Fafo

Åsmund Arup Seip

Sourcingstrategier for IKT i offentlig sektor

Om skytjenester og digitale veivalg i fire statlige virksomheter og fire kommuner

Fafo-rapport
2020:17

Åsmund Arup Seip

Sourcingstrategier for IKT i offentlig sektor

Om skytjenester og digitale veivalg i fire statlige virksomheter og fire kommuner

Fafo-rapport 2020:17

Fafo-rapport 2020:17

ISBN 978-82-324-0563-3 (papirutgave)
ISBN 978-82-324-0564-0 (nettutgave)
ISSN 0801-6143 (papirutgave)
ISSN 2387-6859 (nettutgave)

Omslag: Photo by Sam Schooler on Unsplash
Trykk: Allkopi Netprint AS

Innhold

Forord

Skytjenestene spiller i dag større og større rolle i utviklingen av IKT og digitale tjenester, og markedet domineres av noen store aktører. Den norske regjeringen oppfordrer statlige virksomheter til å benytte seg av skytjenester. Hvilke fordeler og hvilke ulemper mener offentlige virksomheter følger med skytjenestene, hvilke alternativer finnes, og hvilke utfordringer står virksomhetene overfor?

Denne rapporten er skrevet på oppdrag fra NTL og Fagforbundet. Fafo har gjennomført intervjuer i fire statlige virksomheter og fire kommuner, og målet har vært å undersøke hvilke strategier for bruk og anskaffelse av IKT offentlige virksomheter følger. Rapporten berører også spørsmål om sikkerhet og nasjonal kontroll over offentlige data og hvilken kompetanse som er nødvendig og tilgjengelig for offentlige virksomheter.

Noen av resultatene fra denne undersøkelsen ble presentert på NTLs e-forvaltningskonferanse i februar 2020. Jeg vil rette en stor takk til alle som har satt av tid og bidratt gjennom å delta i intervjuene denne 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 Kristin Alsos som har lest rapporten og stilt kritiske spørsmål, og Fafos publikasjonsavdeling som på kort tid har klart å ferdigstille rapporten.

Oslo, august 2020
Åsmund Arup Seip

Sammendrag

Denne rapporten handler om sourcingstrategier for IKT og bruk av skytjenester i offentlig sektor i Norge. Undersøkelsen bygger på intervjuer i fire statlige virksomheter og fire kommuner, dokumenter stilt til rådighet av virksomhetene og kommunene og en gjennomgang av offentlige dokumenter som beskriver myndighetenes politikk og utredninger på området.

Den digitale utviklingen har gått i retning av økt bruk av digitale tjenester levert over internett, såkalte skytjenester. Samtidig har nye plattformer som mobil, nettbrett og bærbare pc-er gjort at kommunikasjon over internett har blitt svært nyttig. Under koronakrisen våren 2020 har vi i hele verden sett en vekst i bruken av videotjenester og skybasert kommunikasjon. Digitaliseringen av biler, hjem og gjenstander vi omgir oss med, «the Internet of things», genererer data. Denne utviklingen har ført med seg et behov for transport og lagring av store mengder informasjon som kan lagres i digitale «skyer».

De moderne nettskyene ble introdusert med skytjenester fra Amazon (2006), Google (2008) og Microsoft (2010), og uttrykket «skytjenester» eller «cloud computing» brukes i dag som en samlebetegnelse på datatjenester som leveres over internett, og kan omfatte alt fra regnekraft (dataprosessering) og datalagring til operativsystemer og programvare. Bruk av gamle dataprogrammer eller bruk av dataprogrammer fra ulike leverandører eller plattformer kan skape det som har blitt kalt «teknisk gjeld», og gjøre deling og utveksling av data vanskelig. Skytjenestene representerer i dag et forsøk på å overkomme mange av disse utfordringene ved å integrere et bredt spekter av tjenester og knytte dem sammen over internett.

Datasikkerhet

Levering av digitale tjenester over nett gir oss utfordringer både i måten vi arbeider og organiserer vår virksomhet på, og i hvordan vi sikrer persondata og andre data av verdi for virksomheter eller Norge som nasjon. I Norge tilpasser vi vår lovgivning til EUs reguleringer når det gjelder salg av tjenester og regulering av personvern. For de fleste formål er EU-landene ett marked

og et felles reguleringsområde for IKT og personvernspørsmål. Men i et globalt marked handler vi ofte utenfor EUs grenser.

Informasjonssikkerhet kan kompromitteres, og offentlige eller private interesser kan krenkes på to ulike måter ved outsourcing av IKT-tjenester: Data kan bli kompromittert gjennom rettslige prosesser under et annet lands jurisdiksjon, og det kan skje ved ulovlig inntrenging eller tilegnelse av informasjon.

Dersom data lagres steder der det vil kunne komme inn under et annet lands jurisdiksjon, vil norske myndigheter eller norske virksomheter kunne miste kontrollen over egne data. Uklarhet om jurisdiksjon kan utgjøre et sikkerhetsproblem. Dette har ført til at EU har relativt strenge regler for overføring av persondata ut av EU/EØS-området. Når det gjelder andre typer data, må den enkelte dataeier og det enkelte land sikre sine data juridisk. Det kan være krevende dersom data lagres i andre land.

Ulovlig inntrenging i dataanlegg, såkalt hacking, er et betydelig problem som berører all IKT. En viktig grunn til at hacking og spionasje rettet mot IKT-tjenester foregår, er at data kan ha stor verdi. Virksomheter, både i det offentlige og i det private, må verne om sine data for å unngå at industrielle hemmeligheter, forskningsmateriale eller samfunnskritisk informasjon kommer på avveie. For nasjonalstaten er den nasjonale sikkerheten viktig.

Et eksempel på beskyttelse av data for å sikre nasjonal suverenitet finner vi Tyskland der myndighetene har valgt å etablere sin egen «private» sky – Die Bundescloud. Målet er å skape uavhengighet av eksterne leverandører som gikk over fra å selge dataprogrammer til å levere leie- eller abonnementstjenester. I Tyskland er digital autonomi blitt et sentralt mål i digitaliseringspolitikken.

En norsk strategi for skytjenester

I Norge har regjeringen lagt en strategi for å øke digitaliseringstakten og ta i bruk skytjenester. Regjeringen Solberg har gjennom en rekke publikasjoner og tiltak lagt et betydelig press på hele offentlig sektor for å øke digitaliseringen og få virksomhetene til å ta i bruk ny teknologi og skytjenester.

Regjeringen peker på at offentlig sektor har et spesielt behov for kontroll over informasjon, og peker på to veier å gå for å ivareta offentlig kontroll. Den ene er gjennom å etablere egne datasentre for statlig eller offentlig sektor. Den andre veien regjeringen foreslår å gå, er å sikre offentlig kontroll gjennom kontrakter som blir inngått med leverandører.

Parallelt med overgang til markedsbaserte skytjenester i offentlig sektor, og etablering av en offentlig markedsplass for slike tjenester, foregår det et

betydelig arbeid med å samordne offentlige digitale tjenester. Et eksempel er Norsk helsenett som er blitt skilt ut fra Direktoratet for e-helse for å bli en nasjonal leverandør av e-helsetjenester.

Samlet sett kan vi se de offentlige tiltakene som en blandingspolitikk: både markedsorientering og offentlig samordning. Regjeringen sier imidlertid lite i de offentlige dokumentene om hvilke generelle prinsipper som skal ligge bak valg av strategi.

Statlige virksomheter

Forsvaret, Meteorologisk institutt, Nav og Universitetet i Bergen er statlige virksomheter som representerer ulike sektorer i staten, har ulik størrelse og ulike driftsoppgaver.

Forsvarets IKT-strategi, som også handler om sourcing, er bygget opp rundt de internasjonale trendene innen IKT-utvikling: en mer strategisk bruk av IKT, integrasjon og kommunikasjon mellom systemer og jevnlig oppgradering og modulbygging. Det er et mål for Forsvaret å øke den digitale kompetansen innenfor IKT og gi de ulike etatene i forsvarssektoren større grad av frihet til å velge hvordan de vil jobbe. Et tredje mål er å utnytte nye plattformer. Her har Forsvaret søkt et samarbeid med Microsoft.

Meteorologisk institutt (MET) behandler store mengder data for å overvåke og varsle været for myndighetene, næringslivet og allmennheten. De siste årene har Meteorologisk institutt valgt å anskaffe programvare gjennom skyløsninger på det administrative området. Instituttet har lagt tre hovedlinjer i sin sourcingstrategi: ta i bruk og utvikle egne IT-ressurser knyttet til kjernevirksomheten, kjøpe tjenester og programvare i markedet når det er kostnadseffektivt, og samarbeide nasjonalt og internasjonalt for å opprette og vedlikeholde kompetanse og kapasitet innenfor instituttets kjernevirksomhet. For Meteorologisk institutt er det viktig å sikre kjernekompetanse slik at det kan drifte og utvikle sin hovedaktivitet. Hovedprinsippet for innkjøp av tjenester og programvare er at det bør foreligge et modent marked med flere tilbydere. Sourcingstrategien går også ut på å unngå å bli låst til én leverandør og å utnytte mulighetene for samarbeid nasjonalt og internasjonalt.

Arbeids- og velferdsetaten (Nav) leverer tjenester etter arbeidsmarkedsloven og folketrygdloven og har 750 årsverk knyttet til sin sentrale IT-avdeling. Navs sourcingstrategi har som formål å maksimere verdiskapningen gjennom bruk av egne ressurser i kombinasjon med kjøp av standardiserte programmer eller kjøp av tjenester. Etaten beveger seg bort fra store monolittiske datasystemer og over til mer mikrotjenestearkitektur med små komponenter

som kan endres etter behov. Dette skal ifølge etaten opprettholde endringsdyktighet over tid. Navs strategi er å bygge opp utviklingstjenestene selv og sette mer av driften ut i skyen. En suksessfaktor er å klare å utvikle og beholde kompetanse.

IT-avdelingen ved Universitetet i Bergen har litt over 100 ansatte. Virksomheten har et behov for tjenester over et bredt spekter og har organisert disse ved å ta i bruk ulike typer infrastruktur. For å kunne tilby en kostnadseffektiv skytjeneste har Universitetet i Bergen og Universitetet i Oslo samarbeidet om å lage en egen skytjeneste med bruk av egne servere for sine brukere. Dette er ifølge universitetet en løsning som gir god kontroll med data. Universitetet i Bergen har valgt å kjøpe tjenester der volumet er stort, for eksempel Microsoft 365 med tilknyttet skylagring. Universitetets sourcingstrategi omfatter administrative og tekniske tjenester og er utformet som en veiledning for beslutninger knyttet til hvorvidt tjenester skal utføres med interne ressurser, skaffes gjennom tjenestekjøp eller organiseres gjennom et samarbeid med en ekstern virksomhet.

Kommuner

Oslo og Bergen er de to største bykommunene i landet, mens Bodø og Fauske kan beskrives som en middels stor og en liten bykommune.

Bergen kommune hadde tidligere et driftsmiljø for IT i hver etat, men kommunen har over tid arbeidet målrettet for å samle driften av IKT i en konsernfunksjon. Kommunen har ikke en fastlagt sourcingstrategi, men kan sies å følge en multisourcingstrategi for drift og innkjøp av digitale tjenester. For kommunen er utviklingen og etableringen av de nye fellestjenestene i offentlig sektor en viktig faktor som vil avgjøre hvor drift og lagring av data vil skje i framtiden. Kommunens driftssystemer som har vært driftet med små endringer over tid, utfordres nå av mer dynamiske systemer som leveres via sky og oppdateres og utvikles kontinuerlig. I tillegg vil informasjonssikkerhet, inntrengingssikkerhet og personvern, ifølge kommunen, være styrende for hvordan de arbeider med de digitale tjenestene i framtiden.

Bodø kommune har de siste 15–20 årene satt bort drift av hele IT-systemet til en driftspartner. En av utfordringene ved utsetting av tjenester er behovet for god merkantil kompetanse. Selv om kommunen opplever å ha god teknisk kompetanse, er utformingen og forvaltningen av avtaler utfordrende, ifølge kommunen. Sikkerhet er et sentralt spørsmål i en sourcingstrategi. Kommunen påpeker at kompetansen til de enkelte brukerne er en kritisk faktor. Sikkerhetsstandarden til større internasjonale leverandører blir vurdert som god.

Fauske kommune har valgt å drifte sine IT-tjenester selv, men har ikke utformet en egen sourcingstrategi. Kommunen opplever at det er en utfordring å få til kompatibilitet mellom de systemene kommunen bruker i dag, og nye skyløsninger. Det sak- og arkivsystemet kommunen bruker, passer for eksempel ikke sammen med Googles desktop-produkter. Slike forhold gjør det vanskelig for kommunen å gjøre endringer. Kommunen peker på at egen IT-drift gjør kommunen mindre avhengig av leverandører for support.

I Oslo kommune leverer Utviklings- og kompetanseetaten IT-tjenester til 50 virksomheter. Utviklingen har gått i retning av å samle IT-kompetansen i én etat, men flere andre virksomheter har fortsatt egne IT-medarbeidere og egne systemdriftsmiljøer. Oslo kommune har valgt å gå over fra å eie infrastrukturen selv til å gå i retning av tjenestekjøp. Målet var å utvikle en multisourcingstrategi med flere skyleverandører. Kommunen peker imidlertid på at det ble utfordrende å operere med mange skyleverandører. Erfaringen er at leverandørene er ganske like, og at kommunen ikke får mer funksjonalitet gjennom å operere med flere leverandører, men at det kan bli vanskelig å sette krav til standardisering, og at det kan bli mer kostbart å forholde seg til flere grensesnitt.

