store og dermed ikke vil være dimensjonerende for en skyløsning. Omfanget vil i stedet avhenge av funksjonalitetskrav og antall involverte parter.

Fremfor å foreslå en omforent definisjon eller objektive kriterier for hvilken informasjon som er å regne som sensitiv og/eller egnet for behandling i en sikker sky, foreslår NSM at innslaget for en offentlig skytjeneste sammenstilles med forslag til innslaget for virkeområdet for ny sikkerhetslov. Dette vil si at informasjon bør behandles i en sikker skytjeneste hvis denne omhandler grunnleggende nasjonale funksjoner som er av en slik betydning at bortfall vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser, forstått som suverenitet, territoriell integritet og demokratisk system. NSM mener dermed at «en sikker skytjeneste bør ha som hovedformål å bidra til å trygge nasjonale sikkerhetsinteresser» (NSM, 2016, s. 13), og anbefaler at den i første omgang bør omfatte et begrenset antall systemer og kunne utvides gradvis. Denne avgrensningen fremstår dels som en tilpasning til vurderingen av EØS-regelverket, da sikkerhetsloven kan gi hjemmel for lagring i Norge. Selv om en slik avgrensning vil begrense antall brukere og kundegrunnlaget er det svært mange virksomheter innen for eksempel elektronisk kommunikasjon, helse, kraftforsyning, transport, vannforsyning, politi, forsvar og sentralforvaltningen som er omfattet av sikkerhetsloven. Avgrensningen er likevel en vesentlig innsnevring holdt opp mot den type informasjon NSM diskuterte at løsningen kunne omfatte i den første rapporten, samt kundegrunnlaget identifisert av Difi.

3.3 Konseptvalgutredning for etablering av en Nasjonal skytjeneste

Regjeringspartiene erklærte i Hurdalsplattformen at regjeringen vil «vurdere i hvilke tilfeller staten bør ta eierskap til digital infrastruktur, plattformer, plattformutvikling og standardutvikling» og «Utrede opprettelsen av en statlig skyløsning for lagring av offentlige data som helsedata, finansdata og informasjon om innbyggere og infrastruktur» (2021, s. 15). I mars 2021 fattet Stortinget vedtak om å be regjeringen utrede behov for og etablering av en felles skytjeneste for forvaltningen.[5] Justisdepartementet har i samarbeid med KMD og FD igangsatt en konseptvalgutredning (KVU) for etablering av en nasjonal skytjeneste for ugradert, skjermingsverdig informasjon. I mandatet er det bestemt at KVU-arbeidet skal ha følgende rammebetingelser:

- KVUen skal vurdere og rangere *statsforvaltningens* reelle behov for en nasjonal skytjeneste for behandling og lagring av *ugradert, skjermingsverdig informasjon* (jf. SL §5-1 og §5-2).
- Hvilken type informasjon som anses ugradert, skjermingsverdig skal være en del av KVU-arbeidet. Det skal også vurderes om det er annen ugradert, beskyttelsesverdig informasjon som bør inngå i en nasjonal skytjeneste.
- Virksomheter som allerede omfattes av FDs tonivå-plattform, eller som er besluttet at skal benytte plattformen, er ikke del av KVUen.
- KVUen skal vurdere konseptuelle alternativer for hvordan ugradert, skjermingsverdig informasjon bør behandles og lagres gjennom en nasjonal skytjeneste. Det må fremgå hvordan alternativene kan innrettes og hvilke rammebetingelser som legges til grunn.
- Det skal legges til grunn ulike ambisjonsnivåer for de konseptuelle alternativene, blant annet en minimumsløsning hvor bare absolutte krav tilfredsstilles.
- Det skal vurderes om det finnes eksisterende løsninger eller løsninger som er under planlegging og etablering som vil kunne dekke behovene for en nasjonal skytjeneste.
- De konseptuelle alternativene skal ta utgangspunkt i nasjonal behandling og lagring av ugradert, skjermingsverdig informasjon.
- Vurdering av sikkerhetsutfordringer som kan oppstå om en leverandør er underlagt utenlandske staters jurisdiksjon, skal være del av KVUen.
- Utredningen skal beskrive, drøfte og foreslå hvem som skal ha hvilke roller i de ulike konseptuelle alternativene. Minst ett av alternativene skal være en skytjeneste som eies og driftes av staten selv, men der kompetanse og innovasjonskraft fra det private benyttes.
- Erfaringer fra andre land skal innhentes, vurderes og omtales i utredningen, med særlig vekt på erfaringer av overføringsverdi til norske forhold.

NSM er ansvarlig myndighet og skal etter planen levere KVUen 1. desember 2022. Ekstern kvalitetssikring skal gjennomføres innen 1. juni 2023, før det eventuelt vedtas forprosjekt og senere implementering.

3.4 Vurdering: Et begrenset mandat

Det ligger flere forutsetning for utredningsarbeidet som legger avgjørende føringer. For det første er mandatet for både «sikker sky» i 2016/2017 og det pågående KVU-

[5] Stortingets vedtak nr. 735 av 2. mars 2021

arbeidet avgrenset til skytjenester for *statsforvaltningen*. Dette utelukker i utgangspunktet hele kommunal sektor – kommuner, fylkeskommuner og underliggende virksomheter – som mulige brukere. Løsninger som omfatter eller kan tas i bruk i hele offentlig sektor, som eksempelvis er en ambisjon i den nye tyske skystrategien (omtalt i kapittel 5), er dermed ikke vurdert. Kartleggingene som er gjort av bruk av skytjenester og behovet for en nasjonal skytjeneste viser tydelig at det er behov, men også at behovet er bredt, på tvers av sektorer og bruksområder. Avgrensningen til statsforvaltningen begrunnes ikke, verken i mandatet til KVU eller i tidligere utredningsarbeid. Det vil i mange tilfeller finnes virksomheter i kommunal sektor som kan ha tilsvarende behov for og nytte av en nasjonal skyløsning. Dersom det eksempelvis legges til rette for at helseforetakene kan benytte en statlig skytjeneste for å lagre helsedata og personopplysninger som vurderes som skjermingsverdige, vil det kunne være et tilsvarende behov i kommunehelsetjenesten, samt behov for at disse systemene er kompatible med hverandre. Virksomhetsstørrelse og samordningsbehov tilsier at nytten av en skyløsning kan være betydelig i kommunal sektor, og Difis kartlegging viste at kommunene i utstrakt grad behandler skjermingsverdig informasjon. Avgrensning til statsforvaltningen fremstår dermed noe vilkårlig, antakelig gjort av hensyn til å redusere praktisk og juridisk kompleksitet og antall involverte parter i en innledende fase. Skytjenesters fleksibilitet og skalerbarhet tilsier derimot at det er mulig å utvide omfanget ved behov.

Videre er avgrensningen mot systemer for behandling av gradert informasjon (FDs tonivåplattform) og mot tjenester for annen ikke-sensitiv informasjon betydelig innsnevrende. Særlig avgrensningen mot Markedsplassen for skytjenester, som anses å ivareta behovet til ikke-sensitiv annen informasjon, er av avgjørende betydning for dimensjonering av en eventuell nasjonal sky. Der eksempelvis Tysklands tilnærming bygger på at et prinsipp om at staten skal tilby tjenestene i egen regi i den grad dette er mulig, vil avgrensningen i stedet kunne legge føringer for at det bare er informasjon som er ulovlig å sette ut til allmenne, markedsbaserte skytjenester som bør behandles i en nasjonal sikker sky. NSMs anbefaling om at en sikker skytjeneste bør følge virkeområdet i ny sikkerhetslov og omfatte informasjon som «etter en verdivurdering er av betydning for opprettholdelse av grunnleggende nasjonale funksjoner» kan innsnevre kundegrunnlaget ytterligere. Løsningene som vurderes vil dermed av nødvendighet ha begrenset omfang.

4 Digital suverenitet? Avveininger og valg for skyløsninger i offentlig sektor

Økt bruk av skytjenester i offentlig sektor har aktualisert spørsmål rundt behovet for *digital suverenitet* og kontroll med hvor data lagres og behandles, hvem som har tilgang og eierskap, og tillit til at data behandles på en måte som ivaretar nasjonale interesser og innbyggernes personvern og rettigheter.

Dette kapittelet tar utgangspunkt i den internasjonale debatten rundt digital suverenitet ved bruk av skytjenester og drøfter prinsipielle problemstillinger knyttet til organisering av skytjenester for offentlig sektor, herunder hensyn til personvern og personvernreglement, nasjonal kontroll og lokaliseringskrav til data, datasikkerhet, og relaterte hensyn som leverandøravhengighet og innløsingseffekter, kompetanse og tillit til myndighetene. Avslutningsvis drøftes avveiningen mellom gevinster ved samordning og virksomhetenes autonomi og ansattes medbestemmelse.

4.1 Digital suverenitet

Behovet for *digital suverenitet,* hva dette innebærer og hvordan det kan oppnås har internasjonalt vært gjenstand for debatt i over et tiår[6]. Ikke minst i Frankrike, Tyskland og i EU-systemet er dette blitt et viktig og uttalt politisk mål. Begrepet digital suverenitet har rukket å etablere seg i diskurser om styring og cybersikkerhet, og beskriver ideen om at nasjonal sikkerhet krever en stat som kan hevde sin suverenitet også i det digitale domenet. I forbindelse med skytjenester brukes digital suverenitet gjerne om nasjonal kontroll og eksklusiv jurisdiksjon over data, og det beslektede begrepet *datasuverenitet* kan defineres som «nasjonale myndigheters eksklusive autoritet og kontroll over alle virtuelle offentlige data» Irion, (2012) s. 41, vår oversettelse. Digital suverenitet er samtidig et bredere begrep og blant annet et hovedmål for EUs datastrategi (EU-Kommisjonen, 2020), som skal skape et indre europeisk marked for data. I tyske strategidokumenter defineres digital suverenitet bredt, som «evner og muligheter for individer og institusjoner til å utøve sine roller i den digitale verden autonomt, sikkert og trygt» (IT-Planungsrat, 2021a, s. 3). I praksis assosieres gjerne digital suverenitet med et mål om uavhengighet fra de dominerende teknologigigantene som Amazon, Google og Microsoft, samt kontroll over verdifulle og sensitive data. Dette er et avgjørende rasjonale både for nasjonale skytjenester i statlig regi i flere europeiske land og det nylig lanserte Gaia-X initiativet for en ny skytjenestearkitektur for både offentlig og privat sektor i europeiske land (omtalt nærmere i kapittel 5). EU ønsker å styrke medlemslandenes digitale suverenitet for å redusere avhengigheten av utenlandske leverandører og risikoen ved utenlandsk tilgang til

[6] Hummel mfl., (2021) finner i en gjennomgang av litteraturen totalt 341 publikasjoner som omhandler digital suverenitet, datasuverenitet eller cybersuverenitet og viser at begrepene, i mangel på en omforent definisjon, knyttes til en rekke relaterte konsepter.

kritiske data. Man tar også i betraktning at skyløsninger er en forutsetning for fremgang på viktige teknologiområder som kunstig intelligens.

Offentlig sektors overgang til skytjenester setter spørsmålet om datasuverenitet på spissen: Hvordan kan myndighetene garantere informasjonssikkerheten når data er lagret i skyen? Hvilke konsekvenser kan det få når offentlige IT-systemer er avhengige av utenlandske leverandører eller kjører i datasentre i utlandet? Kan myndighetenes data bli underlagt et annet lands jurisdiksjon? Hvilke aktører kan få tilgang? Og; vil kritiske systemer fungere i kriser, konflikt eller krig?

En gjennomgang fra 2012 viser at dette allerede da stod høyt på agendaen hos myndighetene i flere land (Irion, 2012). Digital suverenitet er altså ikke et nytt konsept, men har blitt aktualisert av et skiftende sikkerhetspolitisk landskap og nye reguleringer som påvirker kontroll over data. I den norske samfunnsdebatten har digital suverenitet og mulige sårbarheter ved skytjenester særlig blitt aktualisert etter Schrems II-dommen, der EU slo fast at sertifiseringsordningen Privacy Shield ikke lenger regnes som gyldig overføringsgrunnlag for personopplysninger mellom Europa og USA. Bakgrunnen er lovgivning som innebærer at USA-baserte skyleverandører kan pålegges å gi amerikanske myndigheter innsyn i dataene de lagrer, uavhengig av hvilket datasenter de lagret i. For europeiske og norske virksomheter har dette ført til at avhengighet av amerikanske leverandører har fått konkrete juridiske og praktiske implikasjoner, som forbud eller anbefalinger om å ikke benytte konkrete tjenester eller leverandører, eller i det minste skapt usikkerhet rundt lovligheten av dataoverføringer.

Digital suverenitet er et hensyn som blir viktigere i politikkutforming for myndighetene i alle land ettersom digitaliseringen av offentlige systemer og tjenester gjør digital suverenitet til en stadig viktigere del av den statlige suvereniteten og selvråderetten, som er bærende prinsipper for nasjonalstaten og folkeretten (Irion, 2012). En nasjonal skyløsning som fullt ut ivaretar digital suverenitet vil sikre at alle data og metadata forblir under én nasjonal jurisdiksjon, forhindrer utenlandsk tilgang og gir et pålitelig miljø for lagring og behandling av data som ikke kan overføres på tvers av landegrenser. Krav til nasjonal lagring og drift av skytjenester i statlig regi bunner typisk i et ønske om å ivareta digital suverenitet. Det er likevel ikke gitt at dette er den eneste modellen som kan ivareta dette hensynet. Ulike konfigurasjoner av eierskapsmodeller, arkitektur og infrastruktur for skytjenester kan tenkes å støtte opp om digital suverenitet i større eller mindre grad; eksempelvis er offentlig-privat samarbeid og tilrettelegging for tverrsektoriell bruk en viktig del av Gaia-X, som er utviklet med digitale suverenitet som mål. Ved valg av skyløsninger for offentlig sektor bør myndighetene vurdere ulike aspekter som kan styrke eller svekke digital suverenitet. Problemstillinger og avveininger relatert til disse hensynene belyses nedenfor.

4.2 Jurisdiksjon og personvern

Eierskap, kontroll og jurisdiksjon over data er en fundamental del av digital suverenitet og bør være et tungtveiende hensyn ved valg av skyløsninger. Ut over gradert og skjermingsverdige data behandler offentlige virksomheter også store mengder sensitive personopplysninger, eksempelvis helsedata. Å ha kontroll på og eksklusiv jurisdiksjon over disse er av stor betydning, både av hensyn til nasjonal sikkerhet og til borgernes personvern.

Overføring av data over landegrensene vil kunne skape usikkerhet om hvilket lands jurisdiksjon som skal gjelde. Når data lagres eller behandler på steder eller av leverandører som vil kunne komme inn under et annet lands jurisdiksjon står norske

myndigheter eller norske virksomheter i fare for å miste kontrollen over egne data. Det kan oppstå usikkerhet om hvilken jurisdiksjon som beskytter data og dataeier, eller det kan oppstå uenighet om hvilken av flere motstridende reguleringer som skal gjelde. Dette omtales gjerne som juridisk risiko som svekker dataens konfidensialitet. Bekymringen er ikke primært at sikkerheten ved datasentre i utlandet er for dårlig, men at et annet lands myndigheter kan kreve innsyn i eller i ytterste konsekvens hindre tilgang til dataene.

Personopplysninger og GDPR

I et juridisk perspektiv er overføring av personopplysninger over landegrenser en særlig utfordring ved bruk av skytjenester. Behandling av personopplysninger i Norge er regulert i personopplysningsloven som også omfatter EUs personvernforordning (GDPR). Mange offentlige virksomheter behandler store mengder personopplysninger, som enten i seg selv er sensitive eller blir det ved sammenstilling. I tillegg er mengden metadata som skyleverandører samler inn, større enn mange er klar over. Innsamlingen er ofte automatisk, og kan inkludere data som IP-adresser, legitimasjon, og logg- og diagnoserapporter. Det er den dataansvarliges ansvar å sikre at behandling av personopplysninger skjer i tråd med de grunnleggende personvernprinsippene og regelverket forøvrig. EU/EØS-området har et harmonisert regelverk på personvernområdet, men overføring av personopplysninger til tredjeland er strengt regulert. Ved bruk av allmenne skytjenester og private leverandører kan dette være krevende, da det er vanlig at leverandørene enten har servere i tredjeland eller at leverandørene bruker underleverandører i tredjeland, som oftest i USA. I tillegg opplever norske offentlige virksomheter, blant annet i helsesektoren, at leverandørene ikke utøver full åpenhet om bruk av underleverandører (Direktoratet for e-helse, 2021).

Problemet med amerikanske skytjenesteleverandører er forankret i amerikansk lov – nærmere bestemt FISA 702 og US CLOUD Act (Clarifying Lawful Overseas Use of Data Act). Lovene gir amerikanske myndigheter rett til å kreve innsyn i data – inklusive personopplysninger om EU-borgere – dersom de behandles av «Electronic Service Providers» underlagt amerikansk lov, uavhengig av hvor dataene fysisk befinner seg og også dersom disse er lagret på vegne av en kunde eller abonnent. Dette er ikke i overenstemmelse med EUs databeskyttelsesgarantier beskrevet i GDPR, og data kan derfor ikke sendes til USA uten bruk av et gyldig overføringsgrunnlag. Schrems II-dommen fra juli 2020 førte til at «Privacy Shield» ikke lenger var gyldig som overføringsgrunnlag for personopplysninger mellom europeiske og amerikanske myndigheter. Derfor bruker nå de fleste behandlingsansvarlige standardkontrakter for å sende data til USA. Slike standardkontrakter er derimot ikke nok alene, og det er knyttet betydelig usikkerhet til lovligheten av mange skyløsninger. Ytterligere tiltak, som kryptering, er et minimum for å sikre beskyttelse av personopplysninger, ifølge European Data Protection Board (EDPB). Datatilsynet har uttalt at det er utfordrende å benytte skytjenester fra Google, Microsoft og Amazon, men at det vil være mulig om man tar nødvendige forholdsregler.

Den usikre rettssituasjonen har skapt store utfordringer for offentlige virksomheter både i Norge og andre land. Eksempelvis har København satt en stor overgang til Microsofts skytjenester på vent, det danske datatilsynet nedla forbud bruk av Google Chromebooks og Workspace for Education i Helsingør kommune, og Stockholm har etter en utredning kommet frem til at byen ikke kan bruke Microsoft 365. (Røise, 2022). I slutten av mars 2022 antydet Europakommisjonens president Ursula von der Leyden og USAs president Joe Biden en politisk løsning og annonserte at USA og EU

var kommet til en prinsipiell enighet om et nytt regelverk. En oppdatert avtale for overføring av personopplysninger har siden vært under arbeid, men var ikke ennå en realitet per august 2022.

Eksklusiv jurisdiksjon og lokaliseringskrav

I tillegg til begrensningene i EUs personvernforordning GDPR inneholder også sikkerhetsloven, bokføringsloven og arkivloven føringer for hvor og hvordan offentlige virksomheter kan lagre og behandle sine data. Sikkerhetsloven stiller krav til at visse typer informasjon må lagres i Norge. For bruken av skytjenester i offentlig sektor er arkivloven også en betydelig begrensning, med bestemmelser om at det ikke er lov til å føre arkiver ut av landet. Begrepet «arkiv» er definert vidt og innebærer at svært mye som blir produsert eller mottatt i offentlige virksomheter er å anse som arkivmateriale og dermed forbudt å føre ut av landet. Dette gjør at mange offentlige virksomheter hindres i å benytte allmenne skyløsninger, eller er usikre på lovligheten av å gjøre det (Rekkedal og Forseth, 2021).

Hensikten med slike krav er primært å sikre eksklusiv jurisdiksjon over data som behandles, ved å unngå situasjoner der det er uklart hvilket lands lovverk som kommer til anvendelse. Dette kan være svært komplekst ved bruk av allmenne skytjenester, der leverandør eksempelvis kan være registrert i land A, men ha morselskap i land B utenfor EU, datasenter i land C, sikkerhetskopier i land D og benytte flere underleverandører. Videre er rettighetene etter GDPR i stor grad basert på *kundens* lokalisering og det kan være uklart hvem som har status som databehandler og dataansvarlig, og hvilke rutiner som finnes for å informere kunder om (Ghaffar, 2020).

Å eie og drifte skyløsninger i egen regi vil være den sikreste måten å garantere eksklusiv kontroll og jurisdiksjon over data på. Myndighetene kan alternativt stille krav om plassering av datasentre, lokaliserings- eller nasjonalitetskrav til leverandør, underleverandører og personale, eller krav om nasjonalt verneting. Nasjonalitetskrav kan derimot komme i konflikt med EØS-avtalens bestemmelser om likebehandling, jamfør Difis opprinnelige vurdering om at krav til lagring i Norge eller norsk leverandør i utgangspunktet vil være diskriminerende og ulovlig *dersom løsningen anskaffes i markedet og ikke omfattes av sikkerhetsloven* (se kapittel 3.2).

For offentlige virksomheter er det avgjørende å kunne klassifisere data de behandler, og forstå og vurdere hvilke data som er eller kan lagres i ulike skyløsninger, og om noen av disse dataene blir overført utenfor EU. Difis kartlegging av behov og kundegrunnlag for en offentlig skytjeneste viste at offentlige virksomheter «er usikre på hva som er lov og ikke lov når det gjelder skytjenester generelt», og at sikre skytjenester er enda mer utfordrende på grunn av usikkerhet knyttet både til krav til selve tjenesten og anskaffelsesregelverket, i tillegg til at de som kjenner anskaffelsesregelverket kan lite om lovgivningen på informasjonssikkerhetsområdet, og omvendt. En nasjonal skyløsning bør kunne bidra til å forenkle slike vurderinger, gjennom å tilby tjenester som garanterer tilstrekkelig sikkerhets- og personvernnivå samt kontroll med leverandørkjeden – enten denne er helstatlig eller markedsutsatt. Som Difi skriver i sin vurdering kreves likevel «et arbeid med regelverket» og et omfattende veiledningsarbeid for å hjelpe virksomhetene til å stille de riktige sikkerhetskravene til tjenestene og gjennomføre anskaffelsene korrekt» (Difi, 2017, s. 16).

En eventuell nasjonal sky vil være velegnet til å løse virksomhetenes utfordringer knyttet til behandling av personopplysninger eller skjermingsverdige data i skyen. En skytjeneste som eies og kontrolleres av staten kan garantere eksklusiv jurisdiksjon, blant annet gjennom krav til nasjonal lagring. Dersom det skal benyttes private leverandører av infrastruktur eller drift for hele eller deler av tjenesten bør det tilstrebes

at leverandørene er norske, alternativt europeiske, selskaper. Bruk av de store amerikanske skyleverandørene vil reise komplekse juridiske og praktiske spørsmål, blant annet knyttet til hva som rent praktisk vil være mulig å hente ut av data og metadata for en leverandør og hvorvidt det er mulig å garantere eksklusiv jurisdiksjon gjennom kontrakter og organisering; det kan bidra til å undergrave den legitimiteten og tryggheten en nasjonal sky er ment å skape overfor virksomheter og innbyggere.

4.3 Tillit til myndighetene

Betydningen av tillit til myndighetenes og offentlige virksomheters databehandling, personvernpraksis og datasikkerhet er et aspekt nasjonale myndigheter må vurdere ved valg av eierform og organisering av skytjenester. Ideen om at dette er en rettighet staten må garantere innbyggerne står sentralt i diskursen rundt digital suverenitet; Irain m.fl. (2017, s. 2) definerer for eksempel digital suverenitet som at «myndighetene plikter å innføre og håndheve lover som garanterer data-autonomi for innbyggere og selskaper, med formål om å hindre tilgang til data, særlig fra utenlandske myndigheter».

En nasjonal løsning som garanterer borgerne at deres personlige data ikke kommer på avveie vil i seg selv kunne ha betydelig verdi og fremme tillit til offentlige myndigheter og fellesskapsløsninger. Dette kan også øke villigheten til å dele data med det offentlige, noe som i økende grad vil være verdifullt i en datadrevet økonomi og en forutsetning for økosystemer for bedre deling, analyse og utnyttelse av data på tvers av offentlig sektor.

4.4 Datasikkerhet

Ivaretakelse av digital suverenitet og nasjonal sikkerhet ved overgang til skytjenester forutsetter at datasikkerheten er på et tilstrekkelig nivå. NSM har i sine årlige vurderinger av det digitale risikobildet over flere år vist til en økende risiko. I *Risiko 2022* beskriver NSM (2022) et økende «gap mellom trusselen og sikkerhetsnivået i norske virksomheter og samfunnsfunksjoner», der blant annet den spente sikkerhetssituasjonen i Europa, økt cyberaktivitet og kraftig økning i digital utpressing og sabotasje bidrar til økt risiko. «Sikkerhetstiltakene er ikke dimensjonert for det reelle trusselbildet eller innføres ikke raskt nok når nye sårbarheter oppstår», vurderer NSM . Med dette utgangspunktet synes det avgjørende at det offentlige tar skritt for å ivareta datasikkerheten.

I en undersøkelse om IKT-drift i staten utført av A2 for KMD beskrives sikkerhetsarbeidet i offentlige virksomheter som «variabelt», med akseptabel tilstand på noen områder og forbedringsbehov på andre. Nesten én av tre statlige virksomheter oppgir å ha forbedringspotensial når det gjelder å etterleve NSMs grunnprinsipper. 83 prosent av virksomhetene er ikke sertifisert i henhold til ISO 27001 eller annen anerkjent standard for informasjonssikkerhet, selv om de uavhengig av sertifisering oppgir at det legges stor vekt på informasjonssikkerhet. Bruk av ROS-analyser for skytjenester har blitt gjennomført i 62 prosent av virksomhetene og trekkes frem som et område der det finnes forbedringsbehov, særlig blant de minste virksomhetene.

Med dette utgangspunktet kan bruk av utenlandske skytjenesteleverandører i mange tilfeller gi større trygghet mot tap av data, og like god eller bedre beskyttelse mot inntrengning, med unntak av leverandøren selv og eventuelle innsynskrav fra utenlandske myndigheter, som omtalt over (4.2). Det kan derimot knyttes større usikkerhet til tilgjengeligheten i en krisesituasjon.

Som diskutert i kapittel 2 kan skytjenester ha sikkerhetsmessige fortrinn, men reiser også nye problemstillinger. NSM har uttrykt bekymring for den økte bruken av utenlandske skytjenesteleverandører. Bekymringen handler dels om i hvilken grad virksomhetene selv gjør gode og riktige vurderinger før de velger å tjenesteutsette, og om at skytjenester gir lange leverandørkjeder som innebærer flere ledd av sårbarheter, fra datasenteret til transportnettet til klienten. En mer grunnleggende bekymring handler om at vekst i skytjenester over tid resulterer i at flertallet av IKT-tjenestene til norske offentlige og private virksomheter leveres og driftes fra utlandet. Utenlandske skytjenesteleverandører bærer dermed viktige norske samfunnsfunksjoner.

Behovet for nasjonal kontroll over data og infrastruktur må vurderes ut fra flere hensyn, herunder konfidensialitet (risiko for dataavlesning), integritet (risiko for manipulasjon) og tilgjengelighet (i en krisesituasjon). Hvis tjenesten kjører på datasentre lokalisert i Norge og driftes utelukkende fra Norge er tjenesten i prinsippet under nasjonal kontroll. NSM viser likevel til at mulige sårbarheter for dataavlesing fra utlandet eller oversendelse av metadata til utlandet som er vanskelig å oppdage, dersom leverandøren er internasjonal. Dersom tjenesten kjører i et datasenter man ikke selv kontrollerer, blir det også nærmest umulig å oppdage uønsket datatrafikk ut av datasenteret (NSM, 2020b).