Sourcingstrategier og utviklingstrekk

Virksomhetene i denne undersøkelsen har i ulik grad utformet egne sourcingstrategier for IKT. Ingen av kommunene har utformet en skriftlig sourcingstrategi, men enkelte har formulert en utviklingsretning gjennom svært generelle formuleringer. Virksomhetenes erfaringer viser likevel at det er noen felles utviklingstrekk knyttet til organisering og sourcing av IKT i offentlig sektor:

- Mens datadrift i stor grad tidligere har blitt sett på som en støttefunksjon til virksomhetens tjenesteproduksjon, ses den nå i økende grad som en integrert del av de tjenestene virksomheten ønsker å tilby.
- Det har det foregått en økende sentralisering av IKT-driften. Dette er særlig tydelig i de store kommunene Oslo og Bergen. Sentraliseringen er likevel ikke entydig. Den nye arkitekturen som nye IT-systemer bygges etter, åpner for at datasystemene kan utvikles i mindre biter, som byggeklosser. Det har gjort det mulig å etablere selvstendige utviklingsteam som jobber tett med brukere. Nav og Forsvaret kan være eksempler.
- Virksomhetene retter oppmerksomheten og egen datadrift mot kjernevirksomheten. Dette er særlig framtredende i de statlige virksomhetene

som utfører spesialiserte oppgaver. Det blir også påpekt at data knyttet til kjernevirksomheten har stor verdi for virksomheten og må beskyttes.

- Myndighetene krever samordning av IKT-løsningene på visse områder innenfor det offentlige. Kommuner og statlige virksomheter møter på flere felt et krav om samordning, enten om å ta del i nasjonale fellesløsninger eller å bli del av et felles økonomi- og styringssystem innenfor den enkelte sektoren.
- Virksomhetene i denne undersøkelsen opplever et krav fra politisk og overordnet myndighet om å etablere skydrift for ulike tjenester. Det har blitt understreket i flere år gjennom digitaliseringsrundskrivet. Virksomhetene har forsøkt å følge opp dette pålegget.

Denne undersøkelsen av fire statlige virksomheter og fire kommuner viser at de offentlige virksomhetene har organisert sin IKT-drift på ulike måter, og at sourcingstrategiene varierer. De fleste virksomhetene har tatt i bruk skytjenester på ett eller flere felt. Skytjenestene har vist seg å være enkle å bruke, og de utvikles ofte sømløst underveis slik at brukeren alltid har siste versjon av tjenesten. Virksomhetene opplever imidlertid også ulemper med skytjenester. Dette kan være risiko for å bli låst til en tjeneste, høy pris eller problemer med å få nødvendige tilpasninger.

Virksomhetene vurderer sikkerheten ved bruk av skytjenester og lagring i skyen i lys av den type data som skal lagres, og legger stor vekt på at personvernreguleringen (GDPR) følges opp. Her er spørsmålet om hvor data lagres, viktig.

Virksomhetene understreker at det er veldig viktig å ha kompetanse som kjenner til hva virksomheten driver med. Hvis Norge skal ligge langt framme innenfor visse fagområder, er det avgjørende, påpekte virksomhetene, at Norge kan håndtere data selv og foreta kjøringer som er kritiske for virksomhetene. Det genererer kompetanse og kontroll.

Regjeringen har lagt til rette for å organisere en offentlig innkjøpsordning eller markedsplass for skytjenester. Regjeringen har ikke lagt til rette for et samarbeid om offentlig datalagring eller etablering av et felles datasenter for statlig eller offentlig sektor. 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. Kanskje er det tid for å starte en debatt om dette. I framtiden vil eierskap og kontroll over data legge grunnlag for store verdier. Det vil også være en

vei til makt og innflytelse. Derfor er det viktig å drøfte hvordan vi skal regulere disse verdiene, og hvordan vi skal forvalte de verdiene som skapes i det offentlige.

Summary

This report examines sourcing strategies for ICT and the use of cloud services in the public sector in Norway. The study is based on interviews held with four state agencies and four local authorities, as well as documents provided by these parties and a review of official documents describing the government's policies and reports in the area.

The digital development has led to an increase in online digital services, known as cloud services. New platforms such as mobile phones, tablets and laptops also mean that communication via the internet has become a very useful tool. During the height of the coronavirus pandemic in the spring of 2020, we saw worldwide growth in the use of video services and cloud-based communication. The digitisation of cars, homes and objects we surround ourselves with, the 'internet of things', generates data. This development has led to a need for the transfer and storage of large volumes of data that can be stored in digital "clouds".

The modern-day clouds were introduced as cloud services from Amazon (2006), Google (2008) and Microsoft (2010), and the terms 'cloud service' and 'cloud computing' are used today as generic terms for online data services, and can include everything from computing power (data processing) and data storage, to operating systems and software. Using old computer programs or computer programs from different suppliers or platforms can create what has been termed "technical debt", and can represent a barrier to sharing and exchanging data. The cloud services of today seek to overcome many of these challenges by integrating a wide range of services and linking them together over the internet.

Data security

The provision of online digital services presents us with challenges both in the way we work and organise our activities, and in how we secure personal data and other sensitive data of commercial or national value. In Norway, legislation on the sale of services and the regulation of privacy is adapted to

EU regulations. In most cases, the EU member states represent a single market and a common regulatory area for ICT and privacy issues. However, in a global market, we often operate outside the EU's borders.

Information security can be compromised and public or private interests can be violated in two different ways when ICT services are outsourced: data can be compromised through legal proceedings under another country's jurisdiction, and as a result of illegal access to or acquisition of information.

If data is stored in places where it could fall under another country's jurisdiction, the Norwegian authorities or businesses could lose control of their own data. Uncertainty related to jurisdiction can pose a problem for security. Consequently, the EU has relatively strict rules for transferring personal data out of the EU/EEA. With regard to other types of data, the individual data owner and the individual country must legally secure their data. However, this can be a challenge if the data is stored in other countries.

Illegally accessing computer systems, known as hacking, is a major problem that affects all ICT. One of the main reasons why hacking and espionage aimed at ICT services take place is that data can be of great value. Public and private sector actors must protect their data in order to prevent industrial secrets, research material or critically important socioeconomic information from falling into the wrong hands. For the nation state, national security is important.

One country where data is protected to safeguard national sovereignty is Germany, where the authorities have chosen to establish their own 'private' cloud – Die Bun-descloud. The aim is to be independent from external suppliers who previously sold software but now provide leasing or subscription services. In Germany, digital autonomy has become a key goal in digitalisation policy.

A Norwegian strategy for cloud services

In Norway, the government has devised a strategy to increase the pace of digitalisation and use of cloud services. Through a number of publications and measures, the Solberg government has put considerable pressure on the entire public sector to hasten digitalisation and to adopt new technology and cloud services.

The government points out that the public sector has a special need to have control over information, and points to two ways of maintaining public control. One is by establishing separate data centres for the state or public sector. The other method proposed by the government to safeguard public control is through contracts with suppliers.

In parallel with the transition to market-based cloud services in the public sector, and the establishment of an official market place for such services, considerable efforts are underway to coordinate digital services in the public sector. One such example is the *Norsk Helsenett*, which has been demerged from the Norwegian Directorate of eHealth in order to serve as a national supplier of e-health services.

Overall, we can view the measures as a mixed-market policy: both a market-based orientation and public sector coordination. However, the government's documents give little indication of the general principles that should be applied in the choice of strategy.

State agencies

The Norwegian Armed Forces, the Norwegian Meteorological Institute (MET), the Norwegian Labour and Welfare Administration (NAV) and the University of Bergen are state agencies that represent different sectors within the state, and whose size and operations vary.

The Norwegian Armed Forces' ICT strategy, which also covers sourcing, is based on the international trends in ICT developments: a more strategic use of ICT, integration and communication between systems, and regular upgrades and module building. The Armed Forces aim to increase the digital competence within ICT and give the various agencies in the defence sector a greater degree of freedom to choose how they want to work. They also aim to make use of new platforms, and to this end have approached Microsoft with a view to forming a collaboration.

MET processes large volumes of data in order to monitor and forecast the weather for the authorities, the business community and the general public. In recent years, MET has chosen to procure software through cloud solutions in the administrative area. It has laid out three main strands in its sourcing strategy: adopting and developing its own IT resources related to the core activity, procuring services and software in the market when this proves to be cost-effective, and forming national and international collaborations in order to establish and maintain competence and capacity within MET's core activity. It is important for MET to ensure core competence so that it can operate and develop its main activity. The main principle for the procurement of services and software is that there should be a mature market with several suppliers. MET's sourcing strategy also aims to ensure that it is not locked into one supplier and to take advantage of the opportunities for collaboration nationally and internationally.

NAV provides services in accordance with the Labour Market Act and the National Insurance Act, and labour input in its central IT department corresponds to 750 full-time equivalents. NAV's sourcing strategy aims to maximise value creation through the use of its own resources in combination with the purchase of standardised software or the procurement of services. The agency is moving away from large monolithic computer systems towards a more micro-service architecture with small components that can be modified as needed. According to NAV, this will maintain its adaptability over time. NAV's strategy is to build up its own development services and place more of the operational activities in the cloud. Being able to develop and retain competence is critical to the success of its strategy.

The IT department at the University of Bergen has just over 100 employees. The university needs a wide range of services and has adopted different types of infrastructure to accommodate these. In order to be able to offer a cost-effective cloud service, the University of Bergen and the University of Oslo have jointly created a cloud service that uses dedicated servers for their users. According to the universities, this solution enables them to ensure good control of their data. The University of Bergen has chosen to procure services where there are large volumes of data, such as Microsoft 365 and the associated cloud storage. The university's sourcing strategy includes administrative and technical services, and is designed to serve as a guide for decisions related to whether services should be performed using internal resources, outsourced or organised as a collaboration with an external partner.

Local authorities

Oslo and Bergen are the two largest urban municipalities in Norway, while Bodø and Fauske can be described as a medium-sized and a small urban municipality respectively.

Bergen local authority previously had IT operations in every agency, but over time has worked actively to assemble ICT activities in a single group function. Bergen local authority does not have an established sourcing strategy, but can be said to follow a multi-sourcing strategy for the operation and procurement of digital services. For the local authority, the development and establishment of the new shared services in the public sector is an important factor that will determine where data operations and storage take place in the future. The local authority's IT systems, which have been subject to small modifications over time, are now being challenged by more dynamic systems that are delivered via cloud services and continuously being updated and developed. In addition, the local authority says that its use of digital services in

the future will be determined by the need for information security, access security and personal data protection.

For the past 15–20 years, Bodø local authority has been outsourcing all of its IT services to an operating partner. One of the challenges associated with outsourcing services is the need for good commercial expertise. Even though the local authority has good technical expertise, it still considers the framing and management of agreements to be a challenge. Security is a key issue in a sourcing strategy. Bodø local authority points out that the expertise of the individual users is a critical factor. Major international suppliers are considered to have a good standard of security.

Fauske local authority has chosen not to outsource its IT services, but has not devised a sourcing strategy. The fact that its own systems are not always compatible with new cloud systems is a challenge. For example, the document and archive system used by Fauske local authority is not compatible with Google's desktop products. These kinds of issues make it difficult for the local authority to make changes. It points out that keeping its own IT operations in-house makes it less dependent on suppliers for support.

In Oslo local authority, the Agency for Improvement and Development provides IT services for 50 municipal departments. The development has moved towards assembling IT expertise in one agency, but several other departments still have their own IT staff and systems operation. Oslo local authority has chosen to switch from owning the infrastructure itself to procuring services. The goal was to develop a multi-sourcing strategy with several cloud service suppliers. However, the local authority acknowledges that using several cloud service suppliers became problematic. It found that because the suppliers are quite similar, using several suppliers did not add to the functionality of the IT systems. It was also difficult to set requirements for standardisation, and dealing with a number of different interfaces tends to be more costly.

Sourcing strategies and development trends

The participants in this survey have, to varying degrees, devised their own sourcing strategies for ICT. None of the local authorities have formulated a written sourcing strategy, but some have framed a direction for development in a very general sense. Nevertheless, the participants' experiences show that there are some common development trends in the organisation and sourcing of ICT in the public sector:

- While computer operations have been viewed largely as a support function

for service production in the past, they are now increasingly being regarded as an integral part of the services offered.

- There has been an increasing centralisation of ICT operations. This is particularly evident in the large municipalities of Oslo and Bergen. However, this centralisation is not uniform. The new architecture on which new IT systems are based, enables the computer systems to be developed in smaller modules, like building blocks. This has made it possible to establish independent development teams that work closely with the users. NAV and the Norwegian Armed Forces are such examples.
- The focus and in-house computer operations are aimed at the core activity. This is particularly evident in the state agencies that perform specialised tasks. It is also noted that data related to the core activity has a high value for the data owner and must be protected.
- The authorities require coordination of ICT solutions in certain areas within the public sector. Local authorities and state agencies meet the requirement for coordination in several areas, either by taking part in national shared solutions or by being part of a common financial and management system within the individual sector.
- The participants in this survey consider it to be a requirement from higher-level political authorities to establish cloud operations for various services. This has been a focus for several years through the Digitalisation Memorandum. The survey participants have tried to comply with the directive.