En tjeneste drevet i egen (statlig) regi fra Norge vil, gitt tilstrekkelig teknisk og personellmessig sikkerhet, ha høy konfidensialitet, integritet og tilgjengelighet. Myndighetene må avveie dette hensynet blant annet mot kostnader og kompetanse, men også mot funksjonalitet. Difi (2017a) påpeker at skytjenester som må tilfredsstille kravene i forskrift om informasjonssikkerhet sannsynligvis må legges til en privat sky eller gruppesky for å tilfredsstille sikkerhetskravene. Det vises til at private skyløsninger kan leveres på dedikert infrastruktur hos kunden eller i dedikert datasenter, og dermed oppfylle strenge krav til fysisk sikring «samtidig som tjenesten som sådan er en standard skytjeneste lik de de som leveres i en allmenn sky.» Spesialtilpasninger vil være mulig, men: «jo mer som endres, jo mindre får kunden igjen av gevinstene ved å kjøpe skytjenester fremfor tradisjonelle IT-tjenester». Difi ser derfor en mulighet for at «attraktive egenskaper ved skytjenestene, som f.eks. rask skalérbarhet eller 'betal for det du bruker', faller uansett vekk, eller blir kraftig redusert i en privat skytjeneste». Hvorvidt disse fordelene kan opprettholdes i en nasjonal skytjeneste vil derimot i stor grad avhenge av omfanget av en slik nasjonal løsning.

4.5 Konsentrasjonsrisiko og leverandøravhengighet

Et helt sentralt argument for å opprette statlig kontrollerte skyløsninger og/eller nasjonalt lokaliserte datasentre er å motvirke *konsentrasjonsrisikoen* som oppstår dersom de internasjonale skytjenesteleverandørene blir så store at et bortfall av tjenesten blir uhåndterbar for myndighetene. Å legge store deler av kritisk infrastruktur eller andre sentrale samfunnsfunksjoner til allmenne skytjenester innebærer altså en risiko, som kan være større på samfunnsnivå enn på ansvarsområdet til hver offentlig virksomhet. Det samme vil gjelde så store mengder mindre sensitive data og systemer at det i sum vil være kritisk dersom denne kompromitteres eller bli utilgjengelig. En slik risiko er noe staten må være bevisst, planlegge for og kunne håndtere, med tekniske eller politiske tiltak.

En rekke kritiske samfunnsfunksjoner må alltid fungere, også i en krise. En offentlig virksomhet med skjermingsverdig informasjonssystem må kunne opprettholde og tilby sine avtalte leveranser med forsvarlig sikkerhet, fortrinnsvis i hele krisespennet

fra fred, via krise og til krig. Dette utelukker ikke å benytte skytjenester, men risikoen ved å gjøre det må håndteres. Hva skjer for eksempel dersom skytjenesteleverandøren går konkurs? Eller i en krisesituasjoner hvor styringen av infrastruktur overtas av staten der dataene er lagret? For tjenester som er av avgjørende betydning for grunnleggende samfunnsfunksjoner bør risikoen for at tjenesten stenges eller faller bort minimeres gjennom både tekniske og politiske virkemidler (Strand, 2020).

En mindre dramatisk, men relatert utfordring er leverandøravhengighet i form av innlåsingseffekter og transaksjonskostnader ved bytte av leverandør. Der skytjenester ideelt sett gir virksomheten skalerbarhet, fleksibilitet og betaling for bruk, kan realiteten ofte være at en betaler programvare gjennom abonnementer med lengre kontraktsperioder, eller har brukt tid og ressurser på å utvikle, implementere og lære opp medarbeidere i systemer som ikke enkelt lar seg erstatte eller flytte til en annen skyleverandør. Størst mulig tjenestemobilitet bør derfor være et mål, for en nasjonal sky så vel som for tjenestekjøp i markedet. Dette inkluderer å kunne flytte virtualiserte applikasjoner mellom datasentre hos valgte tilbyder eller mellom statlige datasentre, og ideelt også mellom konkurrerende systemer. For å kunne oppnå dette er det et fortrinn at systemene bygger på standardiserte og utbredte løsninger og åpen kildekode. Den tyske skystrategien (se kapittel 5) har eksempelvis store ambisjoner på dette området: Felles tekniske krav til systemer i virksomheter på alle nivåer av offentlig forvaltning skal sørge for gjenbrukbare applikasjoner og hindre avhengighet til enkelte skyløsninger, særlig de store amerikanske, og så langt det er mulig benytte åpne standarder med modulære komponenter som muliggjør tjenestemobilitet (IT Planungsrat 2021b).

4.6 Kompetanse

Hvilken IT-kompetanse som finnes i det offentlige, vil til en viss grad være styrende for hvilke skyløsninger myndighetene bør eller kan velge. En norsk nasjonal skytjeneste av et visst omfang vil, i hvert fall i den grad den skal driftes helt eller delvis i egen regi og med mål om digital suverenitet, kreve en betydelig konsolidering og utvidelse av IT-kompetansemiljøer i det offentlige. I en tidlig fase vil det sannsynligvis også være nødvendig å trekke på private underleverandører og konsulenter i betydelig grad. En fullskala adopsjon av dagens tyske tilnærming med en statlige skyløsninger rettet mot hele eller store deler av offentlig sektor, og med et prinsipp om at staten skal levere så mye som mulig i egenregi, vil etter alt å dømme ikke velges i første omgang dersom en nasjonal sky realiseres - delvis av hensyn til størrelsen på norske IKT-fagmiljøer. Leder av det pågående utredningsarbeidet hos NSM ser derimot *ikke* kompetansenivået og størrelsen på norske IT-miljøer som noe avgjørende hinder for muligheten til å etablere en nasjonal sky (Intervju, NSM 12.06.2022). Samtidig satset heller ikke Tyskland på en altomfattende løsning fra start; Bundescloud begynte som et beskjedent system, og ble realisert med betydelig bruk av eksterne konsulenter. Tyskland har derimot hatt en tydelig ambisjon om å bygge intern IT-kompetanse i staten, både som del av skystrategien og i det større konsolideringsprogrammet for IT-drift (se kapittel 5). Også i Nederland har konsolidering av IT-kompetansemiljøer vært en avgjørende del av datasenter- og skytjenestestrategien. De store statlige IT-leverandørene som drifter datasentrene har økt antall ansatte kraftig ved å samle tidligere virksomhetsinterne driftsmiljøer gjennom virksomhetsoverdragelser. I Danmark har Statens IT, med sin langt mindre omfattende GovCloud, også satset på kompetansebygging på skytjenesteområdet.

Ved kjøp av allmenne skytjenester i markedet må offentlige virksomheter forholde seg til private leverandører som gjerne er internasjonale konsern som Amazon, Microsoft eller Google. Disse leverandørene sitter i stor grad på det meste av kompetansen om hvordan informasjonen lagres og behandles. De store fagmiljøene hos leverandørene befinne seg dessuten i utlandet, og overføringen av kompetanse til kunden kan være begrenset. Samtidig krever en modell basert primært på tjenestekjøp i markedet betydelig bestillerkompetanse. Undersøkelsen fra Difi (2017a) viste at dette ble oppfattet som mangelvare av virksomhetene selv, og at det var et stort behov for veiledning om skytjenester. En viss konsolidering og styrking av statlige IT-fagmiljøer kan dermed synes hensiktsmessig uavhengig av eierskapsmodell for skytjenestene. Større felles tverrfaglige IT-kompetansemiljø er også noe NTL og Fagforbundet tidligere har tatt til orde for, med mål om å sikre bedre kontroll med kritisk IT-infrastruktur (Hanssen, 2019).

5 Omverdensanalyse

Et ønske om digital autonomi og datasuverenitet, i betydningen at myndighetene kan ha fullstendig kontroll over egne data i skyen gjennom eksklusiv jurisdiksjon i tillegg til vanlige sikkerhetstiltak, ligger til grunn for at en rekke land har valgt strategier delvis basert på statlige løsninger og/eller innenlands datasentre (Irion, 2012). I USA leverer Microsoft, Google og Amazon egne høysikkerhetsløsninger til amerikanske myndigheter. Tyskland har valgt å etablere sin egen «private» statlige sky og har i stor grad valgt å organisere og drifte IKT-tjenestene sine selv. Nederlandske myndigheter har også opprettet statlige skytjenester og legger vekt på bruk av programvare med åpen kildekode for å hindre innlåsingseffekter. Frankrike vektlegger som Tyskland digital suverenitet og har etablert egne skytjenester for finans- og innenriksdepartementet. Frankrikes har også tatt initiativ til en sertifiseringsordning av skyleverandører som legger opp til at de ledende amerikanske leverandørene kan lisensiere sin teknologi til europeiske selskaper. Danmark er i ferd med å skalere opp en så langt begrenset, skytjenesteløsning for statsforvaltningen og Sverige har nylig utredet organiseringen av sin IKT-forvaltning. På europeisk nivå har Tyskland og Frankrike tatt initiativ til Gaia-X prosjektet som tar sikte på å bygge en sikker og suveren europeisk datainfrastruktur gjennom offentlig-privat samarbeid og europeiske tjenesteleverandører, med mål om å utfordre de amerikanske skyleverandørene. EU-kommisjonen har også lansert et initiativ for å bygge felles skytjenester som henviser både til Gaia-X og integrasjon mellom eksisterende nasjonale skyløsninger.

Dette kapittelet ser nærmere på nærmere på Tyskland, Nederland, Danmark og felleseuropeiske initiativer.

5.1 Tyskland

Tyske myndigheter har valgt å organisere og drifte store deler av IKT-tjenestene i egen regi. Suverenitet og digital autonomi vektlegges tungt, og det er et tydelig uttalt mål å unngå avhengighet av internasjonale selskaper. Digitaliseringspolitikken som helhet har autonomi som et sentralt mål og tilnærmingen til skytjenester reflekterer dette. Den tyske staten har valgt å etablere og drifte sin egen «private» statlige skytjenesteplattform, kalt die Bundescloud. Målet er å skape uavhengighet fra eksterne leverandører og sikre at viktige data lagres i Tyskland under statens kontroll. Denne tilnærmingen videreføres og utvides i regjeringens skytjenestestrategi vedtatt i 2021, som i tillegg til den føderale administrasjonens IT-tjenester også skal omfatte føderale, delstatlige og lokale offentlige virksomheter.

Skytjenester og datasentre

Bruk av skytjenester øker kraftig i Tyskland, samtidig som landets myndigheter er opptatt av digital suverenitet og datasikkerhet. Det finnes en rekke skytjenester som eies og driftes av offentlige virksomheter fra datasentre lokalisert i Tyskland. De føderale myndighetene har i underkant av 100 datasentre som betjener rundt 200 000 brukere og har opprettet en felles skytjeneste for den føderale administrasjonen;

Bundesclound. I tillegg har en rekke delstatlige og lokale myndigheter egne løsninger. Den nasjonale skytjenestestrategien nevner blant Academic Cloud i Niedersachsen[7], datasenteret til delstatsadministrasjonen i Mecklenburg Vorpommern (DVZ:DIGITAL), Thüringens datadelingsplattform og Sachsens sikre skytjeneste. Et mål for skytjenestestrategien (omtalt nedenfor) er at disse skal danne en felles IT-infrastruktur for tysk offentlig sektor.

Den føderale administrasjonens skytjeneste Bundescloud er den mest omfattende av disse og brukes av mer enn 50 statlige virksomheter. Opprettelsen av en sikker skytjeneste for staten ble planlagt av den tyske regjeringen fra 2011. Allerede fra begynnelsen var et hovedmål å minimere juridisk risiko og mulig innsyn fra amerikanske myndigheter, i tillegg til å adressere det myndighetene anså som sikkerhetsutfordringer ved allmenne skytjenester (Berke, 2011). Vurderingen var at alternativet i praksis vil være eskalerende bruk av private skytjenesteleverandører og datasentre. Et kraftfullt initiativ for å gjøre dette nå og ikke om ti år når dette allerede er etablert praksis var derfor viktig (Stach, 2020). Utbyggingen ble vedtatt i 2015 som del av et omfattende prosjekt for konsolidering av føderale IT-tjenester, igangsatt to år tidligere. Oppdraget ble gitt til det den da nyopprettede sentrale enheten for statens IT (ITZBund) og i 2017 ble de første tjenestene gjort tilgjengelig for statlige virksomheter på Bundescloud-plattformen. Bundescloud eies av den tyske staten og drives på datasentre i Tyskland underlagt strenge krav til sikkerhet, personvern og jurisdiksjon. Bundescloud omfatter blant annet et felles saksbehandlingssystem og en rekke ulike tjenester inkludert infrastruktur som tjeneste, plattform som tjeneste og programvare som tjeneste. Sluttbrukerne blant statsansatte bruker skyen gjennom en egen standardisert tynnklient som kjører på ITZBunds servere, med felles infrastruktur og standard programvare, inkludert virtuelle maskiner med Windows, Office-pakken og programmer for e-post, kalender, fildeling og nettlesere med høyt sikkerhetsnivå (ITZBund, u.å.). All data lagres i Tyskland. Private selskaper er involvert som leverandører, men så langt det er mulig er det valgt tyske leverandører og løsninger basert på åpen kildekode. Eksempelvis er fildelings-løsningen BundescloudBox og den modulære arkitekturen som gjør det mulig å tilby utviklingsplattformen som tjeneste (Paas) basert på en løsninger med åpen kildekode fra tyske Cloudgo (ITZBund 2020) og Nextcloud (Beuth, 2018), som har vunnet anbud for dette. Å kjøpe tjenester i markedet har vært nødvendig for å bygge opp systemet, som startet med et begrenset tjenesteutvalg.

I tillegg til Bundescloud bruker en rekke statlige virksomheter også allmenne og kommersielle skytjenester, siden ikke alle tjenester er tilgjengelige via den statlige skytjenesten. En hovedårsak til dette er de strenge sikkerhetskravene for Bundescloud, som blant annet medfører adgang utelukkende via nettverk med høy sikkerhet og ikke fra Internett (Ehneß, 2019). En ekstern skytjeneste skal likevel bare brukes hvis den føderale administrasjonen ikke selv kan levere tjenesten, og kjøp er å foretrekke fremfor en midlertidig bruksrett (leieavtale). Bruk av eksterne skytjenester er underlagt en rekke krav, herunder at sensitive data skal lagres i Tyskland og ikke kan gjøres kjent for uautoriserte tredjeparter, at kontrakter skal være underlagt tysk lov og oppgi domstoler i Tyskland som verneting, samt at leverandøren må dokumentere at det foreligger tilstrekkelig informasjonssikkerhet etter internasjonal standard (ISO27001) eller den tyske Cloud Computing Compliance Controls Catalogue (C5).