This survey shows that the four state agencies and four local authorities have organised their ICT operations in different ways and that their sourcing strategies vary. Most use cloud services in one or more areas. The cloud services have proven to be easy to use, and they are often developed seamlessly on an ongoing basis such that the user always has the latest version of the service. However, the survey participants also experience disadvantages with cloud services, such as a risk of being locked into one supplier, high prices and problems related to achieving the necessary customisations.

The survey participants assess the security of the use of cloud services and storage in the cloud in light of the type of data to be stored, and place a great deal of emphasis on compliance with the General Data Protection Regulation (GDPR). The question of where data is stored is important in this context.
The survey participants emphasise the importance of having expertise that understands their work. If Norway is to be at the forefront in certain areas,

the participants consider it to be vital for Norway to be able to handle its own data and undertake critical IT work, thereby generating expertise and ensuring control.

The government has facilitated the organisation of a public procurement scheme or market place for cloud services. The government has not facilitated a data storage collaboration for the public sector or the establishment of a common data centre for the public sector. There is little indication in the government's digitalisation strategy or strategy for the use of cloud services that assessments have been made in relation to digital autonomy or to the need to ensure digital competence in the public sector. Perhaps it is time to start a debate on this. In the future, ownership and control of data will be valuable commodities. They will also be a path to power and influence. It is therefore important to discuss how we should regulate these values and manage the values that are created in the public sector.

1 Innledning

Uttrykket «skytjenester» eller «cloud computing» brukes som en samlebetegnelse på datatjenester som leveres over internett, og kan omfatte alt fra regnekraft (dataprosessering) og datalagring til operativsystemer og programvare. Skytjenestene er en del av det vi kaller 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.

De siste ti årene har det foregått en vekst i skytjenester på bekostning av tradisjonelle IKT-tjenester. Både private og offentlige virksomheter har i økende grad skiftet ut egne servere, operativsystemer og programvare med skybaserte datatjenester. Denne prosessen kan beskrives som en overgang fra varebasert innkjøp til tjenestebasert innkjøp av IKT. Mens det har vært vanlig at offentlige virksomheter har kjøpt inn datautstyr og programvare, og driftet dette selv, åpner skytjenestene for at mer og mer IKT kan leveres som tjenester og over internett.

En slik transformasjon av IKT i offentlige virksomheter kan endre virksomhetenes drift og måte å operere på. Det kan ha betydning for hvilken kompetanse virksomhetene trenger, kostnader ved kjøp av tjenester og beslutninger om hvordan IKT skal styres i virksomheten. Det kan også ha betydning for sikkerheten. Dette gjør det viktig å forstå i hvilken grad det skjer en overgang til skytjenester, hvorfor det skjer, og hva som er fordeler og ulemper ved skytjenester. Slik kunnskap kan danne grunnlag for å drøfte hvilke konsekvenser de teknologiske endringene har for offentlig sektor og for samfunnet som helhet.

Sourcing handler om å hente ressurser fra ulike steder og benyttes i vanlig tale om å produsere tjenester selv eller kjøpe tjenester ute. Insourcing og outsourcing handler om å flytte tjenester inn i virksomheten eller ut av virksomheten. En sourcingstrategi kan dermed defineres som en plan for hvilke tjenester virksomheten skal produsere selv med egne ansatte, og hvilke tjenester som skal kjøpes inn fra eksterne leverandører.

De politiske målene for bruk av skytjenester og økt digitalisering i offentlig sektor er ganske tydelige. I 2016 la regjeringen fram en nasjonal strategi for

bruk av skytjenester. I forordet peker daværende kommunal- og moderniseringsminister Jan Tore Sanner på at bruk av IKT og digitalisering av tjenester vil bli en viktig del av en mer kostnadseffektiv offentlig sektor. Regjeringens mål med å legge fram strategien var å fremme bruk av skytjenester i offentlig sektor. Den ønsket at offentlige virksomheter skulle vurdere skytjenester som et alternativ når de skulle anskaffe IKT-tjenester (Kommunal- og moderniseringsdepartementet, 2016).

I januar 2018 ble Nikolai Astrup utnevnt til landets første digitaliseringsminister. Året etter la han sammen med styreleder i KS Gunn Marit Helgesen fram en digitaliseringsstrategi for offentlig sektor for årene 2019–2020, *Én digital offentlig sektor* (Kommunal- og moderniseringsdepartementet, 2019). Strategien presenterer felles mål og innsatsområder for digitaliseringsarbeidet fram mot 2025. Offentlig sektor skal i framtiden i økende grad dele data og etablere et felles «økosystem» for nasjonal digital samhandling som skal kunne legge grunnen for mer sammenhengende tjenester. Men regjeringen så også for seg et styrket samarbeid med privat sektor (Kommunal- og moderniseringsdepartementet, 2019, s. 43). Digital sikkerhet var også en del av strategien. Her ble det lagt vekt på beskyttelse mot uønskede hendelser, en robust digital infrastruktur og ivaretakelse av personvern.

For å fremme overgang til skytjenester stadfestet regjeringen i Jeløyaplattformen at den ville etablere en markedsplass for skytjenester, og i samarbeid med Direktoratet for forvaltning og IKT har departementet begynt arbeidet med å etablere en markedsplass for skytjenester (Difi, 2018).

Dette er de politiske målene. Hvordan følges disse opp? Velger virksomhetene i offentlig sektor skytjenester framfor andre IKT-løsninger? Hvordan organiserer de i praksis sin drift av IKT? Denne rapporten ser på sourcingstrategiene og utfordringene knyttet til skytjenester og IKT-drift i fire statlige virksomheter og fire kommuner. I framstillingen vil betegnelsen offentlig virksomhet bli bruk både om statlige virksomheter og kommuner. Følgende problemstillinger står sentralt i framstillingen:

- Hva er de politiske signalene for den statlige og kommunale politikken på IKT-området?
- Hvordan organiserer de statlige virksomhetene og kommunene driften av IKT?
- Hvilke innkjøpsstrategier- og innkjøpsvurderinger (sourcing) er viktige for virksomhetene og kommunene?

- Hvilke vurderinger gjør virksomheten av hvordan data lagres (skytjenester/driftsansvar/nasjonalitet/sikkerhet)?
- Hvordan vurderer virksomhetene og kommunene kompetansesituasjonen (drifts-, utviklings- og innkjøpskompetanse)?
- Legges det opp til offentlig IKT-samarbeid?

2 Om undersøkelsen

Denne undersøkelsen bygger på intervjuer i fire statlige virksomheter og fire kommuner, dokumenter stilt til rådighet av virksomhetene og kommunene og informasjon fra virksomhetenes og kommunenes nettsider. I tillegg er det foretatt en gjennomgang av offentlige dokumenter, blant annet NOU-er og stortingsmeldinger, som beskriver myndighetenes politikk og utredninger på området.

De offentlige virksomhetene som er med i denne undersøkelsen, ble valgt ut i samarbeid med oppdragsgiver. Det har vært en målsetting å belyse virksomheter av ulik karakter og ulik størrelse. Samtidig har det blitt lagt vekt på at noen av virksomhetene står oppe i betydelige endringsprosesser når det gjelder innkjøp av IKT-utstyr og IKT-tjenester. Det er gjennomført til sammen ti intervjuer med representanter for de ulike virksomhetene. De fleste intervjuene ble gjennomført med IT-direktøren eller andre som er ansvarlig for virksomhetens IKT-virksomhet eller innkjøp. Intervjuet i Bergen kommune ble gjennomført med to informanter til stede. Ved Universitetet i Bergen og i Fauske kommune ble det gjennomført to intervjuer der det ene var med en IT-ansatt som også var tillitsvalgt. Nedenfor følger en liste over alle intervjuene.

I intervjuene ble det stilt relativt åpne spørsmål om hvilke skytjenester virksomheten benytter i dag, herunder hvordan IKT-tjenestene er organisert. Det ble også stilt spørsmål om virksomheten har en sourcingstrategi for skytjenester, og om den eventuelt har vurdert behovet for slike tjenester. Videre ble datasikkerhet, kompetansebehov og fordeler og ulemper ved skytjenester berørt. Virksomhetene fikk også spørsmål om de så et behov for en felles offentlig markedsplass for skytjenester.

Teksten som omhandler de enkelte virksomhetene, bygger på disse intervjuene og på tilgjengelig informasjon fra dokumenter og nettsider. Teksten er ment å presentere virksomhetens synspunkter og er ikke en analyse eller fullstendig beskrivelse av virksomhetens IKT-drift. Enkelte steder er det gjengitt uttalelser fra intervjuene, men i all hovedsak er uttalelsene gitt i intervjuene gjengitt i løpende tekst som er forenklet og syntetisert. Personene

som er intervjuet, har fått tilsendt teksten og har fått mulighet til å lese gjennom og korrigere feil. Det kan likevel forekomme feil eller misforståelser, og disse er forfatterens ansvar alene.

Følgende personer er intervjuet:

Virksomhet	Stilling	Dato
Forsvarsdepartementet	spesialrådgiver	07.01.2020
Meteorologisk institutt	IT-direktør	17.12.2019
Nav	IT-direktør	03.01.2020
Universitetet i Bergen	IT-direktør	09.01.2020
Universitetet i Bergen	senioringeniør/tillitsvalgt	14.01.2020
Bergen kommune	direktør	14.01.2020
Bergen kommune	leder	14.01.2020
Bodø kommune	IT-direktør	08.01.2020
Fauske kommune	driftsansvarlig IKT	08.01.2020
Fauske kommune	IT-konsulent/tillitsvalgt	08.01.2020
Oslo kommune	direktør	13.01.2020

3 En digital utvikling mot skyen

Den digitale utviklingen går fort. Før vi ser på hvordan enkelte offentlige virksomheter har organisert sin IKT-virksomhet, og hva slags sourcingstrategi de har lagt, skal vi peke på noen generelle utviklingstrekk i den digitale verden og se på hvorfor skytjenestene har blitt så populære. Vi skal også berøre spørsmål om sourcing og sikkerhet.

Et viktig kjennetegn ved denne utviklingen er at flere bruker internett som kommunikasjonsarena. Da regjeringen la fram sin stortingsmelding om en digital agenda for Norge i 2016, hadde internett rundt 3 milliarder brukere (Meld. St. 27, 2015–2016, s. 13). I 2019 var dette tallet økt til 4,5 milliarder (Internet Word Stats, 2020). Mer og mer av all samhandling i verden foregår over nett.

Et annet viktig utviklingstrekk er at plattformene vi samhandler på, endrer seg. Mens andelen som har en pc eller laptop, har ligget relativt konstant de siste årene, har andelen som bruker nettbrett og smarttelefon, økt. Dette gjelder både i Norge og i verden sett under ett, og i dag går rundt halvparten av all internettrafikk i verden over mobile plattformer som mobiltelefon og nettbrett (Broadbandsearch, u.d.; Statistisk sentralbyrå, u.d.). Samtidig har internett blitt raskere både gjennom utbyggingen av bredbånd og gjennom byggingen av 4G mobilnett. Denne utviklingen gjør at både programvare og måten vi samhandler på, endrer seg. Et uttrykk for dette er overgangen fra kommunikasjon via e-post til kommunikasjon på sosiale media og via ulike meldingstjenester som er lett tilgjengelige også på mobil. Dette skjer også i offentlig sektor. Oslo kommune har tatt i bruk Workplace, som leveres av Facebook, som verktøy for internkommunikasjon i kommunen.

Under koronakrisen våren 2020 har vi i hele verden sett en enorm vekst i bruken av videotjenester og skybasert kommunikasjon. I Norge har virksomheter både i privat og offentlig sektor hatt utstrakt bruk av hjemmekontor, og begrensninger i reisevirksomheten har ført til at ansatte har kommunisert og samarbeidet gjennom videokonferanser, for eksempel i Zoom og Teams. Mange av disse tjenestene henger sammen i skyløsninger. Det gjør det mulig

å kombinere en rekke tjenester innenfor den samme samhandlingsplattformen, for eksempel videosamtaler med visning og deling av dokumenter, bruk av meldingstjenester eller ulike prosjekt- eller styringsverktøy. Alle ansatte kan lett få tilgang til dokumenter fra en pc uten at det opprettes private nettverkslinjer (VPN) med tilgang til virksomhetens servere. Koronakrisen har vist at skybaserte løsninger kan være svært effektive både når det gjelder kommunikasjon over avstander, og når det gjelder integrasjon av virksomhetenes ulike IKT-verktøy. Dataselskapet Visma skriver at koronakrisen har gjort tilgangen til digitale verktøy ikke bare viktig, men kritisk (Visma blogg, 2020).

Et kjennetegn ved utviklingen er at det stadig genereres nye data. Det er ikke bare vi mennesker som genererer data når vi er på internett. Etter hvert blir flere og flere ting utstyrt med sensorer som genererer data. I en moderne mobiltelefon er det en rekke sensorer som blant annet fanger opp temperatur, fuktighet, lufttrykk, akselerasjon, rotasjon og nærhet når du legger telefonen mot kinnet. Sensorene måler antall skritt du tar, hvor fort du går, og hvor du er, og finnes i alt fra enkle røykvarslere til avanserte roboter. Mange er knyttet sammen over internett, slik at det blir mulig å lese av sensorene i datamaskiner, samle opp tidsserier av informasjon og kombinere data fra flere kilder. Bygging av framtidige 5G mobilnett skal gjøre overføring av slike data enda lettere. Dette er tingenes internett, og det vokser raskt. Det er ikke mulig å si eksakt hvor mye data som genereres, men en beregning viser at det i 2020 trolig vil genereres rundt 145 000 GB per person hver dag (Petrov, 2019). For å ta vare på alle disse dataene og gjøre dem tilgjengelige trengs store felles lagringsplasser som er koblet sammen over internett. Her har nettskyene fått en betydelig rolle.