[7] Academic Cloud er et samarbeid mellom universitetene i Niedersachsen og OwnCloud, drevet fra universitetenes datasentre og tilrettelagt for opptil 210 000 brukere (se academiccloud.de)

Mens retningslinjene i den norsk statlige IKT-strategien anbefaler at skytjenester kjøpes i markedet når dette er kostnadseffektivt, er prinsippet for den tyske staten altså motsatt: Kommersielle tilbydere av skytjenester skal bare benyttes hvis staten ikke selv kan tilby en tilstrekkelig tjeneste.

Også lokale myndigheter i Tyskland er i økende grad opptatt av digital autonomi og avhengighet av utenlandske selskaper. München vedtok i 2020 at åpne standarder og fri programvare med åpen kildekode skal benyttes der det er teknisk og økonomisk mulig. Fra 2006 hadde München også en satsing på løsninger med åpen kildekode men gikk deretter delvis over til Microsoft i en periode (Schaer, 2020). I Hamburg har politikerne tilsvarende ønsket å redusere avhengigheten til Microsoft, som i stor grad har levert byens systemer, og gå over til å benytte løsninger basert på åpen kildekode – etter prinsippet «offentlige penger, offentlig kode». Dortmund og Bremen, samt delstatene Thüringen og Schleswig-Holstein, har tidligere gjort liknende vedtak (Brombach, 2020). Hamburg har også satset på å ta i bruk «Project Phoenix», en voksende samling med sky-, web- og modulbaserte tjenester basert på åpen kildekode for blant annet e-post, dokumenthåndtering, chat og videosamtaler. Tjenesten er utviklet og levert av non-profit-selskapet Dataport ved hjelp av en privat skyløsning med servere i Tyskland og retter seg i hovedsak mot offentlig sektor.

Tysk lovgivning og politisk oppmerksomhet om datasikkerhet har også ført til at private tilbydere har tilpasset sine produkter. Eksempelvis har Microsoft etablert datasentre der tilgangen til kundedata er lagt til en uavhengig dataforvalter, slik at Microsoft ikke har rettigheter til å få tilgang kundedataene, men må søke dataforvalteren om dette. Et amerikansk krav om av innsyn i dataene vil dermed ikke etterkommes uten at det godkjennes av dataforvalteren, som er underlagt tysk lovverk (Brombach, 2016).

Strategi

I juni 2013 vedtok budsjettkomiteen i Bundestag å be regjeringen utvikle et sentralt innkjøpssystem for den føderale administrasjonen. To år senere ble det vedtatt en «akselerert vertikal konsolidering av føderale IT-tjenester». Det ble samtidig satt nye krav til alle føderale myndigheter som innebar at disse kun kan benytte skytjenester som lagrer data i Tyskland og tilbydere som undertegner avtaler om at det ikke skal gis innsyn til andre lands myndigheter (Stupp, 2015).

Konsolideringen av de føderale IT-tjenestene samler IT-systemene for over 200 statlige etater, som tidligere har brukt sine egne systemer. Det er inndelt i 42 ulike delprosjekter, hvorav Bundescloud er ett. Hovedformålet med prosjektet er å beholde suverenitet og kontroll med offentlige data og kunne tilby et høyere nivå av datasikkerhet og personvern. Suverenitet over egne data og den amerikanske lovgivningen som gjør at amerikanske myndigheter kan kreve å få data fra private skyleverandører selv om denne dataen finnes i andre land, var også viktige hensyn. Den tyske regjeringen mener disse hensynene blir bedre ivaretatt når staten gjør dette selv, enn ved bruk av private aktører (Stach, 2020). Bundescloud bidrar til å sikre personvern og datasikkerhet gjennom å lagre data i statens egne datasentre. Å hindre datalekkasjer er enklere når staten selv opererer datasentre og IT-tjenester. I tillegg hindres planlagt overføring av data til tilbyders servere, noe tyske myndigheter har observert skjer hos enkelte etablerte tilbydere. Heike Stach, som ledet prosjektet, har uttalt at bakgrunnen for at den føderale administrasjonen gradvis gikk bort fra å kjøpe skytjenester i markedet at det i praksis ville innebære en risiko som er større enn om de skulle drive systemene selv, og det var også en utfordring at private leverandører ikke nådde opp til sikkerhetskravene Tyskland stilte (Hauge-Eltvik, 2020). Videre ble det sett på

som en ulempe at skytjenester fra private leverandører gikk over til leie eller abonnement av tjenester: Tyske myndigheter ønsker ikke å være avhengige av eksterne leverandører.

«Vi ville ha suverenitet og være autonome, og styre vår egen IT også om ti år», har Stach uttalt, og utdypet at dette er en bekymring når en abonnere på tjenester: «Når perioden er over, har du kanskje ingen garantier for at tjenestene støttes videre. Et enda verre scenario er om en skyleverandør «slår av» tjenesten. Dette er ikke vanlig, men i en krisesituasjon kan det skje. For en statsforvaltning er det en katastrofe, og vi kan ikke ha en sånn risiko» (Hauge-Eltvik, 2020).

Ut over disse hensynene skal sentraliseringen av IT-drift og en felles skytjeneste bidra til at staten skal kunne respondere fleksibelt både på nye teknologitrender og på nye behov hos offentlige virksomheter og deres brukere. Nye IT-løsninger skal kunne settes opp raskt og enkelt og kunne tas i bruk på nye måter, etter behov. Målet er felles IT-service i skyen, sentralisering av anskaffelser og sentralisering av IT-operasjoner ved å begrense antallet datasystemer som har samme funksjon.

Nasjonal strategi for offentlige skytjenester

I 2020 lanserte den tyske regjeringen en overordnet strategi for digital autonomi som også omfatter forbundsstatene og det lokaladministrative nivået (IT-Planungsrat 2020). Et overordnet mål med dette arbeidet er å kartlegge hvor det kan oppstå en kritisk avhengighet av teknologileverandører, søke alternative løsninger og koordinere tiltak for å sikre tilgang til alternative IT-løsninger. Som en del av denne satsingen har den tyske regjeringen også vedtatt en egen strategi for skytjenester i offentlig sektor, lansert i oktober 2020 (IT-Planungsrat, 2021a). Skytjeneste-strategien definerer målsettinger, standarder og arkitektur for hvordan offentlige myndigheter på alle nivåer i Tyskland skal konfigurere og bruke sine egne skytjenester. Et hovedmål er å styrke Tysklands digitale suverenitet, definert som «evner og muligheter for individer og institusjoner til å utøve sine roller i den digitale verden autonomt, sikkert og trygt» (IT-Planungsrat, s. 3). Ifølge strategien er digital suverenitet under press på nasjonalt, delstatlig og lokalt nivå, på grunn av veksten i digitale administrative prosesser. En strategisk markedsanalyse utført for de føderale myndighetene viste også at avhengighet av programvaretilbydere gir konkrete begrensninger på digital suverenitet i form av utfordringer med informasjonssikkerhet, juridisk uklarhet, kostnader, fleksibilitet og innovasjon utenfor myndighetenes kontroll. Den nasjonale strategien for skytjenester i offentlig sektor er ett av flere virkemidler for å utbedre dette, og har som mål å standardisere eksisterende offentlige skytjenesteløsninger og legge grunnlaget for fremtidige løsninger.

Det eksisterer allerede en rekke datasentre og skytjenester som drives og brukes av offentlige virksomheter – herunder Bundescloud og de andre skytjenestene nevnt over - men disse er i liten grad kompatible med hverandre. Skytjenestestrategien skal introdusere felles standarder og åpne løsninger som legger til rette for en modulær, interoperatibel skytjenesteinfrastruktur for hele offentlig sektor. Målet er at offentlige virksomheter i større grad skal kunne dele løsninger med hverandre og benytte flere skytjenester. Strategien definerer felles standarder som skal sikre digital suverenitet gjennom krav blant annet til sikkerhet, personvern og tysk jurisdiksjon, for private- eller gruppeskytjenester på alle forvaltningsnivå. Den har også en rekke tekniske krav, som skal muliggjøre gjenbruk og skalering av applikasjoner og løsninger på tvers av offentlige virksomheter, øke markedsmakten som kan utøves av offentlig sektor, og gjøre offentlige skyløsninger kompatible med hverandre og med GAIA-X.

De uttalte målene med strategien er å 1) redusere avhengighet og innelåsing ved gjøre offentlige IT-systemer utbyttbare og interoperatible samt øke det offentliges markedsmakt; 2) øke effektiviteten i utvikling, implementering og drift av IT-systemer gjennom å benytte standardiserte, skalerbare, gjenbrukbare og enkelt tilgjengelige løsninger; 3) sikre personvern og informasjonssikkerhet «by design» og; 4) optimalisere datautveksling og delt datalagring mellom føderale, delstatlige og lokale offentlige virksomheter (IT-Planungsrat, 2021a, s. 7). I praksis vil dette innebære felles standarder for de fleste aspekter ved skytjenestene, blant annet standarder for maskinvare og programvare, felles kodebibliotek, utviklingsplattformer og arkitekturkrav til applikasjonsutvikling, standarder for leveranse og drift av applikasjoner og samarbeid med IT-leverandører. Offentlige virksomheter som benytter én eller flere slike skytjenester skal da være garantert at data lagres og prosesseres på en forutsigbar og gjennomsiktig måte og at tjenestene oppfyller krav til sikkerhet og personvern. De skal også kunne dele, adoptere eller gjenbruke løsninger fra andre virksomheter på ulike forvaltningsnivåer i sin egen sky, uten lisensrestriksjoner.

Standardiseringen gjelder alle skytjenester som eies og driftes av offentlige virksomheter, på de tre forvaltningsnivåene. Tekniske krav til disse skytjenestene spesifiseres i et eget arkitekturrammeverk (IT-Planungsrat, 2021b), som skal legge grunnlaget for at tjenestene til sammen kan danne en desentralisert, offentlig skyinfrastruktur. Det skal bli mulig for offentlige virksomheter å søke etter, bestille, avbestille og tilpasse IT-tjenester gjennom en felles portal, som skal administreres av en egen koordinerende organisasjon. Infrastrukturen skal være under offentlige myndighetenes kontroll og langt på vei driftes av deres IT-avdelinger, men det defineres også roller og ansvar for bruk av underleverandører og standardiserte løsninger som skal muliggjøre bytte av tilbydere og innkjøp av tjenester som en integrert del av den offentlige skyen. Datasentrene må oppfylle en rekke juridiske og tekniske krav, blant annet at de skal være fullstendig underlagt tysk lov og at offentlige myndigheter alltid skal ha «suveren kontroll» med kodenøkler til lagret data, og tilsvarende over både maskinvare og programvare for viktige tjenester. I tillegg kommer strenge sikkerhetskrav satt av den tyske informasjonssikkerhetsmyndigheten BSI, herunder minstekrav (ISO27001) og helst C5-sikkerhetsstandarden for skytjenester. Det også et mål at det brukes løsninger basert på åpen kildekode. I tillegg etableres det standarder for koblinger mot allmenne skytjenester og kantenheter (edge computing).

Kostnader og kompetanse

Etableringen av Bundescloud har vært finansiert som en del av konstitueringen av de statlige IT-tjenestene. Satsingen er omfattende, eksempelvis har ITZBund alene om lag 4000 ansatte og et årlig budsjett på 1,132 milliarder Euro i 2022 (ITZBund, 2022). Kostnadene ved etableringen av en statlig skytjeneste forsvares ved at det bidrar til vesentlig effektivisering av en tidligere fragmentert IT-infrastruktur. Ifølge prosjektleder Heike Stach var det forventet at det ville bli dyrt, men de reelle kostnadene har blitt noe lavere enn forventet (Hauge-Eltvik, 2020). Strategien har vært å investere i egen kompetanse, egne datasentre og egen infrastruktur. Bruk av eksterne spesialister er spesielt kostbart, noe som gradvis trappes ned i takt med at staten bygger opp egen kompetanse. Å bygge opp fagmiljøer og kompetanse i staten har vært et mål med satsingen. Å ha egen kompetanse i det offentlige ses som avgjørende for å oppnå digital suverenitet og autonomi (Hauge-Eltvik).

5.2 Nederland

Nederland har valgt å opprette egne private skytjenester for statsforvaltningen, og staten drifter selv flere datasentre. Denne tilnærmingen ble valgt med utgangspunkt i kostnadshensyn og utfordringer knyttet til personvern og datasikkerhet. Det er gradvis åpnet opp for bruk av allmenne skytjenester for data med lavere beskyttelsesbehov. Skytjenester benyttes i økende grad både i staten og i kommunal sektor.

Strategi

Den digitale agendaen for forvaltningen (Nederlands regjering, 2022), agendaen for cybersikkerhet (Nationaal Cyber Security Centrum, 2018) og datastrategien (Nederlands regjering, 2019) legger de overordnede føringene for den digitale politikken. Innenriksdepartementet (BZK) har ansvaret for den digitale agendaen, mens sektoransvarlige statsråder har ansvar for IT innen sine sektorer.

Nederlands tilnærming til skytjenester i offentlig sektor har i stor grad basert seg på å levere disse tjenestene internt. I 2010 fikk regjeringen i oppdrag av parlamentet å utvikle en strategi for skytjenester basert på «sky først»-prinsippet samt en analyse av nytte, kostnader og risiko ved bruk av skytjenester og opprettelse av en privat skytjeneste for staten. Regjeringen svarte i 2011 (Nederlands innenriksdepartement, 2011) og konkluderte da med at selv om det fantes fordeler med kommersielle, allmenne skytjenester var det betydelig ulemper knyttet til dette for offentlige sektor, og anbefalte at staten skulle implementere skytjenester internt og i egen regi. Bakgrunnen for dette var at markedet ble vurdert som lite modent, i tillegg til at forvaltningen hadde høye krav til sikkerhet og personvern, og at lagring av sensitiv informasjon i skytjenester utenfor landets grenser var forbundet med risiko. Det ble derfor besluttet å opprette en private statlige skytjenester i egen regi, omtalt som Rijkscloud, som del av et større reformprogram for å effektivisere forvaltningen (Nederlands regjering, 2011). Hensikten var å realisere gevinstene knyttet til bruk av skytjenester, som stordriftsfordeler, brukervennlighet og innovasjon, uten kompromisser med hensyn til personvern og datasikkerhet.

Fra 2016 ble det åpnet for en viss bruk av allmenne skytjenester i den nederlandske statsforvaltningen, gitt at en rekke vilkår er oppfylt. Ved valg av eksterne leverandører skal det gjennomføres risiko- og personvernanalyser og virksomheten må vurdere kvalitet, juridiske aspekter, datasikkerhet og risiko for innlåsing (Nederlands regjering, 2020). De siste årene har forvaltningen beveget seg noe mot en multi-cloud tilnærming der også kommersielle leverandører brukes. Eksempelvis er det i 2021/2022 inngått avtaler med Google om bruk om Workspace og Workspace for Education (The Cloud Report, 2022). Adgangen til å kjøpe skytjenester i markedet er begrenset av personvern- og datasikkerhetsbestemmelser, herunder GDPR og rammeverket for informasjonssikkerhet kalt BIO, som er utarbeidet av det nasjonale cybersikkerhetssenteret NCSC. Håndtering av konfidensiell informasjon deles i BIO inn i tre beskyttelsesnivåer. På det laveste nivået er det tillat å bruk av allmenne, private og hybride skyløsninger. På mellomnivået er dette tillatt kun dersom virksomheten kan identifisere og håndtere «avanserte og langsiktige trusler», og for en del informasjon vil det på dette beskyttelsesnivået utelukkende være tillatt å bruke de statlige datasentrene eller private skytjenester. På det høyeste beskyttelsesnivået er det ikke tillatt å bruke noen form for skytjeneste eller felles datasenter. På de to lavere nivåene skal det benyttes en risikobasert tilnærming. Den nederlandske sikkerhetstjenesten AIVD og innenriksdepartementes vurdering er at ingen allmenne skytjenester per i dag er sikre

nok til å benyttes for gradert informasjon, eller for vitale systemer og prosesser som krever beskyttelse mot statlige aktører (NORA, 2019).

Skytjenester og datasentre

Den statlige organisasjonen for felles IT-tjenester (SSC-IT) driver fire større datsentre, som også danner infrastruktur for skytjenester. SSC-IT leverer IT-tjenester med høy sikkerhet til om lag 40 000 brukere i syv departementer og underliggende virksomheter, og har over 1200 ansatte fordelt på 50 lokaliteter. Utgangspunktet for etableringen av datasentrene var det ovennevnte reformprogrammet (Nederlands regjering, 2011), som hadde som mål å effektivisere statsforvaltningen og kutte utgifter, blant annet ved å konsolidere den da fragmenterte IT-infrastrukturen i staten. Antallet datasentre i de involverte departementene skulle reduseres fra 64 til fire, med felles drevne fasiliteter. Formålet var i tillegg til kostnadsreduksjon, å styrke IT-sikkerhet og personvern. I 2013 åpnet det første av de fire datasentrene, ODC-Noord i Gröningen, og i løpet av de neste to årene åpnet også datasentre i Amsterdam, Apeldoorn og Rijswijk. Ved ODC-Noord har antall ansatte økt fra 5 til over 100, og tilbudet er utvidet fra samlokaliserte servere og lagring til å omfatte utviklingsverktøy og skytjenester som virtuell maskinvare, infrastruktur, og programvare som tjenester (HaaS, IaaS og PaaS) (ODC-Noord, u.å.). I tillegg til SCC-IT leveres denne type skytjenester også av DICTU, en statlig IT-tjenesteleverandør med 1600 ansatte som både leverer komplette IT-tjenester til to departementer og en rekke fellestjenester til forvaltningen. DICTU leverer blant annet ID-løsninger, meldingstjenester og adgangskontroll og jobber med å etablere en sikker privat sky for statsforvaltningen (DICTU, u.å.). Ifølge ledelsen ved SSC-IT har sentraliseringen av datasentre høyere sikkerhetsnivå gjennom økt kontroll, mulighet til å realisere stordriftsfordeler, bedre forutsetninger for digital utvikling gjennom en moderne driftsorganisasjon og ny teknologi. Skytjenester som leveres fra datasentre i Nederland som er drevet eller kontrolleres av staten er også med på å øke fysisk sikkerhet og kontroll med personale. Åpen kildekode og åpne standarder er et strategisk valg for å unngå innlåsingseffekter (SOU 2021: 1, s. 46). Kundene kan betale for bruk og konsentrere seg om kjernevirksomheten. Dette kan gi betydelige besparelser, eksempelvis oppga utdanningskultur og vitenskapsdepartementet kostnadsbesparelser på 30 prosent da de gikk over til å bruke skytjenester levert av ODC-Noord, sammenliknet med sine egne interne systemer (Hillenius, 2017). En rapport fra den nederlandske riksrevisjonen er likevel til dels kritisk til denne typen statlige tjenesteutsetting med utgangspunkt i at selve overgangene kan være krevende og at departementene har lite innsyn i leverandørens aktiviteter og dermed begrenset kontroll med kostnadene (Nederlands Riksrevisjon, 2019).

5.3 Danmark

Bruk av allmenne skytjenester er utbredt i dansk offentlig sektor. Danske myndigheter har ikke en samlet strategi for bruk av skytjenester eller innkjøp av IT-tjenester, og bildet er derfor svært variert (Digitaliseringsstyrelsen, 2022, s. 10). Det stilles i liten grad krav til nasjonal lagring og databehandling, med unntak av offentlige IT-systemer som behandler personopplysninger av kritisk betydning for nasjonal sikkerhet. Usikkerhet rundt personvern og datasikkerhet har i økende grad vært gjenstand for debatt og flere skytjenesteprosjekter ble forsinket i forbindelse med Schrems II-dommen. Statens IT, som er felles leverandør av IT-tjenester til en rekke statlige virksomheter, har siden 2020 utviklet en egen statlig skytjeneste, kalt GovCloud, som et

pilotprosjekt. I løpet av 2022 utvides tilbudet i denne tjenesten med lansering av en kunderettet selvbetjeningsportal (Statens IT, 2022).

Strategi og organisering

Anskaffelse av skytjenester og valg av tilbyder er langt på vei opp til den enkelte offentlige virksomhet, og det eksisterer ikke en overgripende, felles strategi for skytjenester i offentlig sektor. Flere strategier legger visse føringer for offentlig IT-drift, herunder digitaliseringsstrategien for offentlige sektor (Digitaliseringsstyrelsen, 2016), strategien for IT-styring i statsforvaltningen (Digitaliseringsstyrelsen, 2017) og den nasjonale cyber- og IT-sikkerhetsstrategien (Digitaliseringsstyrelsen, 2018). Disse omhandler i liten grad skytjenester.

Det danske digitaliseringsdirektoratet (Digitaliseringsstyrelsen), som er underlagt Finansdepartementet og jobber på strategisk nivå med å utvikle og koordinere den offentlige forvaltningens digitalisering og IT-infrastruktur og også jobber for å styrke IT-sikkerheten i staten, har utarbeidet en egen veiledning for bruk av skytjenester (Digitaliseringsstyrelsen, 2020). Veiledningen beskriver prinsipielle problemstillinger rundt offentlige myndigheters bruk av skytjenester og gir retningslinjer for bruk og anskaffelse av skytjenester for offentlige virksomheter. Digitaliseringsstyrelsen fremholder at kommersielle skytjenester kan muliggjøre nye tjenester og innovasjon i offentlige virksomheter. Samtidig vises det til utfordringer og risiko knyttet til sikkerhet og kostnader og tiltak virksomhetene kan ta for å minimere disse.

Ved anskaffelse og bruk av skytjenester må offentlige myndigheter sørge for at tjenesten holder tilstrekkelig sikkerhetsnivå og overholder data- og personvernlovgivning og andre juridiske krav. Da det ofte vil være vanskelig å kontrollere at leverandøren møter alle krav, kan det benyttes en risikobasert tilnærming ut fra tilgjengelig dokumentasjon, sertifiseringer og revisjonsberetninger. Det skal alltid gjøres en risikovurdering, og konsekvensanalyse skal gjennomføres ved 'høy risiko for fysiske personers rettigheter. Krav til behandling av personopplysninger, databehandleravtaler og utfordringene rundt overføring av data til tredjeland utenfor EU og EØS behandles i detalj i veiledningen, men den legger ikke restriksjoner på bruk av kommersielle utenlandske skyleverandører. Forutsetningen er at lovverket for datasikkerhet overholdes, at det kan etableres et tilstrekkelig overføringsgrunnlag og at det ut fra risikovurdering og eventuelt konsekvensanalyse holder et tilstrekkelig sikkerhetsnivå. Det oppfordres likevel til designvalg som øker beskyttelsen, som å avgrense oppbevaring av data til EØS og sikre tredjeland.

Databeskyttelsesloven (§ 3, stk. 9) legger noen ytterligere begrensninger, i form av at personopplysninger som kan «true statens sikkerhet» behandles i offentlige IT-systemer kan underlegges krav om lagring i Danmark. Dette lokaliseringskravet gjelder eksempelvis store landsdekkende administrative systemer og registre. Tilsvarende krav finnes også i Retshåndhevelsesloven som gjelder politi, påtalemyndigheter og domstolene. Kravet utelukker i praksis bruk av de fleste internasjonale skytjenesteleverandørene for denne type data, men er ikke til hinder for bruk av skytjenester som sådan hvis disse er basert på datasentre lokalisert i Danmark (Digitaliseringsstyrelsen, 2020, s. 30). Formålet med lokaliseringskravet er å sikre at IT-systemer som behandler personopplysninger er underlagt eksklusiv dansk jurisdiksjon. Krav og omfang er spesifisert i en egen veileder (Justisministeriet, 2020). Tjenester som omfattes inkluderer blant annet ID-porten MitID, Digital Post, statens lønnssystemer og forsvarets sentrale IT-system. Terskelen for bestemmelsen er likevel høy og store landsdekkende IT-systemer blant annet i skatt- og arbeidsforvaltning er ikke omfattet av lokaliseringskravet.

Skytjenester og datasentre

Offentlige virksomheter i Danmark tar i økende grad i bruk skytjenester og outsourcede IT-tjenester med mål om å oppnå stordriftsfordeler og fleksibilitet, og beveger seg samtidig i noen grad vekk fra egne serverrom (Digitaliseringsstyrelsen, 2022). Statlige, regionale og kommunale virksomheter som kjøper skytjenester i markedet kan benytte seg av rammeavtaler via Statens og kommunernes indkøbsservice (SKI), herunder avtaler for skylagring og programvare som tjeneste (KMD, u.å.). Mange danske kommuner har satset stort på skytjenester (Haslund, 2018). Eksempelvis har København kommune vedtatt å flytte 250 IT-systemer fordelt på 1000 servere til Microsofts skytjeneste og legge ned to kommunale datasentre. Overføringen av data til skyen ble derimot satt på vent etter Schrems II-dommen i 2020 og veiledning fra det danske Datatilsynet (Weng, 2022). Per juni 2022 avventer København fortsatt, i påvente av skriftlig avtale om overføringsgrunnlag mellom EU og USA og nye regler på området (Olifent, 2022). Datatilsynet har også nylig advart landets kommuner mot å bruke amerikanske skyløsninger til å behandle personopplysninger uten å ha tilstrekkelige avtaler, og forbød Helsingør kommune å behandle personopplysninger ved bruk av Google Chromebooks og Workspace for Education (Aukrust, 2022).

Om lag halvparten av statlige myndigheter har flyttet hele eller deler av sin IT-drift til Statens IT (Digitaliseringsstyrelsen, 2022). I strategien for IT-styring i staten vektlegger regjeringen at statsforvaltningen i større grad skal benytte felles IT-løsninger og samle grunnleggende IT-drift for å oppnå stordriftsfordeler og økt profesjonalisering. Allerede i 2008 innledet Finansdepartementet et prosjekt om hvordan organiseringen av datasentre og IT-infrastruktur i staten kunne effektiviseres og utnytte mulighetene for stordriftsfordeler med konsolidering av datasentre, med utgangspunkt i et regjeringsvedtak om å effektivisere statsforvaltningen gjennom økt samarbeid. Prosjektet identifiserte behov for felles datasentre med ny maskinvare som kunne sikre stabilitet for applikasjoner og tjenester, samt en ny organisering av IT-tjenestene. Resultatet ble opprettelsen av Statens IT (SIT), som fra 2010 leverte IT-tjenester til åtte departementer. I 2016 ble det vedtatt å utvide tilbudet til hele statsadministrasjonen, og Statens IT leverer i dag driftstjenester til 19 departementer og underliggende etater, med til sammen 35 000 brukere.[8] Tjenestene er i hovedsak arbeidsplassløsninger, it-drift, servicedesk og til en viss grad støtte til utvikling og sikkerhet hos kundene. Statens IT drifter totalt over 6000 servere. Et felles datasenter for Statens ITs brukere ble opprettet i 2013, fordelt på tre steder. (Kildebogaard, 2013). SIT leier også fasiliteter i et kommersielt datasenter lokalisert i Danmark (NNIT, 2021). Også i statsforvaltningen benyttes skytjenester i økende grad, men ifølge direktør Michael Ørnø i Statens IT (Haslund, 2020). er overgangen gradvis og det er i hovedsak nye systemer og tjenester som legges i skyen, fremfor at eksisterende løsninger flyttes fra egne servere. Statlige virksomheter har altså primært hybride løsninger, som bruker både skytjenester og egne servere. Infrastruktur og plattform som tjeneste (IaaS og PaaS) ses som vekstområder. Statens IT har selv investert i kompetansebygging på skytjenester og bygger også opp kapasiteten for å tilby rådgivning rundt informasjonssikkerhet på skyplattformer.