Selv om skytjenester har aner tilbake på 1990-tallet, ble de moderne nettskyene (cloud computing) og skytjenestene introdusert fra 2006 da Amazon etablerte sitt datterselskap *Amazon Web Service* (AWS). To år senere lanserte Google sin tjeneste *Google App Engine*, som er en skybasert plattform for utvikling og drift av nettjenester, og i 2010 lanserte Microsoft sin skytjeneste *Azure* (Wikipedia, u.d.). I dag er disse tjenestene videreutviklet og bygget ut, og sammen med andre selskaper leverer de skytjenester over nett som dekker svært bredt.

Uttrykket «skytjenester» brukes i dag om flere ulike typer tjenester. Betegnelsen kan brukes om datasentre eller servere som er tilgjengelige for mange brukere via et nettverk. Et vanlig kjennetegn er at skytjenesten leveres over internett, det vil si fra et annet sted enn der operatøren holder til. Vi kan

skille mellom tre ulike typer skytjenester (Kommunal- og moderniseringsdepartementet, 2016; Watts & Raza, 2019):

- Programvare som tjeneste (SaaS – Software as a Service), for eksempel tekstbehandlingsprogrammer, regnskapsprogrammer eller CRM-programmer (Customer Relationship Management). Microsoft 365 (tidligere Microsoft Office 365) og Dropbox er eksempler på programvare levert som tjeneste. Når du kjøper programvare som tjeneste, er det vanligvis tjenesteleverandøren som har ansvar for alt, oppretting av nettforbindelse, lagring, servere, virtualisering[1], operativsystemet, hjelpeprogrammer (middleware), at det virker hele tiden, og at programmet blir oppdatert og feil rettet.
- Plattform som tjeneste (PaaS – Platform as a Service), for eksempel databaser, operativsystem, utviklingsverktøy. Google App Engine og Microsoft Azure er eksempler på plattformer levert som tjeneste. Når du kjøper plattform som tjeneste, leverer tjenesteleverandøren vanligvis nettforbindelse, lagring, servere, virtualisering, operativsystem og hjelpeprogrammer, men ikke selve programvaren som håndterer data.
- Infrastruktur som tjeneste (IaaS – Infrastructur as a Service), for eksempel lagring, dataservere, regnekapasitet som stilles til rådighet over nettet. Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine er eksempler på tjenester som kan levere infrastruktur. Når du kjøper infrastruktur som tjeneste, leverer tjenesteleverandøren vanligvis bare nettforbindelse, lagring, servere og virtualisering.

Disse ulike tjenestene kan leveres som skytjenester på flere måter. De kan leveres fra en allmenn sky (Public Cloud), det vil si kommersielle skytjenester som i prinsippet er tilgjengelige for alle. Amazon, Google og Microsoft Azur er blant de største. Skytjenester kan også leveres fra en privat sky (Private Cloud) som bare brukes av én virksomhet eller i et samarbeid mellom noen virksomheter (gruppesky). En virksomhet kan dessuten benytte seg av tjenester levert i en kombinasjon av en allmenn og privat sky (hybridsky).

[1] Virtualisering betyr å opprette virtuelle utgaver av datamaskinressurser som så framstår for brukeren som tilsvarende fysiske ressurser. Virtualisering kan gjøre det mulig å kjøre flere operativsystemer på samme maskin uten å starte opp på nytt eller at én stor datamaskin kjører separate systemer for mange brukere på en gang. Virtualisering gjør det lettere og billigere å skalere opp og ned tjenesten etter behov.

Skytjenestene har de siste årene blitt utviklet på stadig flere felt, og vi finner dem nå nesten over alt. Hva har gjort dem så populære? En måte å forstå dette på er gjennom å se på hva som ligger i metaforen «teknisk gjeld».

3.1 Teknisk gjeld og behovet for endring

«Teknisk gjeld» er en metafor som av og til brukes for å beskrive uferdige eller unødvendig kompliserte løsninger som hindrer effektiv drift. Ikke sjelden er det da snakk om utdaterte IKT-løsninger. Uttrykket «teknisk gjeld» sies å stamme fra Ward Cunningham og arbeidet med dataprogrammering på begynnelsen av 1990-tallet (Letouzey & Whelan, 2019). I det øyeblikk man begynner å kode et dataprogram som skal gi inntekter i framtiden, begynner man å etablere en «teknisk gjeld». Alt arbeidet som går med til å vedlikeholde dette dataprogrammet, kan ses som en rente på den tekniske gjelden. Blir vedlikeholdsarbeidet for stort eller effektiviteten av dataprogrammet for liten i forhold til andre dataprogrammer, vokser den tekniske gjelden og blir tyngende for virksomheten.

Metaforen gir et bilde på betydningen av å holde ved like og oppdatere eller skifte ut IT-elementer som er foreldet. Dette er et kontinuerlig arbeid som skyløsningene i dag har gjort lettere. Oppdatering av programvaren i bilen Tesla kan tjene som eksempel. Dette kan i mange tilfeller gjøres over mobilnettet. I stedet for å innkalle tusenvis av biler til verksted for å foreta en oppdatering av bilens dataprogram, kan dette gjøres i løpet av noen timer mens bilen står i eierens garasje. Vedlikehold og utvikling av programvare kan også gjøres langt billigere når det gjøres samtidig, og på samme måte, for mange brukere på en gang.

Måten dataprogrammene bygges på, er også en annen i dag. Store systemer består i dag oftere av mange mindre deler som kan skiftes ut eller endres uavhengig av helheten. Små hyppige oppdateringer har tatt over for større periodevise oppgraderinger.

Ved å ta i bruk teknologi binder man seg til visse valg og begynner dermed å opparbeide en «teknisk gjeld». Da Trygdeetaten, som det den gang het, på slutten av 1970-tallet bestemte at beregningen av trygdeytelser skulle skje med databehandling, ble det utviklet et eget dataprogram for dette. Navs IT-system for trygdeytelser feiret i 2018 40 år. Systemet stammer fra den gangen arbeidsledighetstrygden ble utbetalt kontant til folk som ventet i kø. Det ble introdusert i 1978 og er gjennom årene blitt bygget ut til å kunne håndtere stadig flere trygdeytelser. Infotrygd ble utbygget og tilpasset etter hvert som

nye behov oppsto og informasjonsteknologien utviklet seg, men dataprogrammet ble også etter hvert en hemsko for utvikling av nye digitale tjenester og en «teknisk gjeld» som har kostet Nav mye i utviklingstjenester.

I dag krever vi noe annet av et dataprogram enn det vi gjorde i 1978. Mens det tidligere var vanlig å gjennomføre kjøringer periodevis, for eksempel ved månedlige utbetalinger, er det gjerne et mål for dagens og morgendagens systemer at deling av data og uthenting av informasjon kan skje i sanntid. Da Direktoratet for e-helse, som er et fag- og myndighetsorgan underlagt Helse- og omsorgsdepartementet, skulle beskrive kunnskapsbehovet og satsingsområdene, la direktoratet vekt på at det måtte skapes en felles grunnmur for digitale tjenester (Direktoratet for e-helse, u.å., s. 26):

> «Den nasjonale IKT-grunnmuren må styrkes for å kunne realisere digitale samhandlingsløsninger mellom virksomheter i sektoren.»

Direktoratet for e-helse mente kunnskapen om nye lagringsteknologier og distribuerte systemer måtte styrkes. Disse kunne åpne for nye måter å lagre data på, blant annet bruk av skytjenester og deling av data i tilnærmet sanntid. Denne teknologien vil etter direktoratets syn kreve et særlig blikk på personvern, men vil kunne åpne for tjenester med stor nytteverdi for fellesskapet (Direktoratet for e-helse, u.å., s. 27).

Spørsmålet om deling av data er viktig for både offentlig og privat sektor. I februar 2020 nedsatte regjeringen en ekspertgruppe som skal se på utfordringene og mulighetene som ligger i deling av data i næringslivet og mellom offentlig og privat sektor. Statsråd Helleland ville dele data for å skape gode tjenester og arbeidsplasser i hele landet (Kommunal- og moderniseringsdepartementet, 2020):

> «Mange i offentlig sektor er godt i gang med å dele og tilgjengeliggjøre data. Fremover blir det viktig med samarbeid i og med næringslivet om denne jobben. Vi tror at jo mer data som deles, jo større blir nytten for samfunnet.»

Deling og utveksling av data i sanntid krever at dataprogrammene kan «snakke sammen», og at de er knyttet sammen i nettverk. Bruk av gamle dataprogrammer eller bruk av dataprogrammer fra ulike leverandører eller plattformer kan skape det som har blitt kalt «teknisk gjeld», og gjøre deling og utveksling av data vanskelig. Skytjenestene representerer i dag et forsøk på å overkomme mange av disse utfordringene ved å integrere et bredt spekter av tjenester og knytte dem sammen over internett.

3.2 Utvikling fra varer til tjenester

Den digitale utviklingen har også gjort det lettere å selge tjenester. Mens datamaskiner og dataprogrammer tidligere i all hovedsak kunne regnes som varer man betalte for og beholdt som en eiendel, blir de samme funksjonene nå levert som tjenester man betaler for når man bruker dem, eller som en abonnementstjeneste som leveres så lenge man betaler et abonnement. Slike digitale tjenester kan nær sagt leveres fra hvor som helst i verden.

Denne globaliseringen har vidtrekkende konsekvenser. Mens handel med varer på tvers av verdenshavene alltid har hatt betydning for Norge, er det et relativt nytt fenomen at også handel med tjenester har fått så stort volum. Amerikanske selskaper som Facebook, Google og Microsoft leverer nå tjenester i Norge både gjennom å være til stede og på nett over landegrensene. Der hvor virksomheter tidligere kjøpte en stor datamaskin som kunne håndtere virksomhetens programmer og dekke behovet for regnekapasitet, blir nå både håndteringen av programmer og regnekapasiteten ofte kjøpt over nett som en tjeneste. Slike tjenester kan gjerne bli fakturert fra Dublin, mens virksomhetens data kanskje lagres på en server i Prineville i Oregon i USA. IKT-tjenester er dermed blitt en viktig del av den internasjonale handelen, og både markeder, regulering og mulighetene for kontroll er dermed blitt endret.

Også arbeidsmarkedet knyttet til IKT er endret. Det er ikke lenger i like stor grad lokalt eller nasjonalt, men er blitt europeisk og globalt. Globaliseringen betyr at leveransen av tjenester skjer på tvers av ulike nasjonale jurisdiksjoner. Det gjør det vanskelig å regulere og kontrollere tjenestene. Både når det gjelder skattlegging, kontroll av personvern og i spørsmål om selskapers og nasjoners sikkerhet, står vi overfor betydelige utfordringer.

I Norge tilpasser vi vår lovgivning til EUs reguleringer når det gjelder salg av tjenester og regulering av personvern. For de fleste formål er EU-landene ett marked og ett felles reguleringsområde for IKT og personvernspørsmål. Men i et globalt marked handler vi ofte utenfor EUs grenser.

Et eksempel på hvilke utfordringer man kan stå overfor, finner vi i saken fra høsten 2019 da Skatteetatens opplysninger om 9000 personer ble eksponert. *Dagens Næringsliv* meldte at dataselskapet Evry, som har ansvaret for å drifte og støtte Skatteetatens pc-bruk, oppdaget at 14 ansatte i Ukraina hadde hatt tilgang til norske personopplysninger (*Dagens Næringsliv* 19.12.19). Dette var et brudd på avtalen Evry hadde med Skatteetaten. I Ukraina er dyktig og billig datakompetanse lett tilgjengelig, og disse miljøene brukes derfor ofte av selskaper i andre land. Men Ukraina ligger utenfor EU, og Skatteetaten hadde satt en begrensning på hvor data skulle flyttes. Evry valgte å bringe noen av de ukrainske dataekspertene til Norge slik at de isteden kunne jobbe

med Skatteetatens data fra Fornebu utenfor Oslo. De samme menneskene, men under en annen jurisdiksjon. Eksempelet viser at i en globalisert verden kan både data og mennesker flyttes for å sikre billige tjenester og effektiv ressursbruk.

Eksempelet viser imidlertid at det ikke er likegyldig om man flytter mennesker eller data. Men det er heller ikke slik at det ene er sikkert mens det andre er usikkert. Det er knyttet ulike sikkerhetsproblemer til ulike løsninger. Det å bringe ansatte fra land utenfor EU inn i norske bedrifter kan i noen tilfeller oppfattes som en sikkerhetsrisiko. Etter presidentskiftet i USA i 2017 har både handelskrigen og sikkerhetspolitiske avveininger ført til at også installeringen av datautstyr kan anses som en sikkerhetsrisiko hvis det er produsert i land som ikke er med i vårt sikkerhetspolitiske samarbeid eller godkjent av USA. Europeiske lands beslutning om ikke å kjøpe 5G-teknologi fra kinesiske Huawei, tatt etter at USA i 2018 forbød føderale myndigheter og deretter private selskaper å handle med Huawei, er et eksempel (Ball, 2019). Levering av digitale tjenester gir oss dermed utfordringer både i måten vi arbeider og organiserer vår virksomhet på, og i hvordan vi sikrer persondata og andre data av verdi for virksomheter eller Norge som nasjon.