Som et svar på økt etterspørsel etter skytjenester fra kundene og økt oppmerksomhet rundt personvern- og sikkerhetsutfordringer har Statens IT utviklet GovCloud, en egen statlig skytjenesteplattform. GovCloud er en plattform som tjeneste som er utviklet og drevet av SIT, der applikasjoner og data til enhver tid befinner seg i SITs datasentre i Danmark (Statens IT, 2020). Prosjektet ble startet i 2018, da SIT i

[8] Se oversikt på statens-it.dk/om-os/hvem-leverer-vi-til/

samarbeid med DMI og DIGIST besluttet å etablere GovCloud-plattformen, først til service- og applikasjonsutvikling og deretter til drift av applikasjoner. GovCloud er en fleksibel utviklingsplattform som utvikles løpende med input fra kundene. DMI og DIGST var de første brukerne og ved utgangen av 2020 kjørte 17 statlige virksomheter pilotprosjekter på plattformen (Haslund, 2020). GovCloud er fortsatt i startfasen og klassifiseres i Statens ITs årsrapport for 2021 som et «utviklingsprosjekt under oppføring» (Statens IT, 2021, s. 33). SIT jobber med å videreutvikle løsningen, og som svar på økt etterspørsel etter skytjenester vil SIT gi kundene sine større tilgang til plattformen. I 2022 lanseres derfor en selvbetjeningsportal for GovCloud, som skal gi SITs kunder mulighet til å selv utvikle og administrer egne applikasjoner, i en «løsning, der er agil og i overensstemmelse med markedets standard og pris» (Statens IT, s. 20). GovCloud er basert på container-teknologi og benytter hovedsakelig åpen kildekode. Tjenesten er selvbetjent, slik at SIT kun administrerer infrastrukturen, mens kunden kan konsentrere seg om å utvikle, vedlikeholde og forbedre sine applikasjoner og overlate ansvaret for driftsplattformen til SIT. Integrasjon til SITs eksisterende driftsmiljø skal lette migrasjon av eksisterende applikasjoner til skyen og trinnvis videreutvikling av applikasjoner. Applikasjoner og data på GovCloud skal effektivt kunne flyttes til andre skyplattformer.

GovCloud skal muliggjøre bruk av flere ulike skyløsningen innenfor en felles ramme for databeskyttelse, datadeling, sikkerhet, i tillegg til innkjøp og administrasjon. Prosjektet har mål om å bidra til økt anvendelse av skyteknologier i offentlig sektor, og bidra til at utvikling av offentlig IT kan være økonomisk, rask, fleksibel og sikker (Statens IT, u.å.).

5.4 EU og Gaia-X

EU har ikke etablert en sentralisert skytjeneste, men har lenge hatt skytjenester på sin politiske agenda og fremmet initiativ til å utvikle og knytte sammen europeiske skyløsninger.

EU-kommisjonen lanserte i 2019 et initiativ for å utvikle en europeisk skytjenesteføderasjon (European Cloud Federation). En politisk deklarasjon om skytjenester (EU, 2020) ble signert av medlemslandene i oktober 2020. Deklarasjonen tar opp utfordringene med leverandøravhengighet og de amerikanske skytjenesteleverandørenes dominans og peker på behovet for økte investeringer i europeiske skytjenester. Deklarasjonen fremsetter et mål om å utvikle «neste generasjons EU-sky» som fyller behovene for både offentlig og privat sektor blant annet med tanke på datasikkerhet, mobilitet, interoperabilitet, transparens, åpenhet, datakraft, energieffektivitet og driftssikkerhet. For å oppnå dette setter landene og Kommisjonen som mål å investere i ny infrastruktur for skytjenester, knytte eksisterende skytjenester for offentlig og privat sektor sammen og definere felles regler for dem.

Dette initiativet omtales som den europeiske skytjenesteføderasjonen. Initiativet skal samle så mange samarbeidspartnere som mulig og drives av «European Alliance for Industrial Data, Edge and Cloud», som er opprettet av EU-kommisjonen (EU, 2021). Alliansen består av representanter fra medlemslandene, skytjenesteleverandører og -brukere og har som mandat å utarbeide planer for investering i og implementering av neste generasjons skytjenester, med utgangspunkt i eksisterende initiativer. Den skal utvikle regler og standarder for skytjenester kalt «EU Cloud Rulebook». Arbeidet er i en tidlig fase og alliansen hadde sitt første arbeidsmøte i desember 2021.

Ambisjonen er å knytte sammen eksisterende og fremtidige skyløsninger i både offentlig og privat sektor. Deklarasjonen nevner Gaia-X og en rekke eksisterende nasjonale initiativ for skytjenester for offentlig sektor i medlemslandene som et utgangspunkt for fremtidig samarbeid. Det er også et uttalt mål å modernisere skytjenester i offentlig sektor og koble sammen eksisterende nasjonale, regionale og lokale skytjenester for offentlig sektor på tvers av land – på frivillig basis og når det er hensiktsmessig - med et fremtidig mål om «pan-europeisk datalagring og -behandling [som kan] muliggjøre rask leveranse av offentlige tjenester til EUs innbyggere og bedrifter» (EU, 2020, s. 5).

Kommisjonen har vedtatt å bruke 2 milliarder euro i perioden 2021-2027 i sammenheng med den europeiske datastrategien på å skape neste generasjons skytjenester, og ser for seg samlede investeringer på opptil 10 milliarder euro på skytjenester og europeiske fellesområder for data (data spaces) i perioden. Satsingen er på et tidlig stadium, men EU har i 2022 blant annet lyst ut midler gjennom Connecting Europe Facility (CEF) for mulighetsstudier og utbygging og oppgradering av høyhastighets ryggradsnettverk for å knytte sammen skytjenesteleverandører, offentlige myndigheter og selskaper som drifter viktig infrastruktur (Connecting Europe Facility, 2022).

Gaia-X

Gaia-X er et initiativ for utvikling av en europeisk føderert datainfrastruktur. Målet er å skape et økosystem for brukere i både offentlig og privat sektor som sikrer digital suverenitet og sikkerhet gjennom implementering av felles regler og tekniske standarder. Gaia-X er altså ikke en skytjeneste, men skal koble sammen mange skytjenesteleverandører gjennom en arkitektur basert på prinsipper om føderering, distribuert konsensus, desentralisering og automatisert regulering (Gaia-X, 2022).

Initiativet startet som et Fransk-Tysk samarbeid. Ideen kom fra tyske industribedrifter som så et behov for europeiske skytjenester uten innlåsingseffekter og juridisk risiko (Melin 2021, s. 1). Gaia-X ble lansert i juni 2019 av de to landenes økonomi- og energiministre og involverte da 22 store selskaper, 11 franske og 11 tyske. Fra 2020 gikk Gaia-X inn i en ny fase som et tydeligere europeisk prosjekt og mål om å bli en åpen europeisk infrastruktur som representerer europeiske verdier på områder som personvern, datasikkerhet, dataportabilitet og digital suverenitet (Autolitano & Pawlowska, 2021). En egen stiftelse, Gaia-X AISBL, ble opprettet i juni 2020 med hovedkontor i Brussel. Høsten 2022 var over 350 bedrifter og organisasjoner fra en rekke land medlemmer, herunder en rekke skytjenesteleverandører og teknologiselskaper (Gaia X, 2022). Kun representanter for europeiske organisasjoner kan velges til styret i stiftelsen og det er planlagt et Governmental Advisory Board med representasjon fra EU-landene. Gaia-X skal likevel ikke være et lukket europeisk system, men legge til rette for å skape et åpent marked for skytjenester. Det er åpnet for medlemskap for organisasjoner også utenfor Europa, og en rekke store internasjonale IT-selskaper og skytjenesteleverandører er representert blant medlemmene, herunder Alibaba, AWS, Cisco, Ericsson, Fujitsu, Google, HP, Huawei, IBM, Intel, Microsoft, Oracle, Salesforce, SAP og VMware (Melin, 2021).

EU-kommisjonen (2020) henviser til Gaia-X i sin datastrategi og i deklarasjonen for European Alliance for Industrial Data, Edge and Cloud (EU, 2021), men EU er ikke involvert i finansiering eller styring (Melin, 2021, s. 2). Ifølge Gaia-X egenbeskrivelse kan prosjektet «ses som et forslag rettet mot Europa» og det pågår en intens dialog med EU-Kommisjonen om å tilpasse og harmonisere Gaia-X og satsingen på en kommende europeisk skytjenesteføderasjon, som European Alliance for Industrial Data,

Edge and Cloud arbeider med (Gaia-X, 2020). Nasjonale hub'er som samler interesserte aktører er etablert eller er under etablering i de fleste EU-landene.

Gaia-X finansieres av medlemmene og skal i hovedsak jobbe med å utvikle tekniske spesifikasjoner og harmonisere regelverk som muliggjør sikker lagring, og interoperabilitet og dataportabilitet mellom ulike leverandører av skytjenester. Dette innebærer blant annet tekniske krav, standarder for databruk, et kontroll- og styringssystem basert på programvare med åpen kildekode, og en godkjenningsordning for Gaia-X-tjenester.

En uttalt målsetting for Gaia-X er å «beskytte og øke den industrielle konkurransekraften [...] for det europeiske fellesskapet gjennom å redusere avhengighet og legge til rette for konkurranse» (Hoppe m.fl., 2020, s. 5). Gaia-X sikter mot å tilby et alternativ til de ledende amerikanske skytjenesteleverandørene og vektlegger transparens, sikkerhet og innebygget personvern. Dette skal oppnås ved å skape en desentralisert nettverksinfrastruktur som muliggjør sikker lagring, deling og behandling av data i hele Europa, i et økosystem som knytter sammen datasentre, skytjenesteleverandører, sektor-spesifikke skyløsninger og kantenheter (edge computing), i et føderert system. Gaia-X skal ikke selv bygge eller drifte maskinvaren i et slikt system, men legge forutsetningene for å knytte sammen leverandører og muliggjøre skalerbarhet, interoperabilitet og fritt valg av tilbydere. Løsningen skal være åpen og transparent, ha innebygd personvern og sikre datasuverenitet ved at brukerne har full kontroll og oversikt over behandlingen av egne data. Alle spesifiserte skytjenester skal baseres på programvare med åpen kildekode og leverandørene spesifiserer selv hvilke etablerte standarder for sikkerhet og personvern som tjenesten oppfyller.

Stiftelsen jobber med å utvikle pilotprosjekter innen en rekke bruksområder som industri, jordbruk, helse og mobilitet (Gaia X, 2022). Disse er per nå rettet hovedsakelig mot privat sektor, men det er også ambisjoner om at offentlige virksomheter skal ta i bruk Gaia-X. Den tyske skytjenestestrategien legger opp til at skytjenester i offentlig sektor skal kunne integreres med Gaia-X, og det er i det tyske Gaia-X hub'en nedsatt en arbeidsgruppe og utarbeidet et eget posisjonspaper for Gaia-X i offentlig sektor (Tysk Gaia-X Hub, 2021). Målet er å informere offentlige virksomheter om Gaia-X og understøtte offentlig-privat samarbeid som kan legge til rette for utvikling av løsninger som sikrer digital suverenitet, og det skal utredes hvilke krav offentlige virksomheter vil ha oppfylt for å ta i bruk til Gaia-X, og jobbes for at disse tas hensyn til i utviklingen av arkitekturen.

Det svenske Skatteverket har fulgt Gaia-X tett og vurderer at Gaia-X kan gi svenske myndigheter flere muligheter, dels ved at anskaffelsesprosesser av eksterne IT-tjenester kan forenkles når spesifikasjonene er åpne og sikrer konkurransenøytralitet, samtidig som Gaia-X legger til rette for at det tydeliggjøres hvordan skytjenester oppfyller ulike sertifiseringer, lover og regler. Det bemerkes at det:

> «kan även vara intressant att utreda om statlig it-drift kan använda sig av de specifikationer som tas fram inom Gaia-X för att på så sätt ta del av marknadens innovationskraft. Det skulle också kunna förenkla för myndigheter att dynamiskt välja leveransform, antingen från samordnad statlig it-drift, från kommersiella aktörer eller en kombination» (Melin, 2021, s. 10).

Det vises også til at rettstilstanden rundt overføring av opplysninger til tredjeland medfører at mange virksomheter ikke benytter skytjenester dersom de behandler personopplysninger eller gradert informasjon, og «Skatteverket noterat att om Gaia-X redan varit på plats hade det varit betydligt enklare att komma framåt för alla organisationer som vill använda molntjänster» (Melin).

Gaia-X ser dermed ut til å kunne utvikles til et aktuelt alternativ for offentlige virksomheters som vurderer å kjøpe skytjenester i markedet, og deltakelse er i prinsippet åpent for norske virksomheter. Samtidig er utviklingen av Gaia-X fortsatt på et svært tidlig stadium og utgjør i dag ikke noe alternativ til de store amerikanske skytjenesteleverandørene. En studie fra 2021 konkluderer med at det er «klart for tidlig å avgjøre om Gaia-X vil bli en suksess eller ikke» (Autolitano & Pawlowska, 2021, s. 14). Det svenske skatteverket (Melin, 2021, s. 9-10) viser tilsvarende til at en stor utfordring er at forventningene til stiftelsen så langt overstiger det som har blitt levert, og at det finnes en risiko for at interessen for prosjektet avtar dersom utviklingen tar for lang tid. Det har senere også blitt rapportert om misnøye med fremdriften og uenighet innad i arbeidsgruppene og anklager om at enkelte medlemmer, herunder organisasjoner som representerer ikke-europeiske teknologigiganter, primært driver lobbyvirksomhet og ikke ønsker at prosjektet lykkes (Westendarp & O'Brien, 2022).

6 Et veivalg for offentlig sektor

Strategier for skytjenester i offentlig sektor er ikke bare et spørsmål om teknologi og økonomi, det er også et politisk veivalg. En rekke hensyn må veies mot hverandre i utforming av strategi og valg av løsninger, herunder ulike kombinasjoner av tjenestekjøp i markedet, virksomhetsintern IKT og nasjonalt kontrollerte skyløsninger. Kostnadshensyn, fleksibilitet og innovasjon må veies mot personvernhensyn, autonomi, kompetansebygging og tillit til myndighetene. Optimale løsninger vil kombinere hensyn til alle disse verdiene. Dels står valget mellom outsourcing til markedet og statlig samordning og styring. Mer grunnleggende handler veivalget likevel om digital suverenitet og i hvilken grad myndighetene verdsetter og prioriterer dette. Om det ses som en kjerneoppgave for staten å hevde sin suverenitet også i det digitale domenet, vil hensyn til fleksibilitet og økonomi trumfes av kontroll med hvor data lagres og behandles, hvem som har tilgang og eierskap, samt innbyggernes tillit til systemet. Ulik betoning av truslene mot den digitale suvereniteten, antakelser om kostnadseffektivitet og ulike nasjonale forutsetninger har medført at vi blant våre naboland finner ulike modeller for skytjenester i offentlig sektor.