4 Sourcing og sikkerhet

Jo mer integrert IKT-tjenestene blir, og jo mer kompleks og globalisert teknologien blir, jo større blir sikkerhetsutfordringene. Jevnlig kommer det meldinger om sikkerhetshull i dataprogrammer og IKT-tjenester. I mai 2019 sendte Cybersecurity and Infrastructure Security Agency (CISA), som hører inn under innenriksdepartementet i USA, ut et sikkerhetsvarsel om et sikkerhetshull i eldre versjoner av Windows (CICA, 2019). I januar 2020 var Nasjonal sikkerhetsmyndighet i Norge (NSM) ute med en oppfordring om å oppdatere Microsoft Windows på grunn av en sårbarhet ved kryptering og sertifikater ved bruk av fjernstyring av pc-er (Remote Desktop Client) (Nasjonal sikkerhetsmyndighet, 2020).

Nasjonal sikkerhetsmyndighet beskriver kompleksiteten ved økende bruk av digitale tjenester og skytjenester slik i sine grunnprinsipper for IKT-sikkerhet (Nasjonal sikkerhetsmyndighet, 2018, s. 4):

> «Den stadig økende bruken av digitale tjenester innebærer blant annet at brukere blir mer mobile og at bruken av skybaserte tjenester øker. Denne situasjonen gir fordeler, men kompleksiteten vokser når data og applikasjoner blir distribuert til flere enheter og lokasjoner. Konsekvenser av dette er større avhengighet til tredjeparter slik at sikringsbehovet for virksomheter og deres informasjonsverdier strekker seg ut over egen virksomhet. Med dette følger også nye typer trusler som må adresseres.»

Rådene fra Nasjonal sikkerhetsmyndighet gjelder både privat og offentlig virksomhet og er i hovedsak prosedyrer for sikkerhetsvurdering som bygger på internasjonale standarder fra Den internasjonale standardiseringsorganisasjonen (ISO) og det amerikanske National Institute of Standards and Technology (NIST).

Digital sikkerhet dreier seg blant annet om personvern. Det er brukere av tjenestene som etter lovgivningen er behandlingsansvarlige, og som har et overordnet ansvar for at personvernprinsippene og regelverket overholdes. Leverandøren av IKT-tjenesten er databehandler og håndterer personopplysningene på vegne av en behandlingsansvarlig. Både private og offentlige

virksomheter som skal håndtere persondata, er behandlingsansvarlige og må sikre at vilkårene etterleves av tjenesteleverandører gjennom å inngå en avtale med databehandler om hvordan dette skal skje. Datatilsynet, som er tilsynsmyndighet etter personvernlovgivningen, peker på at bruk av skytjenester gir utfordringer for personvernet, men viser for øvrig til Nasjonal sikkerhetsmyndighet og Difi for ytterligere informasjon (Datatilsynet, 2018).

Selv om bruk av skytjenester og av underleverandører kan skape utfordringer knyttet til sikkerhet og personvern, er det viktig å være oppmerksom på at håndteringen av personopplysninger før de sendes ut på nettet, også innebærer risiko for at personopplysninger skal bli kompromittert. Gode prosedyrer som sikrer at personopplysninger håndteres korrekt internt i virksomheten, og at bare autorisert personell har tilgang til opplysningene, reduserer risiko. Digitaliseringsdirektoratet har laget en veileder om opplæring og kulturutvikling innen informasjonssikkerhet for offentlige virksomheter og understreker at det er et lederansvar å sørge for at medarbeiderne har tilstrekkelig kunnskap om informasjonssikkerhet for å kunne utføre sine oppgaver (Digitaliserngsdirektoratet, 2015).

4.1 Nasjonal sikkerhet

Høsten 2018 publiserte *New York Times* en artikkel om president Trumps bruk av en usikret mobiltelefon. «When Trump Phones Friends, the Chinese and the Russians Listen and Learn», lød overskriften (New York Times, 24.10.2018). Avisen viste også til lekkasjen som avslørte at amerikanske myndigheter hadde avlyttet den tyske kansleren Angela Merkels mobiltelefon. Omtrent samtidig begynte en amerikansk kampanje for å hindre at den kinesiske teknologigiganten Huawei skulle få bygge ut siste generasjons mobilnett i land amerikanerne anså som allierte. To amerikanske senatorer henvendte seg til Canadas statsminister Truedeau og ba Canada gjøre som amerikanerne og australierne og hindre Huawei i å levere utstyr til mobilnettet (The Globe and Mail, 11.10.2018). Disse hendelsene ga høsten 2018 allmennheten et innblikk i mulighetene for spionasje som ligger i bruken av moderne teknologi. Diskusjonen om IKT-sikkerhet kom imidlertid blandet inn i en handelskrig og en sikkerhetspolitisk innstramning med skarpere tegning av fiendebilder, som ikke gjør det lettere å skille teknologi fra politikk.

For spesialister var sårbarheten som ligger i teknologisk utstyr, ikke noen nytt. Den 11. februar 2020 kunne *Washington Post* sammen med tyske og sveitsiske medier avsløre at tysk og amerikansk etterretning siden 1970-tallet har solgt kryptoutstyr som de to landenes etterretningstjeneste har kunnet benytte til avlytting i mer enn 120 land. Kryptoutstyr fra det sveitsiske

selskapet Crypto AG, hemmelig eiet av CIA og vesttysk etterretning, ble brukt til også å avlytte andre Nato-land (Washington Post, 11.2.2020), men ikke Norge. Oberst og avdelingsdirektør i Nasjonal sikkerhetsmyndighet Hans Robert Bjørnaas kunne fortelle *Dagens Næringsliv* at myndighetene i Norge ikke har villet gå utenlands for å kjøpe kryptoutstyr. «Vi har hatt fokus på nasjonal kontroll av krypto helt siden vi fikk denne industrien oppe og gå i Norge på 1950-tallet» (Dagens Næringsliv, 15.2.2020). Behovet for nasjonal kontroll over et så viktig utstyr har gjort at kryptoutstyret har blitt produsert i Norge. Det har ikke blitt sendt over til andre parter eller solgt til andre land. Bjørnaas viser til avsløringene rundt Crypto AG og sier at denne historien «er blant argumentene NSM har brukt for å vise behovet for å ha kunnskap om produksjon av krypto på nasjonale hender» (Dagens Næringsliv, 15.2.2020).

Har denne kunnskapen også betydning for offentlige virksomheter som skal håndtere og lagre data i skytjenester? Informasjonssikkerhet kan kompromitteres, og offentlige eller private interesser kan krenkes på to ulike måter ved outsourcing av IKT-tjenester: Data kan bli kompromittert gjennom rettslige prosesser under et annet lands jurisdiksjon, og det kan skje ved ulovlig inntrenging eller tilegnelse av informasjon.

4.2 Motstridende eller usikker jurisdiksjon

Bevegelse av tjenester over landegrensene kan skape usikkerhet om hvilket lands jurisdiksjon som skal gjelde. Dette gjelder også i strafferetten, der et lands myndigheter ønsker å forfølge kriminelle over landegrenser. Spørsmålet om jurisdiksjon kan reguleres i konvensjoner, og mange land har et utstrakt samarbeid. Av og til ender likevel spørsmålet om jurisdiksjon opp som uavklart.

Dersom data lagres steder der det vil kunne komme inn under et annet lands jurisdiksjon, vil norske myndigheter eller norske virksomheter kunne miste kontrollen over egne data. Det er dette hensynet som ligger bak reguleringen som finnes i visse norske lover om hvor ulike typer data skal lagres, og i norsk og europeisk regulering av hvor persondata kan lagres. Reguleringen av personopplysninger skjer gjennom EUs personvernforordning GDPR og personopplysningsloven. Arkivloven og bokføringsloven er eksempel på andre lover som regulerer hvor og hvordan det offentlige kan lagre data i utlandet. I 2018 skapte det betydelig diskusjon da USA vedtok den såkalte Cloud Act. Loven sier at amerikanske myndigheter kan, etter en rettslig avgjørelse, kreve at data- og kommunikasjonsselskaper må levere ut data de har lagret for en kunde eller en abonnent på enhver server de eier og opererer, også i utlandet. Dette gjelder ikke bare amerikanske selskaper, men alle

som opererer på amerikansk jord og faller inn under amerikansk jurisdiksjon (Punke, 29.5.2019).

I Sverige gikk en ekspertgruppe i eSam, et samarbeidsorgan mellom statlige myndigheter og Sveriges Kommuner och Regioner, ut og varslet at det å overlate hemmeligstemplede eller taushetsbelagte data til en utenlandsk tjenesteleverandør måtte likestilles med å anse data for kompromitterte (eSam, 23.10. 2018):

> «Om sekretessreglerade uppgifter görs tekniskt tillgängliga för en tjänsteleverantör som till följd av ägarförhållanden eller annars är bunden av regler i ett annat land, enligt vilka tjänsteleverantören kan bli skyldig att överlämna information utan att internationell rättshjälp anlitats eller annan laglig grund föreligger enligt svensk rätt, får uppgifterna anses vara röjda.»

Uttalelsen skapte diskusjon, og ekspertgruppen måtte gi utfyllende kommentarer til denne uttalelsen året etter. Der er ekspertgruppen langt mer positiv til skytjenester, men understreker at hemmelige eller taushetsbelagte data («sekretessreglerade uppgifter») må sikres gjennom juridisk bindende avtaler, og at utlevering til en fremmed makt ikke må skje uten at det er godkjent av svenske myndigheter (eSam, 20.9.2019).

Spørsmålet om kryssende eller motstridene jurisdiksjoner er ikke noe som bare gjelder skytjenester. Cloud Act gir heller ikke amerikanske myndigheter full tilgang til data. En av direktørene i Amazon Web Service viser til at selskaper og domstoler kan forsøke å avvise eller bestride et slikt krav om utlevering dersom de mener forespørselen krenker personvernets rettigheter i det fremmede landet dataene er lagret i, for eksempel GDPR i Europa (Punke, 29.5.2019). Det amerikanske justisdepartementet ga i april 2019 ut et White Paper om Cloud Act hvor departementet understreker at Cloud Act bare viderefører eksisterende lovgivning i USA, og at loven bidrar til å styrke det mellomstatlige arbeidet for å bekjempe cyberkriminalitet (U.S. Department of Justice, 2019):

> «The CLOUD Act is designed to permit our foreign partners that have robust protections for privacy and civil liberties to enter into executive agreements with the United States to obtain access to this electronic evidence, wherever it happens to be located, in order to fight serious crime and terrorism.»

Også norske og europeiske myndigheter forbeholder seg retten til å hente data i andre land hvis det er del av en strafferettsprosess. I 2019 avsa Høyesterett i Norge en kjennelse som ga norske myndigheter rett til å hente ut data som var lagret i USA av et norsk, men amerikansk eid, selskap (Høyesterett, 2019).

Dersom data føres ut av ett land og over i et annet, kan det oppstå usikkerhet om hvilken jurisdiksjon som beskytter data og dataeier, eller det kan oppstå uenighet om hvilken av flere motstridende reguleringer som skal gjelde. Det har for eksempel vært usikkerhet om hvorvidt amerikansk lovgivning og avtaler med EU er i pakt med EUs personvernregulering.[2] Uklarhet knyttet til jurisdiksjon kan utgjøre et sikkerhetsproblem. Dette har ført til at EU har relativt strenge regler for overføring av persondata ut av EU/EØS-området. Når det gjelder andre typer data, må den enkelte dataeier og det enkelte land sikre sine data juridisk. Det kan være krevende dersom data lagres i andre land.

4.3 Hacking og spionasje

Ulovlig inntrenging i dataanlegg, såkalt hacking, er et betydelig problem som berører all IKT. Mens beskyttelse og sikkerhet tidligere var noe som dedikerte sikkerhetsselskaper holdt på med, er dette nå blitt en integrert del av skyleverandørens tjenester. I økende grad benytter de store selskapene maskinlæring for å overvåke nettrafikk og kundenes handlingsmønster og kan på den måten levere stor grad av sikkerhet. Microsoft rapporterte i 2017 at de hadde 3500 ansatte som jobbet med sikkerhet, og at selskapet investerte mer enn en milliard dollar i året på sikkerhet (Microsoft, 2017). Likevel har flere av de store selskapene, som vi har sett, vært utsatt for sikkerhetsbrudd og skandaler forbundet med utnytting av personopplysninger. Facebooks rolle i Cambridge Analytica-saken, der analyseselskapet Cambridge Analytica fikk tilgang til flere millioner Facebook-kontoer uten samtykke, informasjon som skal ha blitt brukt til å påvirke presidentvalget i USA, er et eksempel på det siste (The Guardian, u.d.).