Der Norge hittil har ligget tett opptil Storbritannias markedsbaserte strategi med statlige virksomheter i rollen som bestiller av tjenester via en markedsplass for skytjenester, representerer Tyskland en tilnærming der digital suverenitet settes først. Begrunnelsen er ikke bare sikkerhet og kontroll over data, men også at offentlig sektor skal kunne være fleksibel i møte med nye utviklingstrekk, og en attraktiv arbeidsplass for de flinkeste IT-folkene. Den tyske strategien tar også utgangspunkt i at statens aktive rolle og drift av skytjenester i egen regi, kan gi økonomiske og praktiske fordeler.

Den nederlandske tilnærmingen er beslektet, men fremstår mer pragmatisk. Statlige datasentre og egne skytjenester for statsforvaltningen ble opprettet da det ble vurdert at markedet ikke kunne levere, verken med tanke på kostnadsbesparelser eller krav til personvern og datasikkerhet. Med et mer modent marked har myndighetene gradvis åpnet for en multi-cloud tilnærming der også allmenne skytjenester brukes for data med lavere beskyttelsesbehov.

Danmark ser ut til å nærme seg en kombinert strategi fra motsatt hold, og er i ferd med å opprette en skytjeneste for statsforvaltningen som respons på økt bruk av allmenne skytjenester og interesse fra virksomhetene. Danmark har tilsynelatende gode erfaringer med konsolidering av IT-tjenester og datasentre for offentlig sektor. Den statlige skytjenesten GovCloud er en relativt forsiktig tilnærming som kan gi en pekepinn om hvordan et første steg kunne sett ut for en statlig norsk skytjeneste. Begrunnelsen for satsingen inneholder koblinger til digital suverenitet i form av å etablere en ramme for databeskyttelse, datadeling og sikkerhet, samtidig som målet er en økonomisk, rask, fleksibel og sikker løsning.

Samlet peker erfaringene fra disse landene mot at en nasjonal skytjeneste vil være en realistisk mulighet også for norske myndigheter. Landene som har etablert nasjonale skytjenester vurderer at skytjenester i egenregi og konsolidering av IT-tjenester har redusert leverandøravhengighet og gjort forvaltningen bedre i stand til å møte nåværende og fremtidige behov, med skalerbare og fleksible IT-tjenester. Motivene

er i stor grad knyttet til digital suverenitet og sikkerhet, men også kostnadsbesparelser. De økonomiske effektene er vanskelige å vurdere, da det stort sett ikke er utført evalueringer før og etter slike satsinger. Ut fra beskrivelser gitt av ansvarlige myndigheter trenger kostnadene ikke være avskrekkende høye og skytjenester kan gi betydelige besparelser, særlig sammenliknet med intern IT-drift. Satsingene har også til en viss grad vært motivert av kompetansebygging. Utfordringer relatert til kompetansebehov har vært løsbare og vil etter alt å dømme også være det i Norge; NSM viser til at det finnes sterke fagmiljøer som vil kunne bære en slik satsing og NTL viser tilsvarende til at tilbakemeldinger fra medlemmer og tillitsvalgte tilsier at det finnes tilstrekkelig kompetanse i staten gitt at denne konsolideres[9].

Skytjenester ser ut til å være i ferd med å bli en uunngåelig standard for statlige og kommunale virksomheter også i Norge. Det er i stadig mindre grad et alternativ å velge skytjenester helt bort, spørsmålet er heller hvilke data og systemer i hver enkelt virksomhet som egner seg til behandling i skyen, hva virksomheten har lov til å flytte dit, og hvilke skyløsninger som velges.

De gjeldende politiske signalene til norske offentlige virksomheter kan oppsummeres med at «Regjeringen har i sine strategidokumenter sterkt oppfordret virksomheter i offentlig sektor til å ta i bruk skytjenester, men har presentert få motforestillinger mot å bruke slike tjenester» (Seip, 2020, s. 92). Økonomiske innsparinger, skalering, trygghet, energieffektivitet, fleksibilitet og innovasjon er hovedbegrunnelsene. Gjennomgangen i kapittel 2 viser at disse fordelene langt på vei også vil gjelde en nasjonal sky som eies og/eller driftes av offentlige myndigheter. Tydelige advarsler om konsentrasjonsrisiko, personvernutfordringer og behov for behandling fra datasentre i Norge, blant annet fra NSM, viser at også norske myndigheter i økende grad tar utfordringene ved de allmenne skytjenestene på alvor, og argumenter om digital suverenitet har gradvis blitt fremmet i den norske offentlige debatten.

Utredningsarbeidet som har foregått siden 2016 vil kunne få praktiske konsekvenser i form av en nasjonal skytjeneste om ikke lenge. Forutsetningene som er lagt for utredningen av en norsk nasjonal sky er likevel innsnevrende, og det er uvisst hvilket ambisjonsnivå en eventuell norsk nasjonal sky vil ha. Mandatet for KVU-arbeidet er avgrenset til skytjenester for statsforvaltningen, og omhandler ikke kommunal sektor. Avgrensningen mot både systemer for behandling av gradert informasjon (FDs tonivåplattform) og mot Markedsplassen for skytjenester, som anses å ivareta behovet med tanke på ikke-sensitiv annen informasjon, er også av avgjørende betydning for dimensjonering av en nasjonal sky. Løsningene som vurderes vil dermed av nødvendighet ha et begrenset omfang, selv om det ikke er utenkelig at en nasjonal sky kan utvides betydelig hvis den viser seg å bli en suksess. I en innledende fase vil et mindre omfang være hensiktsmessig, blant annet av hensyn til investeringskostnader, testing av nye løsninger, og nødvendig kompetansebygging. Omfang og kundegrunnlag påvirker likevel hvilken samfunnsmessig nytte en slik løsning vil kunne gi, i en mer moden fase. Eventuelle økonomiske besparelser knyttet til overgang til skytjenester og konsolidering av IT-drift er tett knyttet til skalering og stordriftsfordeler. Teknologisk forsprang og et stort tjeneste- og applikasjonsutvalg som gjør skytjenester attraktivt sammenlignet med intern IKT-drift, er også betinget av at skyløsningen, datasentrene og driftsmiljøene er av en viss størrelse.

Dersom en tar NSMs bekymring om for «den samlede nasjonale avhengigheten til utenlandske skyleverandører og hva denne avhengigheten kan medføre ved potensielle kriser og konflikter» på alvor, må en samtidig vurdere hvilke løsninger som kan

[9] Intervju med NSM, 20.06.2022; korrespondanse med NTL på e-post, 16.09.2022

bidra til å reelt redusere den samlede nasjonale avhengigheten. Jo skarpere avgrenset en nasjonal sikker sky er, jo mindre vil den bidra til å dempe den samlede avhengigheten av utenlandske skyleverandører.

Forutsatt at en statlig drevet skytjeneste kan gjøres konkurransedyktig på pris synes det å være grunn til å forvente sterk etterspørsel fra offentlige virksomheter (jf. 2.2). En eventuell nasjonal skytjeneste bør derfor så langt det er mulig tilrettelegges for å kunne utvides etter behov, med tanke både på nye tjenester og nye brukere. På grunn av kompleksiteten og kostnadene ved å etablere en statlig drevet nasjonal sky er det sannsynlig at en slik løsning i begynnelsen vil være begrenset i omfang. I så fall er det avgjørende at arkitekturen legger til rette for at nye bruksområder og kunder kan komme til, i tillegg til at skytjenester i offentlig sektor i så stor grad som mulig er kompatible med hverandre. Dette vil kunne muliggjøre deling, gjenbruk og videreutvikling av tjenester og applikasjoner på tvers av virksomhetene som benytter skyplattformen.

Det er også grunn til å stille et mer prinsipielt spørsmål ved i hvilken grad data *kan* beholdes og kontrolleres innenfor rammene av en liten nasjonalstat. Fra et norsk perspektiv kan det derfor være nødvendig å se digital suverenitet i en europeisk sammenheng. Som en liten nasjon er vi avhengige av et tett samarbeid med EU/EØS og et felles europeisk marked. Utviklingen i våre naboland og særlig på EU-nivå bør følges nøye, og det bør vurderes om Norge kan dra nytte av felles europeiske løsninger som Gaia-X og den europeiske skytjenesteføderasjonen. Foreløpig er disse likevel nærmere idéstadiet enn et reelt alternativ til de amerikanske skygigantene, som tar stadig større markedsandeler i Europa. Hvorvidt EUs ambisjoner for digital suverenitet manifesterer seg i reelle alternativ for norske offentlige virksomheter gjenstår å se.

Litteratur

A2. (2021). *Kartlegging av drift og forvaltning av IKT-løsninger i statlige virksomheter. Sluttrapport.* A-2 Norge AS.

Aukrust, Øyvind. (2022, 17. juli.) Nå blir det vanskeligere å bruke Chromebook i danske skoler. Frykter at personopplysninger når amerikanske myndigheter. *Aftenposten.* aftenposten.no/verden/i/KzodWE/naa-blir-det-vanskeligere-aa-bruke-chromebook-i-danske-skoler-frykter-at-personopplysninger-naar-amerikanske-myndigheter

Autolitano, S. & Pawlowska, A. (2021). Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study. *IAI-Papers*. Istituto Affari Internazionali (IAI), Roma, Italia. iai.it/sites/default/files/iaip2114.pdf

Berke, Jurgen. (2011, 17. desember). IT-Sicherheit: Friedrich will Bundes-Cloud aufbauen. *Wirtschafts Wocke*. wiwo.de/politik/deutschland/it-sicherheit-innenminister-friedrich-will-bundes-cloud-aufbauen/5965544.html

Beuth, Patric. (2018, 17. april). Deutsche Firma baut die Dropbox für den Bund. *Der Spiegel.* spiegel.de/netzwelt/web/open-source-software-nextcloud-baut-die-bundescloud-a-1203261.html

Brombach, Harald. (2016, 21. september). Microsoft åpner datasentre frie for amerikansk innsyn. *Digi.no.* digi.no/artikler/microsoft-apner-datasentre-frie-for-amerikansk-innsyn/358408

Brombach, Harald. (2020, 8. juni). Enda en tysk storby vil frigjøre seg fra Microsoft. *Digi.no* digi.no/artikler/enda-en-tysk-storby-vil-frigjore-seg-fra-microsoft/493652

Connecting Europe Facility (CEF). (2022). *Call for proposals CEF 2 Digital - Backbone networks for panEuropean cloud federation (CEF-DIG-2021-CLOUD).* Version 2.0 14. Mars 2022. ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/cef/wp-call/2021/call-fiche_cef-dig-2021-cloud_en.pdf

Direktoratet for forvaltning og økonomistyring (DFØ). (2021, 15, desember). *Om markedsplassen.* markedsplassen.anskaffelser.no/om-markedsplassen

Direktoratet for forvaltning og økonomistyring (DFØ). (2022, 2 juni 2022). *Status for markedsplassen for skytjenester - Statens innkjøpsforum 2022.* youtube.com/watch?v=xkeF5UYAu08

DICTU. (u.å.) Cloud. Hentet 18. juni 2022 fra https://dictu.nl/diensten/cloud

Direktoratet for forvaltning og IKT (Difi). (2017a). *Sikker sky (fase 2 del 2).* Upublisert.

Direktoratet for forvaltning og IKT (Difi) (2017b). *Vurdering av hvorvidt anskaffelsesregelverket (og tilknyttet EØS-lovgivning) legger begrensninger på offentlige virksomheters mulighet til å stille krav til nasjonal lagring og behandling av data*. Upublisert.

Direktoratet for forvaltning og IKT (Difi). (2018). Innkjøpsordning/markedsplass for skytjenester. Forprosjektrapport. (Difi-rapport 2018:6). Direktoratet for forvaltning og IKT.

Digitaliseringsstyrelsen. (2016). *Den fællesoffentlige digitaliserings-strategi 2016–2020*. digst.dk/strategier/digitaliseringsstrategien/.

Digitaliseringsstyrelsen. (2017). *Strategi for it-styring i staten*. digst.dk/strategier/strategi-for-it-styring-i-staten/

Digitaliseringsstyrelsen. (2018). *National strategi for cyber- og informationssikkerhed 2018–2021*. digst.dk/strategier/cyber-og-informationssikkerhed/.