En viktig grunn til at hacking og spionasje rettet mot IKT-tjenester foregår, er at data kan ha stor verdi. Virksomheter, både i det offentlige og i det private, må verne om sine data for å unngå at industrielle hemmeligheter,

[2] I juli 2020 fant EU-domstolen at Privacy Shield, en rammeavtale om overføring av data mellom Europa og USA, var ugyldig på grunn av at amerikansk lov ikke gir tilstrekkelig personvern og sikrer databeskyttelsesrettighetene til personer når personlige opplysninger blir overført til USA fra Europa (Room, 2020).

forskningsmateriale eller samfunnskritisk informasjon kommer på avveie. For nasjonalstaten er den nasjonale sikkerheten viktig. Historien om hvordan Crypto AG ble brukt til å spionere på fremmede makter, viser at det ikke er enkelt å ivareta nasjonal sikkerhet. Langt på vei er det et spørsmål om kompetanse og kontroll over egne data. Et av de landene som har tatt konsekvensen av dette, er Tyskland.

4.4 Datasuverenitet og digital autonomi – Die Bundescloud

I juni 2013 vedtok budsjettkomiteen i den tyske Bundestag å be regjeringen utvikle et sentralt innkjøpssystem for den føderale administrasjonen. Sommeren 2017 var Die Bondescloud etablert som en plattform. Den hadde da flere mål enn bare å være en sentral innkjøpsportal (Stach, Heike, 2020):

- databeskyttelse og IT-sikkerhet
- suverenitet og kontroll
- rask tilpasning til teknologiutviklingen
- produktiv, effektiv, stabil og bærekraftig drift
- være en attraktiv arbeidsgiver for IT-eksperter
- kostnadseffektive og bærekraftige tjenester

Planen er at Bundescloud over tid skal samle alle sider av IT-drift for Tysklands sentraladministrasjon: innkjøpstjenester, drift og IT-konsulenttjenester.

En av grunnene til at den tyske staten valgte å etablere sin egen «private» sky, var at skylagring og programvare fra private leverandører gikk over til å bli basert på leie eller abonnement av tjenester. «Vi ville ikke være avhengige av eksterne leverandører. Vi ville ha suverenitet og være autonome, og styre vår egen IT også om ti år», uttalte Heike Stach som er med i ledelsen av utviklingsprosjektet (Fri Fagbevegelse, 11.2.2020). I et foredrag holdt i Oslo understreket hun at digital autonomi var et viktig mål for Tyskland.

Etter hvert som IKT får en kritisk rolle i samfunnet, er det viktig for et samfunn å sikre at digitale funksjoner ikke er avhengige av enkeltfaktorer og enkeltselskaper. Når data lagres av andre enn statlige etater, og statlige virksomheter blir nødt til å akseptere standardiserte skytjenester framfor tilpassede tjenester, øker avhengigheten av andre aktører. Å bli knyttet for sterkt til enkeltleverandører kan øke risikoen for kostnadsøkninger og å bli låst til én operatør («lock-in»). En stat må også vurdere datatilgjengeligheten. Det dreier seg ikke bare om oppetid under normale forhold, men data må være

tilgjengelige også i tilfelle krig eller cyberangrep. Digital autonomi skal sikre at føderale myndigheter skal kunne være operative i konfliktsituasjoner (Stach, Heike, 2020).

Tyskland legger stor vekt på digital autonomi, og dette har blitt et sentralt mål i digitaliseringspolitikken. Det er lansert en overordnet strategi for digital autonomi som også omfatter forbundsstatene og det lokaladministrative nivået. Målet er å kartlegge hvor det kan oppstå en kritisk avhengighet av IKT-teknologi, søke alternative løsninger og koordinere tiltak for sikre tilgang til alternative IT-løsninger.

Mens retningslinjene i den norsk statlige IKT-strategien sier at private skytjenester skal brukes framfor offentlige løsninger, der dette er kostnadseffektivt, er den tyske anbefalingen stikk motsatt: Private skytjenester skal bare benyttes hvis staten ikke selv kan tilby en tilstrekkelig tjeneste. Da planleggingen av Bundescloud var i en tidlig fase, ble det utformet noen minimumskrav til statlige virksomheter som ønsket å benytte allmenne skytjenester (Stach, Heike, 2020):

- Ekstern skytjeneste skal bare brukes hvis den føderale administrasjonen ikke selv kan levere den tjenesten som er nødvendig. Behandling av sensitive data er bare tillatt i Tyskland. Sensitive data må ikke gjøres kjent for uautoriserte tredjeparter.
- Kontrakter som gjelder skytjenester, må være underlagt tysk lov og må oppgi domstoler i Tyskland som verneting.
- Å oppnå permanent bruksrett (kjøp) er å foretrekke framfor en midlertidig bruksrett (leieavtale).
- Leverandøren av skytjenester må dokumentere at det foreligger tilstrekkelig informasjonssikkerhet etter internasjonal standard (ISO27001) eller den tyske Cloud Computing Compliance Controls Catalogue (C5).

Eksempelet fra Tyskland viser at det er ulike måter å tenke rundt sourcingstrategier for IKT i offentlig sektor. Tyskland har i stor grad valgt å organisere og drifte IKT-tjenestene sine selv og ønsker å være uavhengig av internasjonale selskaper som leverer skytjenester. Her har Norge valt en helt annen strategi. Norske myndigheter oppfordrer statlige virksomheter og kommuner til å kjøpe skytjenester av kommersielle aktører.

5 En nasjonal strategi for skytjenester

I Norge har regjeringen lagt en strategi for å øke digitaliseringstakten og ta i bruk skytjenester. Regjeringen Solberg har gjennom en rekke publikasjoner og tiltak lagt et betydelig press på hele offentlig sektor for å øke digitaliseringen og få virksomhetene til å ta i bruk ny teknologi. I stortingsmelding nr. 27 (2015–2016) presenterer regjeringen en overordnet politikk for hvordan Norge kan ta i bruk IKT til samfunnets beste. Målet er en «brukerrettet og effektiv» offentlig forvaltning som legger grunn for verdiskapning og deltakelse. Helt fra første stund har skytjenester satt en gyllen standard for hvilken vei regjeringen mente det var riktig å gå:

> «Skytjenester begynner å bli den dominerende måten å levere IKT-tjenester på, særlig til forbrukere og til næringslivet. Offentlig sektor følger etter. Skytjenestenes skalerbarhet og 'betal for det du bruker-prinsippet' kan være gode løsninger for kjøpere av IKT som ser etter kostnadseffektive løsninger» (Meld. St. 27, 2015–2016, s. 13).

Dette ble fulgt opp samme år da regjeringen la fram en egen nasjonal strategi for å ta i bruk skytjenester (Kommunal- og moderniseringsdepartementet, 2016). I dette dokumentet anbefaler regjeringen offentlige virksomheter å bruke skytjenester:

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

Regjeringen trekker fram flere fordeler med skytjenester. Den viser til den amerikanske standardiseringsorganisasjonen NIST (National Institute of Standards and Technology) og hvilke kjennetegn denne organisasjonen mener skytjenester har (Kommunal- og moderniseringsdepartementet, 2016, s. 7):

«*Behovsbaserte*. Skytenester blir levert etter kvart som ein har bruk for dei. Dei kan skaffast raskt, og kunden betener seg sjølv på nett når han har bruk for auka kapasitet (for eksempel servertid eller lagring), utan at han treng å involvere leverandøren.

Leverte over nett. Tenestene er tilgjengelege over nettet, og kunden får tilgang gjennom standard-mekanismar som kan nyttast gjennom ulike typar klientar – frå mobiltelefonar og nettbrett til PC-ar.

Delte ressursar. Leverandøren kan fordele dataressursane sine dynamisk etter dei ulike kundane sine behov.

Umiddelbar fleksibilitet. Dei tenestene kunden treng kan skalerast opp eller ned etter kva kunden har bruk for, slik at ressursane i praksis blir opplevde som uendelege.

Betaling etter bruk. Ressursbruken blir målt, kontrollert og rapportert, og er gjennomsiktig for både kunden og leverandøren av tenesta.»

Den nasjonale strategien presenterer få motforestillinger mot bruk av skytjenester. Regjeringen legger stor vekt på at bruk av skytjenester kan gi økonomiske innsparinger. Prising av skytjenester med betaling for bruk gjør at kostnadene blir «transparente», og man slipper å betale for mer datakraft, lagring og programvarelisenser «enn ein treng til kvar tid», heter det i strategien (Kommunal- og moderniseringsdepartementet, 2016, s. 9). Det legges også vekt på at skytjenester gir økt sikkerhet. Dette gjelder særlig leveringssikkerhet og datasikkerhet knyttet til selve driften av datasentre. Store leverandører har ofte bedre kompetanse, omfattende sikringstiltak og ressurser til å skifte ut maskinvare og oppgradere programvare regelmessig (Kommunal- og moderniseringsdepartementet, 2016, ss. 10, 11).

Den nasjonale strategien for bruk av skytjenester legger opp til at offentlig sektor i økende grad skal bruke skytjenester. Regjeringen peker på at offentlig sektor har «eit spesielt behov for kontroll over kven som forvaltar informasjon, og kor dette blir gjort (Kommunal- og moderniseringsdepartementet, 2016, s. 26). Strategien peker på to veier å gå for å ivareta offentlig kontroll. Den ene er gjennom å etablere egne datasentre for statlig eller offentlig sektor. Dette vil kunne tilfredsstille de strengeste kravene til sikkerhet. Regjeringen viser til en utredning fra 2015 (Nexia International, 2015) og slår fast at det ikke er «avdekka behov for at sentrale styresmakter forhandlar fram felles avtalar om datasenterdrift, eller etablerer eit felles datasenter for statleg- eller offentleg sektor» (Kommunal- og moderniseringsdepartementet, 2016, s. 26).

Den andre veien regjeringen foreslår å gå, er gjennom å sikre offentlig kontroll gjennom kontrakter som blir inngått med leverandører. Her ligger det en utfordring i å få på plass avtaler som flere parter kan bruke (standardavtaler), og som samtidig ivaretar det offentliges behov. Det vil også være behov for «mekanismer for å følge opp kontrakten», for eksempel gjennom bruk av en uavhengig tredjepart som kan foreta revisjon (Kommunal- og moderniseringsdepartementet, 2016, s. 27).

Regjeringens nasjonale strategi for bruk av skytjenester i offentlig sektor har blitt fulgt opp i digitaliseringsrundskrivet som oppdateres jevnlig. Der stiller regjeringen 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. Dersom det ikke foreligger spesielle hindringer, «og skytjenesten gir den mest hensiktsmessige og kostnadseffektive løsningen, bør en velge slike [sky]tjenester» (Kommunal- og moderniseringsdepartementet, 2019). Regjeringen peker på at særlige krav til sikkerhet kan være til hinder for bruk av skytjenester. Målsettingen som ligger bak kravet om å ta skytjenester i bruk, er dels et ønske om å øke effektiviteten, men også et politisk ønske om at det offentlige skal begrense sin virksomhet på områder der private kan levere bedre tjenester: «Det offentlige skal i utgangspunktet ikke gjøre selv det som markedet kan gjøre bedre og mer effektivt», heter det i digitaliseringsrundskrivet (Kommunal- og moderniseringsdepartementet, 2019, s. pkt 1.10). Disse retningslinjene følger opp politikken som ble slått fast i stortingsmeldingen fra 2016 om en digital agenda for Norge. Her uttrykker regjeringen at selv nasjonale fellesskapsløsninger, som skal gi helhetlige og tverrsektorielle tjenester (som for eksempel Altinn), bør bygges på markedsløsninger: «Det bør ikke etableres nasjonale felleskomponenter som er i konkurranse med et velfungerende marked» (Meld. St. 27, 2015–2016, s. 74).

Den positive framstillingen av skytjenester i regjeringens strategidokumenter og anbefalinger samsvarer godt med slik tjenestene framstilles av selskapene som leverer slike tjenester. Et eksempel er Evry som understreker at skytjenester kan være fleksible og skalerbare, og lokker med lyse framtidsutsikter: Skytjenestene er «designet for å muliggjøre digital transformasjon» (Evry, u.d.). Noe forenklet beskriver regjeringens nasjonale strategi for skytjenester fordelene ved skytjenester slik (Kommunal- og moderniseringsdepartementet, 2016, s. 7):

- Skytjenester gir tilgang til avanserte programmer.
- Man betaler etter bruk.

- Man får lett tilgang fra nettleser hvor som helst.
- De kan skaleres opp og ned etter behov.
- De har kontinuerlig oppdatering og utvikling.

Skytjenester har åpenbart en rekke fordeler. Det kan likevel være grunn til å spørre om en slik utelukkende positiv beskrivelse er dekkende. Det er heller ikke gitt at markedet alene kan sikre levering av tjenester som dekker det offentliges behov eller den ønskede sikkerheten. Vi har sett at tyske myndigheter har valgt en annen strategi og bygger opp egne systemer for å skaffe statlige virksomheter tilgang til skytjenester. På noen områder arbeider også norske myndigheter for å samordne offentlig virksomhet og etablere egne offentlige IKT-systemer.

5.1 Marked eller statlig samordning?

Parallelt med overgang til markedsbaserte skytjenester og etablering av en offentlig markedsplass for slike tjenester foregår det et betydelig arbeid med å samordne offentlige digitale tjenester. I digitaliseringsrundskrivet pålegger regjeringen statlige virksomheter å bruke det som kalles nasjonale felleskomponenter og fellesløsninger. Dette er blant annet ID-porten, digital postkasse og Altinn, og det omfatter folkeregisteret, enhetsregisteret og matrikkelen. På ulike felt har myndighetene sett behov for nasjonale fellesløsninger og iverksatt tiltak. Fra 2020 er for eksempel Norsk helsenett skilt ut fra Direktoratet for e-helse for å bli en nasjonal leverandør av e-helsetjenester. Dette omfatter blant annet e-resept, kjernejournal og grunndata over helseressurser. Dette får blant annet betydning for kommunene som må knytte seg til Helsenettet, som skal være en lukket og sikker digital samhandlingsarena. I tillegg leder Direktoratet for e-helse prosjektet Akson, et prosjekt for å opprette en felles digital journalløsning for kommunene og for å sikre en felles samhandling på tvers av helsetjenestene i Norge (Direktoratet for e-helse, 2020).

Innenfor universitets- og høyskolesektoren driver Unit samordningsprosjekter (Unit, 2019). Digitaliseringsstyret har vedtatt en portefølje av prosjekter som blant annet omfatter HR, saksbehandling og arkiv, samordnet studentopptak og sikkerhetssatsing. Innen økonomi- og lønnstjenester er Direktoratet for økonomistyring valgt som tjenesteleverandør, og i perioden 2018–2022 skal det utvikles standardiserte arbeidsprosesser og nye digitale økonomisystemer skreddersydd for UH-sektoren (BOTT Universitetssamarbeidet, u.d.).

Eksemplene viser at statlige myndigheter ser behov for å samordne IKT i offentlig sektor og har satt i gang større offentlige prosjekter for å realisere dette. Det ser dermed ut til at regjeringen både anbefaler offentlige virksomheter å satse på marked der private tilbyr skytjenester på kommersiell basis, og på offentlig samordning av IKT-tjenester og infrastruktur med drift av offentlige eller private virksomheter. Samlet sett kan vi se de offentlige tiltakene som en blandingspolitikk. Regjeringen sier imidlertid lite i de offentlige dokumentene om hvilke generelle prinsipper som skal ligge bak valg av strategi. I det følgende skal vi se hvordan IKT er organisert i fire statlige virksomheter og fire kommuner. Hvilke sourcingstrategier har virksomhetene, og hvordan forholder de seg til myndighetenes styringssignaler?

6 Organiseringen av IKT i fire statlige virksomheter

Hvordan organiserer statlige virksomheter og kommuner sin IKT-drift, og hvilke sourcingstrategier har de? De fire statlige virksomhetene som gjennomgås, er valgt fordi de representerer ulike sektorer i staten, har ulik størrelse og ulike driftsoppgaver. På hvert sitt felt har de omfattende oppgaver som skal løses med hjelp av IKT.

Beskrivelsen av de enkelte virksomhetene bygger på intervjuer og tilgjengelig informasjon fra dokumenter og nettsider. Teksten er ment å presentere virksomhetens erfaringer og er ikke en analyse eller fullstendig beskrivelse av virksomhetens IKT-drift.

6.1 Forsvaret

Forsvaret ledes av forsvarssjefen med støtte fra forsvarsstaben. Organisasjon består av 14 driftsenheter, blant annet Hæren, Sjøforsvaret, Luftforsvaret og Heimevernet. Cyberforsvaret er en driftsenhet som drifter, sikrer og forsvarer Forsvarets datasystemer (Forsvaret, u.å.). I 2016 ble Forsvarsmateriell opprettet som en egen etat direkte underlagt Forsvarsdepartementet. Forsvarsmateriell har som hovedoppgave å planlegge, anskaffe og forvalte materiell til Forsvaret og andre etater under Forsvarsdepartementet (Forsvaret, 2017). Forsvaret har rundt 16 000 militært og sivilt ansatte.

Organisering av IKT-tjenestene

IKT-funksjonen i Forsvaret har over 1500 ansatte fordelt på Forsvarsdepartementet og de ulike etatene. Cyberforsvaret og Forsvarsmateriell har en sentral funksjon, men også Forsvarsdepartementet, Forsvarets forskningsinstitutt og Forsvarsbygg drifter egen IKT.

I forsvarssektoren er det Forsvarsmateriell som står for de store anskaffelsene til Forsvaret. Forsvarsgrenene er brukere av IKT, og Cyberforsvaret drifter og leverer IKT-tjenester. Investeringene i IKT er betydelige, og Forsvaret

forventer at IKT-investeringene øker til over 2 milliarder per år i 2022. Hovedutfordringen for forsvarssektoren ligger i å sikre evne og kapasitet til å styre, forvalte og utvikle IKT i de kommende årene.

En arbeidsgruppe i Forsvaret har utformet en IKT-strategi som ble godkjent av forsvarsministeren i 2019 (Forsvarsdepartementet, 2019). I rapporten fra arbeidsgruppen presenteres det en beskrivelse av nåsituasjonen i sektoren og hvilke utfordringer organisasjonen har.

En hovedutfordring for forsvarssektoren er at det tar svært lang tid fra et behov oppstår, til det er gjennomført anskaffelser og IKT kan tas i bruk. Prosessen oppfattes som lite fleksibel, og kompetansen på IKT og risikofaktorer er ikke god nok. Det påvirker evnen til å vurdere alternativ teknologi ved nyanskaffelser (Forsvarsdepartementet, 2019, s. 16). Deler av sektoren oppfatter IKT som infrastruktur og ser ikke betydningen av teknologien og muligheten den gir for å øke den operative evnen. Forsvaret har også en rekke systemer som ofte blir videreutviklet heller enn erstattet av nye mer moderne systemer. Årsaken er at det kan være vanskelig å erstatte de eksisterende systemene og samtidig ta vare på de dataene som finnes, men også uklar organisering og uklarhet knyttet til hvem som har beslutningsmyndighet ved oppgraderinger og videreutvikling av systemene, bidrar til at beslutninger utsettes eller uteblir (Forsvarsdepartementet, 2019, s. 17).

Gjennomgangen av nåsituasjonen i forsvarssektoren peker på at det er behov for kompetanse i hele organisasjonen på IKTs betydning, og at nye driftsmodeller og muligheter må tas i bruk.

Sourcingstrategi

Forsvarets IKT-strategi, som også handler om sourcing, er bygget opp rundt de internasjonale trendene innen IKT-utvikling: en mer strategisk bruk av IKT, ikke bare som støttefunksjon; integrasjon og kommunikasjon mellom systemer, ikke adskilte plattformer; jevnlig oppgradering og modulbygging, ikke store monolittiske systemer. Valg langs disse linjene skal gi en smidig organisasjon med plass for innovasjon. Strategien krever økt grad av partnerskap, og spesialrådgiveren i Forsvarsdepartementet sier at det er viktig at Forsvaret får levert IKT-tjenester i både fred, krise og væpnet konflikt, samtidig som distinksjonsprinsippet (skille mellom sivile og militære) ivaretas i henhold til krigens folkerett (intervju 7.1.2020).

I IKT-strategien identifiserer Forsvaret tre «målområder». Innenfor målområdet *fremtidsrettet og nytenkende* ligger blant annet tiltak for å øke den digitale kompetansen innenfor IKT. Dette kan gjøres ved «å samarbeide med leverandører for å hente inn relevant kompetanse i utvikling og drift av IKT»

(Forsvarsdepartementet, 2019, s. 41). Et annet tiltak er å styrke kulturen for innovasjon. En viktig avveining er å balansere risiko og innovative løsninger. Forsvarets IKT-løsninger må være sikre nok, men samtidig ikke legge unødige begrensninger på bruk av ny teknologi (Forsvarsdepartementet, 2019, s. 46).

Innenfor målområdet *koordinert og delegert* er målet å gi de ulike etatene i forsvarssektoren større grad av frihet til å velge hvordan de vil jobbe. Forsvarsdepartementets oppgave skal være «å definere mål og overordnede spilleregler for samhandling mellom underliggende etater», mens etatene selv skal stå friere i sine valg innenfor de opptrukne spillereglene (Forsvarsdepartementet, 2019, s. 42). Styringen av sektoren skal i større grad foregå gjennom å definere en IKT-arkitektur som setter strengere krav til hvilke IKT-løsninger som kan etableres. Tanken er at dette vil skape et helhetlig system og mulighet for digitalt samarbeid på tvers av administrative og operative systemer (Forsvarsdepartementet, 2019, s. 51).

Det tredje målområdet er *evne til å unytte nye plattformer*. Strategien legger opp til en kontinuerlig utvikling og tilpasning av eksisterende og ny teknologi. Dette krever langsiktige relasjoner til leverandører. Personell hos leverandører må kunne sikkerhetsklareres, og distinksjonsprinsippet i krigens folkerett medfører at det må gjøres spesifikke vurderinger knyttet til leveranser fra sivile leverandører i en krigssituasjon. Forsvaret vil måtte ha ulike tilnærminger til ulike deler av leveransene og viser til at samarbeid mellom Forsvaret og markedet ikke er noe nytt i forsvarsindustrien.

Ansvaret for den sentrale koordineringen og etableringen av styringsmekanismer innenfor IKT-området er lagt til Forsvarsdepartementet. På sikt vil de ulike etatene i forsvarssektoren anskaffe og ta i bruk forsvarssystemer og applikasjoner for drift innenfor den nye arkitekturen. Forsvarssektoren tar sikte på å øke bruken av skytjenester. I IKT-strategien heter det: «Sektoren kan i økende grad vurdere å anskaffe IKT som en tjeneste (SaaS) i stedet for on premise der hvor det er mulig og hensiktsmessig. Løsninger bør være fleksible og skalerbare med et tilstrekkelig nivå av sikkerhet» (Forsvarsdepartementet, 2019, s. 57).

6.2 Meteorologisk institutt

Meteorologisk institutt (MET) overvåker og varsler været for myndighetene, næringslivet og allmennheten. Værvarsling av høy kvalitet er viktig for en rekke brukere, blant annet innen luftfart, sjøfart og veivedlikehold. Tjenesten som leveres av Meteorologisk institutt, bidrar til å sikre liv og verdier og gi

kunnskap som gjør samfunnet i stand til å planlegge for framtidige klimaendringer. Instituttet driver forsking og utvikling på sine fagområder. Meteorologisk institutt beskriver sine verdikjeder gjennom flere ledd fra innhenting av observasjoner via behandling og modellering av værdata til tolkning og formidling til ulike brukergrupper (Meteorologisk institutt, 2018). I dette inngår også forskning. Meteorologisk institutt har blitt flyttet fra forskningssektoren til miljøsektoren på grunn av den voksende betydningen instituttets arbeid har fått for miljø- og klimautviklingen.

Organiseringen av IKT-tjenestene

IKT er en del av hele verdikjeden til Meteorologisk institutt og omfatter blant annet IT-arkitektur, drift, utvikling og vedlikehold. IT-divisjonen ved Meteorologisk institutt har medarbeidere med høy kompetanse innenfor de fleste IT-disipliner og har inntil nå levert det meste av IT-tjenestene instituttet trenger. IT-ansatte har levert alt fra administrativ støtte til modellkjøring og utvikling som også krever geofaglig forståelse. IT-driften ved Meteorologisk institutt omfatter blant annet (Meteorologisk institutt, 2019)

- brukerstøtte
- klienthåndtering (pc og mobil)
- 24/7 on-site driftsovervåking
- applikasjonsdrift og meteorologisk produksjon
- infrastrukturdrift (server, lagring, nettverk, kommunikasjon, backup)
- applikasjonsutvikling
- støtte/bidrag til forskningsprosjekter nasjonalt og internasjonalt

De siste årene har Meteorologisk institutt valgt å anskaffe programvare gjennom skyløsninger (Software as a Service – SaaS) på det administrative området. Den gamle programvaren var utdatert og uten support, og nye skyløsninger ble valgt for en rekke tjenester. Dette gjaldt først og fremst ulike støttefunksjoner, blant annet

- e-post og samhandlingsløsninger
- økonomisystem
- lønn- og personalsystem
- reiseregningssystem
- anskaffelsesløsning
- rekrutteringsløsning
- sak- og arkivløsning
- intranett og met.no

- videokonferanseløsning
- krisehåndteringsverktøy

Strategien har vært å kutte ut å selv håndtere det som andre kan levere bedre og billigere. «Vi prøver å bruke kreftene der vi kan gjøre en forskjell», påpekte IT-direktøren (intervju 17.12.2019). Programvare ble innkjøpt som tjenester fra forskjellige leverandører, og Meteorologisk institutt valgte for flere av tjenestene å benytte rammeavtaler inngått gjennom Statens innkjøpsavtale og Uninett/Unit.[3] Som samhandlingsplattform har instituttet valgt å bruke Google G-suite fordi det er billig og fungerer godt når instituttet har brukere på ulike plattformer som Linux, Windows og Mac.

Meteorologisk institutt har og behandler en enorm mengde meteorologiske data gjennom kontinuerlig analyse. Instituttet lagrer data på egne servere (i egen sky) og vedlikeholder maskinpark og øvrig infrastruktur som er nødvendig. Kjøring av modeller for atmosfæren gjøres flere ganger om dagen på maskiner hos National Supercomputer Centre (NSC) i Sverige gjennom et samarbeid med Finlands og Sveriges meteorologiske institutter i det som er kalt MetCoOp (Meterological Cooperation on Operational Numeric Weather Prediction (NWP)). Modellering av vær krever enormt stor regnekapasitet, og datautstyret er svært kostbart. Det foreligger planer for utvidelse av dette samarbeidet til flere land (Meteorologisk institutt, 2020). Det er etablert et operasjonelt værvarslingssamarbeid på europeisk nivå, blant annet gjennom EUMETSAT og ECMWF (Meteorologisk institutt, 2019).[4]

Ved siden av det samarbeidet med andre meteorologiske institusjoner har Meteorologisk institutt IKT-samarbeid med universitet- og høyskolesektoren og med NRK om tjenesten yr.no.