Digitaliseringsstyrelsen. (2020). *Vejledning i anvendelse af cloudservices, version 1.1*. digst.dk/media/22430/vejledning-i-anvendelse-af-cloudservices-v11-juli-2020.pdf

Digitaliseringsstyrelsen. (2022). *Afrapportering for initiativ om Grønne Datacentre*. digst.dk/media/26780/digitaliseringsstyrelsens-afrapportering-for-initiativ-om-groenne-datacentre.pdf
Direktoratet for e-helse og Helsedirektoratet. (2021). *Helseopplysninger i skyen.* Helse- og omsorgsdepartementet.
Ehneß, Susanne. (2019, 25. juni). Welche Cloud-Dienste nutzt die Bundesverwaltung? *eGovernment Computing.* egovernment-computing.de/welche-cloud-dienste-nutzt-die-bundesverwaltung-a-840885/
EU. (2020). *Declaration: Building the next generation cloud for businesses and the public sector in the EU.* ec.europa.eu/newsroom/dae/redirection/document/70089
EU. (2021). *Declaration of the European Alliance for Industrial Data, Edge and Cloud*. EU-Kommisjonen. ec.europa.eu/newsroom/dae/redirection/document/78362
EU-Kommisjonen. (2020). *A European strategy for data*. (Meddelelse fra Kommisjonen til Europaparlamentet, Rådet, det europeiske økonomiske og sosiale utvalg og Regionsutvalget). EU-Kommisjonen.
Føyen Torkildsen AS. (2015). *Utredning av juridiske forhold ved bruk av nettsky i kommunal sektor – en mulighetsstudie.* (KS FoU-prosjekt 144008). KS.
Gaia-X. (2022). About Gaia-X. Hentet 3. august fra gaia-x.eu/what-is-gaia-x/about-gaia-x/
Ghaffar, H. T. A. N. (2020). Government Cloud Computing and National Security. *Review of Economics and Political Science*. Vol. ahead-of-print No. ahead-of-print. doi.org/10.1108/REPS-09-2019-0125
Hanssen, N. (2019, 14 mars). Fagforbundet vil ha kontrollen med offentlige data tilbake i etatene - og inviterer NTL til felles initiativ. *Fri Fagbevegelse.* frifagbevegelse.no/ntlmagasinet/fagforbundet-vil-ha-kontrollen-med-offentlige-data-tilbake-i-etatene--og-inviterer-ntl-til-felles-initiativ-6.158.617207.b58ba04742
Haslund, Alexander. (2018, 2. november). Danske kommuner satser stort på cloud computing: "Det kan ikke længere betale sig for os at have servere stående selv". *Computerworld.* computerworld.dk/art/245228/danske-kommuner-satser-stort-paa-cloud-computing-det-kan-ikke-laengere-betale-sig-for-os-at-have-servere-staaende-selv
Haslund, Alexander. (2020, 16. november). Her er Michael Ørnøs cloud-planer for Statens It: "Du ser ikke os drage over hals og hoved ind i noget cloud". *Computerworld.* computerworld.dk/art/254173/her-er-michael-oernoes-cloud-planer-for-statens-it-du-ser-ikke-os-drage-over-hals-og-hoved-ind-i-noget-cloud
Hauge-Eltvik, Anders. (2020, 11. februar). Nå får tyskerne sin egen skytjeneste for lagring av all offentlig informasjon. *Fri Fagbevegelse*. frifagbevegelse.no/aktuell/na-far-tyskerne-sin-egen-skytjeneste-for-lagring-av-all-offentlig-informasjon-6.158.678855.cdeb734c7a
Hillenius, Gilles. (2017). Open source makes Dutch government cloud a reality. *EU-Kommisjonen, Open Source Observatory (OSOR).* joinup.ec.europa.eu/collection/open-source-observatory-osor/document/open-source-makes-dutch-government-cloud-reality.
Hoppe, Gerd m.fl. (2020). GAIA-X: A Pitch Towards Europe. Status Report on User Ecosystems and Requirements. Berlin, BMWi, May 2020. data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-a-pitch-towards-europe.html
Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. Big *Data & Society*, 8(1). doi.org/10.1177/20539517209820
Irain, M., Jorda, J. & Mammeri, Z. (2017). Landmark-based data location verification in the cloud: Review of approaches and challenges. *Journal of Cloud Computing* 6(1): 1–20.
Irion, K. (2012). Government cloud computing and the policies of data sovereignty. *Policy & Internet* 4(3-4): 40-71.

IT-Planungsrat. (2020). *Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung; Eckpunkte – Ziel und Handlungsfelder*. Resolusjon fra det 31. møtet i IT-Planungsrat. it-planungsrat.de/fileadmin/beschluesse/2020/Beschluss2020-19_Entscheidungsniederschrift_Umlaufverfahren_Eckpunktepapier.pdf
IT-Planungsrat. (2021a). *Germany's government cloud strategy – The federal approach.* FITKO.
IT Planungsrat. (2021b). *Germany's government cloud strategy: Target architecture framework.* FITKO.
ITZBund (u.å.). *Der Bundesclient – ein standardisierter IT-Arbeitsplatz für die digitale Verwaltung*. Hentet 13.05.2022 fra itzbund.de/DE/itloesungen/egovernment/bundesclient/bundesclient_node.html#title2333681
ITZBund. (2020. 4. februar). *Software nach einheitlichen Standards und Methoden in der Cloud entwickeln*. itzbund.de/SharedDocs/Pressemitteilungen/DE/2020/2020-04-02_BC_Entwicklungsplattform.html
ITZBund. (2022). *ITZBund in Zahlen.* itzbund.de/DE/dasitzbund/ueberuns/ueberuns.html
Justisministeriet. (2020). *Vejledning om lokationskravet i databeskyttelsesloven.* datatilsynet.dk/Media/E/5/Vejledning%20om%20lokationskravet%20i%20databeskyttelsesloven.pdf
Kildebogaard, Jesper. (2013, 23. april). Statens It: Vi sparer fire millioner om året på strøm med nyt datacenter. *Version2.* version2.dk/artikel/statens-it-vi-sparer-fire-millioner-om-aaret-paa-stroem-med-nyt-datacenter
KMD. (u.å.). *SKI Rammeavtaler.* Hentet 15.06.2022 fra kmd.dk/loesninger-og-services/it-services/ski-rammeaftaler
Kommunal- og moderniseringsdepartementet. (2016). *Nasjonal strategi for bruk av skytjenester*.
Kommunal- og moderniseringsdepartementet. (2022). *Digitaliseringsrundskrivet.* Rundskriv H-5/21. regjeringen.no/no/dokumenter/digitaliseringsrundskrivet/id2895185/
KS. (2020). KS Fiks-plattformen. Versjon:2.0. developers.fiks.ks.no/fiks-plattformen.pdf
Melin, Daniel. (2021). *Delrapportering av regeringsuppdrag att bevaka Gaia-X*. Skatteverket. bluesciencepark.se/wp-content/uploads/2021/09/Gaia-X-delrapport-juni-2021.pdf
Nationaal Cyber Security Centrum. (2018). *A cyber secure Netherlands. National Cyber Security Agenda*. english.ncsc.nl/binaries/ncsc-en/documenten/publications/2019/juni/01/national-cyber-security-agenda/National-Cyber-Security-Agenda.pdf
Nederlands innenriksdepartement. (2011). *Informatie- en communicatietechnologie (ICT).* Mld. til parlamentet 26643, No. 179. Brev fra innenriksdepartementet. zoek.officielebekendmakingen.nl/kst-26643-179.html
Nederlands regjering. (2011). *Vernieuwing van de rijksdienst [Reform av forvaltningen]* Mld. til parlamentet 31490, no. 54. https://zoek.officielebekendmakingen.nl/kst-31490-54.html.
Nederlands regjering. (2019). *NL DIGITAAL: Data Agenda Government*. nldigitalgovernment.nl/wp-content/uploads/sites/11/2019/04/data-agenda-government.pdf
Nederlands regjering. (2020). *Strategische i-agenda Rijksdienst 2019–2021*. open.overheid.nl/repository/ronl-c91d925c-2933-4750-a061-e542fa810fbd/1/pdf/strategische-i-agenda-rijksdienst-2019-2021-editie-2020.pdf
Nederlands regjering. (2022). *Digital Government Agenda*. nldigitalgovernment.nl/digital-government-agenda/
Nederlands Riksrevisjon. (2019). *Staat van de rijks-verantwoording 2019*. rekenkamer.nl/publicaties/rapporten/2020/05/20/staat-van-de-rijksverantwoording-2019.
Nexia Management Consulting. (2015). *Kartlegging og analyse av landskapet for offentlige datasenter i Norge.* Kommunal- og moderniseringsdepartementet.

NIST. (2011). The NIST Definition of Cloud Computing. NIST Special Publication 800-145. National Institute of Standards and Technology.
NNIT. (2021, 14. januar). Statens IT flytter ind. mynewsdesk.com/dk/nnit/news/statens-it-flytter-ind-418931
NORA, Nedelands Overheid Referentie Architectur. (2022). *BIO Theme Cloud services - Summary AIVD position and policy exploration BZK*. noraonline.nl/wiki/BIO_Thema_Clouddiensten/Standpunt_AIVD_en_beleidsverkenning_BZK
NSM. (2016). *Sikker sky*. Upublisert. Nasjonal Sikkerhetsmyndighet.
NSM. (2017). *Sikker sky fase 2*. Upublisert. Nasjonal Sikkerhetsmyndighet.
NSM. (2020a). *Helhetlig digitalt risikobilde 2020*. Nasjonal Sikkerhetsmyndighet.
NSM. (2020b, 12. august). *Spørsmål om sky og tjenesteutsetting*. Nasjonal Sikkerhetsmyndighet. nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/ofte-stilte-sporsmal-om-sky-og-tjenesteutsetting/sporsmal-om-sky-og-tjenesteutsetting/
NSM. (2022). *Risiko 2022*. Nasjonal Sikkerhetsmyndighet.
ODC-Noord. (u.å.). Historie ODC-Noord. Hentet 5. juni 2022 fra odc-noord.nl/historie-odc-noord/
Olifent, Louise. (2022, 10. juni). Tross løfter om ny data-avtale: København tør ikke flytte på enormt sky-prosjekt. *Digi.no.* https://www.digi.no/artikler/tross-lofter-om-ny-data-avtale-kobenhavn-tor-ikke-flytte-pa-enormt-sky-prosjekt/520179
Røise, M.B. (2022, 29. januar). Stockholm mener det er for problematisk å ta i bruk Microsoft 365. *Digi.no.* digi.no/artikler/stockholm-mener-det-er-for-problematisk-a-ta-i-bruk-microsoft-365/516820?key=RNIKBEqt
Regjeringen (2021). *Hurdalsplattformen*. Statsministerens kontor.
Rekkedal, K., A. og Forseth, G. F. (2021, 4. juli). Arkivloven begrenser bruken av skytjenester. *Finansavisen*. finansavisen.no/nyheter/debattinnlegg/2021/07/04/7696125/arkivloven-begrenser-bruken-av-skytjenester
Schaer, Cathrin. (2020, 14. mai). Linux not Windows: Why Munich is shifting back from Microsoft to open source – again. *ZDNet.* zdnet.com/article/linux-not-windows-why-munich-is-shifting-back-from-microsoft-to-open-source-again/
Seip, Å. A. (2020). *Sourcingstrategier for IKT i offentlig sektor. Om skytjenester og digitale veivalg i fire statlige virksomheter og fire kommuner*. Fafo-rapport 2020:17. Fafo.
SOU 2021:1 *Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering. Delbetänkande av It-driftsutredningen.* Statens Offentliga Utredningar, Infrastrukturdepartementet.
Stach, Heike. (2020, 11. februar). *Data storage as a federal responsibility*. Innlegg på eForvaltningskonferansen 2020. Tilgjengelig på youtube.com/watch?v=hzx2MIRQYBs
Statens IT. (u.å.). Om GovCloud. Hentet 17.06.2022 fra govcloud.dk/om-govcloud/D
Statens IT. (2020). *Servicespecifikation GovCloud*. govcloud.dk/media/11706/servicespecifikation-govclouddk.pdf
Statens IT, 2021
Statens IT. (2022). *Mål og Resultatplan 2022.* statens-it.dk/media/11844/maal-og-resultatplan-2022.pdf
Meld. St. 27 (2015–2016). Digital agenda for Norge. IKT for en enklere hverdag og økt produktivitet. Kommunal- og distriktsdepartementet.
Stupp, C. (2015, 15. august). Germany to set up 'Bundescloud'. EURACTIV. euractiv.com/section/digital/news/germany-to-set-up-bundescloud/
Strand, L. (2020). *Norge i den digitale skyen: En beredskapsmessig tåkeheim?* Nasjonal Sikkerhetsmyndihget. https://nsm.no/hold-deg-oppdatert/meninger/norge-i-den-digitale-skyen-en-beredskapsmessig-takeheim
The Cloud Report. (2022, 31. mai). Google Cloud and Central Dutch Government Sign Workspace Agreement. cloud.report/featured-news/google-cloud-and-central-dutch-government-sign-workspace-agreement

Tysk Gaia-X Hub. (2021). *Gaia-X Domain Public Sector Position Paper Version 1.0 2021*. bmwk.de/Redaktion/EN/Publikationen/Digitale-Welt/211116-pp-public.pdf?__blob=publicationFile&v=3

Watts, S., & Raza, M. (2019, 6 15). SaaS vs PaaS vs IaaS: What's The Difference and How To Choose. Hentet 4. mai, 2022 fra bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-differenceand-how-to-choose/

Weng, Ditte Vinterberg. (2022, 17. mars). Efter Schrems II-vejledning fra Datatilsynet: Københavns Kommune forsøger at finde løsning sammen med Microsoft på kæmpe cloud-omstilling. *Computerworld*. computerworld.dk/art/260160/efter-schrems-ii-vejledning-fra-datatilsynet-koebenhavns-kommune-forsoeger-at-finde-loesning-sammen-med-microsoft-paa-kaempe-cloud-omstilling

Westendarp, L. og O'Brien, P. (2022, 20. juli). Gaia-X board member blames lobbying for project's gridlock. *Politico.* politico.eu/article/eu-lobbying-cloud-project-gaia-x-board-member-says-cloud-project-must-neuter-lobbies-role-to-get-on-track/

Skytjenester for offentlig sektor

Denne rapporten diskuterer problemstillinger knyttet til digital suverenitet og muligheten for en offentlig eid nasjonal skytjeneste.

I tråd med anbefalinger i Regjeringens strategidokumenter kjøper offentlige virksomheter i økende grad skytjenester i markedet og disse understøtter allerede en rekke viktige offentlige tjenester. Dette reiser spørsmål blant annet knyttet til fremtidig avhengighet av leverandører, datasikkerhet, personvern og juridisk risiko fordi data lagres utenlands, eller behandles av leverandører underlagt andre lands jurisdiksjon. Rapporten diskuterer prinsipielle avveininger nasjonale myndigheter står ovenfor ved valg av eierskapsmodeller og organisering av skyløsninger. Hvilke vurderinger har norske myndigheter gjort, og hvordan har andre land valgt å innrette skytjenester for offentlig sektor? Rapporten oppsummerer kunnskapsgrunnlaget på feltet og ser nærmere på erfaringer fra Tyskland, Nederland og Danmark, som i ulik grad benytter egne statlige skytjenester.

Fafo

Borggata 2B
Postboks 2947 Tøyen
N-0608 Oslo
www.fafo.no

Fafo-rapport 2022:22
ID-nr.: 20825