Sourcingstrategi

Meteorologisk institutts sourcingstrategi for IKT har som mål at instituttet skal «opprettholde og videreutvikle sin kompetanse på utvikling av verktøy og leveransekjeder for innsamling, lagring, beregning og tilgjengeliggjøring

[3] Uninett er et statlig aksjeselskap som driver den digitale grunnmuren for forskning og utdanning i Norge. Unit er Direktoratet for IKT og fellestjenester i høyere utdanning og forskning.

[4] European Organisation for the Exploitation of Meteorological Satellites (EUMETSAT) ble etablert i 1986 og er en mellomstatlig organisasjon som i dag har 30 medlemsstater. The European Centre for Medium-Range Weather Forecasts (ECMWF) er også en mellomstatlig organisasjon for meteorologisk samarbeid som ble etablert i 1975, og som i dag har støtte fra 34 stater.

av data, høy-ytelsesinfrastruktur (PPI og HPC)[5] og optimalisering av modeller» (Meteorologisk institutt, 2019).

Meteorologisk institutt er helt avhengig av å ha stabile og gode tjenester og har valgt tre hovedlinjer i sin sourcingstrategi: Instituttet vil ta i bruk og utvikle egne IT-ressurser knyttet til kjernevirksomheten, kjøpe tjenester og programvare i markedet når det er kostnadseffektivt, og samarbeide nasjonalt og internasjonalt for å opprette og vedlikeholde kompetanse og kapasitet innenfor kjerneområdene, som lagring, beregning og tilgjengeliggjøring av meteorologiske data.

Sourcingstrategien bygger på noen hovedprinsipper. For det første er det viktig å sikre kjernekompetanse for instituttet slik at det kan drifte og utvikle sin hovedaktivitet. IT-kompetanse som også kjenner til det geofaglige feltet, er sentralt. Dette er kompetanse instituttet vil dele og utvikle i samarbeid med andre nasjonale og internasjonale aktører. Meteorologisk institutt har, ifølge IT-direktøren, forsøkt å gjøre beregninger av kostnadene ved å lagre og drifte de store datamengdene hos skyleverandører, men har konkludert med at det foreløpig er langt billigere for instituttet å lagre og drifte data selv.

I Meteorologisk institutts sourcingstrategi er det et hovedprinsipp for innkjøp av tjenester og programvare at det bør foreligge et modent marked. Det vil si at det må være flere tilbydere og mulig å skifte leverandør. Det er også viktig å sikre at instituttet ikke «låses inne» hos en leverandør, fordi det er kostbart eller vanskelig å flytte data eller tjeneste. Programmer som brukes av mange aktører, såkalt hyllevare, er egnet for kjøp og driftig av eksterne aktører, framfor å drifte internt. Før det tas valg mellom å utvikle og drifte programmer og tjenester selv eller kjøpe dette i markedet, skal pris (pris vs. Total Cost of Ownership) og risiko vurderes (Meteorologisk institutt, 2019).

Et tredje hovedprinsipp i sourcingstrategien er at instituttet skal utnytte de samarbeidsmulighetene som finnes både nasjonalt og internasjonalt. Det internasjonale samarbeidet knyttet til datalagring og beregninger har vist seg svært nyttig og rimelig. Å styrke det internasjonale meteorologiske samarbeidet ligger også innenfor instituttets samfunnsoppdrag. Meteorologisk institutt har god kompetanse på Linux og ønsker innenfor klima- og miljøsektoren å bli en tilbyder på dette området (Meteorologisk institutt, 2019).

[5] PPI (Post Processing Infrastructure) benyttes som parallellisert distribuert virtualisering og prosesseringsinfrastruktur. PPI er kraftig lokalt klustret regnekapasitet som brukes til å bearbeide modelldata slik at de kan visualiseres for brukerne. HPC (High Performance Computing) kan omfatte avansert modellering og bruk av kunstig intelligens.

Selv om Meteorologisk institutt ønsker et økt internasjonalt samarbeid velkommen og er åpent for å kjøpe skytjenester der det er billigere og bedre enn å drive det selv, er det viktig for instituttet at det har kompetanse i Norge som kan håndtere data, og som kan kjøre virksomhetskritiske data. Det sikrer kompetanse til å kunne kvalitetssikre data og kontroll med tjenesten. Samtidig er deling av data og informasjon nødvendig innenfor meteorologien, og det er viktig for Meteorologisk institutt å samarbeide slik at instituttet ikke blir stående alene.

6.3 Nav

Arbeids- og velferdsetaten er underlagt Arbeids- og sosialdepartementet og forvalter arbeidsmarkedsloven, folketrygdloven (med unntak av kapittel 5) og andre lover hvor oppgaver er lagt til etaten. Nav hadde i 2018 over 14 000 ansatte, hvorav 750 årsverk ble benyttet i Arbeids- og velferdsdirektoratets sentrale IT-avdeling (Arbeids- og velferdsdirektoratet, 2019, s. 61 figur 24).

Organisering av IKT-tjenestene

Nav har over flere år utviklet IT-tjenester for selvbetjening og automatisering av arbeidsprosessene. I 2018 ble det etablert en referansearkitektur og teknologiplattform for automatisering og hendelsesorientering av saksbehandling, og anskaffelser av verktøy bidro til å gjøre alle deler av Nav mer datadrevet. Rundt 15 000 ansatte hadde ved utgangen av 2018 fått bærbar pc, og ny digital arbeidsflate ble gjort tilgjengelig både på pc og tynnklient. Microsoft 365 er tatt i bruk for de fleste ansatte (Arbeids- og velferdsdirektoratet, 2019, s. 61). Nav har fortsatt en del IT-systemer med lang historie. Infotrygd rundet 40 år i 2018 (Ringnes, 2018).

I 2016 endret Nav strategi på IT-feltet. Fram til da hadde etaten satset på å skaffe spisskompetanse gjennom kjøp av tjenester. Etaten hadde avtaler i konsulentmarkedet både på forvaltning og på utvikling. Nav manglet et eget utviklingsmiljø. Fra 2017 begynte etaten å bygge opp utviklerkompetansen slik at de kunne ta eierskap i utvikling og forvaltning av de systemene som er unike for etaten. Man erkjente at det var nødvendig å ha god kompetanse også når man valgte å kjøpe inn systemer og tjenester. I perioden 2017 til 2020 steg antall IT-ansatte fra rundt 550 til 750, og veksten kom nesten utelukkende innenfor utviklere og design. Ledelse og støttefunksjoner er blitt redusert.

Samtidig endret Nav på arbeidsformen. Tidligere har forretningssiden laget et system med kravspesifikasjoner som IT-avdelingen har brukt for innkjøp av tjenester. Nå har man valgt en arbeidsform med autonome tverrfaglige team. De jobber med grenseflaten mot brukerne og tar brukernes problemstillinger som utgangspunkt for utvikling. Teamene har stor frihet til å løse oppgavene innenfor visse rammer, og arbeidet vurderes både ut fra IT-løsninger og tilfredshet hos brukerne. Det gjør at digitaliseringen blir en integrert del av tjenesteleveringen. Dette skal sikre «raskere, bedre og billigere» tjenester med redusert risiko fordi teamene fortløpende leverer små deler om gangen (Arbeids- og velferdsdirektoratet, 2019, s. 62).

Sourcingstrategi

Navs sourcingstrategi har som formål å «maksimere verdiskapningen i etaten gjennom optimal bruk av egne ressurser i kombinasjon med differensiert bruk av leverandørmarkedet i form av standardløsninger eller kjøp av tjenester» (Arbeids- og velferdsdirektoratet, 2019, s. 61).

IT-direktøren peker på at Nav går bort fra de store monolittiske systemene og over til mer mikrotjenestearkitektur, med små komponenter som kan endres etter behov, og med løsere avhengighet av hverandre. Dette skal opprettholde endringsdyktighet over tid (intervju 3.1.2020). Navs strategi er å bygge opp utviklingstjenestene selv og sette mer av driften ut i skyen. Mens man tidligere driftet datasenteret selv, og kjøpte utviklingstjenester i markedet, er strategien nå den omvendte. På sikt er målet å flytte standardisert teknologi ut i skyen. Dette kan for eksempel være lagring og prosessering. Skyleverandørenes tjenester kan skaleres, og de kan levere prosesseringskraft i perioder Nav trenger det. Skytjenester på høyt nivå er tjenester som de autonome utviklingsteamene i Nav bør kunne benytte etter behov. Nav har derfor som strategi å gå i skyen med infrastruktur og plattform. «Men applikasjonene våre ønsker vi ikke nødvendigvis å flytte ut som de er», påpeker IT-direktøren, «de må vi bygge på nytt i en ny arkitektur» (intervju 3.1.2020).

Nav har ikke så store datamengder at lagring i sky byr på kostnadsutfordringer. Behovet for prosessorkraft kommer periodevis og egner seg også for kjøp i skytjenester. Nav har imidlertid mange ansatte og mange brukere av datatjenestene. Det gjør at lisensbaserte produkter, som Microsoft 365, som alle ansatte bruker, blir svært kostbart.

For Nav har digitalisering gitt betydelige effektivitetsgevinster. Nav jobber med digitalisering innenfor alle ansvarsfeltene. I 2018 fikk for eksempel alle arbeidsgivere tilgang til en digital inntektsmelding. Det innebar at 900 000 papirskjemaer ble fjernet årlig (Arbeids- og velferdsdirektoratet, 2019, s. 62).

Nav har også samarbeidsprosjekter med ulike aktører som Skatteetaten og EU for å sikre modernisering av folkeregisteret og integrasjon med velferdstjenestene i EU. Digisos er et samarbeidsprosjekt mellom Nav, KS og åtte kommuner for å digitalisere tjenester til brukere av sosialtjenestene.

Nav behandler mye sensitive data, blant annet helsedata. De siste års endringer av personvernlovgivningen har rettet oppmerksomheten blant annet mot databehandleravtaler og lagring. Navs jurister og innleide advokater som er eksperter på personvern, har jobbet med de store dataleverandørene for å få på plass nødvendige avtaler. I avtaler med disse aktørene kan man få avtalt lagring og databehandling i definerte regioner. De fleste av Navs data kan lagres i EU-regionen, men enkelte tjenester er av samfunnskritisk karakter og kan måtte håndteres i Norge. Dette er regulert i sikkerhetsloven.

IT-direktøren mener Nav opplever personvernreguleringen som klar og tydelig. På reguleringssiden kan forvaltningsloven og særlovgivning som er skrevet i en annen tid og av folk uten spisskompetanse på teknologi, være en større utfordring. Det ligger noen muligheter i dagens teknologi som lovverket ikke åpner for, selv om dette hadde vært til beste for brukeren. Lovgivningen krever for eksempel at søkere må sende inn søknader med mye informasjon Nav sitter på fra før. Dersom Nav fikk kombinere informasjon etaten har tilgang til, ville det være mulig å etablere en mer hendelsesorientert levering av tjenester. Da kunne Nav være i forkant og være mindre avhengig av å vente på at brukere skal sende inn søknader som strengt tatt er unødvendige. Et annet eksempel IT-direktøren trekker fram, er tolketjeneste. I forslaget til ny lov om offentlige organers ansvar for bruk av tolk som var på høring i 2019, ble det forutsatt at det er mennesker som benyttes som språktolker. Det er sannsynligvis bare et tidsspørsmål når maskiner gjør dette like godt som mennesker, påpeker IT-direktøren.

Skal Nav lykkes i å nå sine visjoner, er en av de store utfordringene å klare å utvikle og beholde kompetanse. Nav var, ifølge IT-direktøren, tidlig ute med å ansette og utvikle teknologer selv og har klart å vokse til tross for en enorm etterspørsel etter IT-kompetanse. «For Nav er det viktig å holde på eierskapet til applikasjonene våre. Benytter vi for mange konsulenter, forsvinner dette eierskapet ut», påpeker IT-direktøren (intervju 3.1.2020).

En annen utfordring ved bruk av skytjenester er såkalt «lock in», at man blir bundet til én leverandør og ikke klarer å bytte leverandør uten store omkostninger. Et eksempel på dette er at det i praksis er vanskelig for en organisasjon å veksle mellom bruk av Microsoft 365 og Google Docs. IT-direktørene i Nav mener man må være oppmerksom på dette, og vurdere verdien av tjenesten opp mot en eventuell «lock in»-effekt når man kjøper tjenester.

Bruk av åpne standarder og avtaler som gir mulighet for raskt å gå ut av en tjeneste, kan motvirke innelåsing. Det bør være et mål å kunne skifte skyleverandør på dagen, men det vil være flere områder der dette i praksis er uhensiktsmessig.

Anskaffelsesregelverket kan også by på utfordringer på skyområdet, påpeker IT-direktøren. Det å velge en skyleverandør er en dynamisk anskaffelse. Poenget er jo å kunne skalere tjenesten opp og ned etter behov. Da kan det være vanskelig å definere alle behov i den første avtalen som inngås, og som innkjøper må man da ut med nytt anbud når behovene endrer seg. Det kan være ressurskrevende. Store leverandører vil gjerne bruke sine standardavtaler for ikke å sitte med et stort antall ulike avtaler. Det passer ikke alltid i den offentlige innkjøpsprosessen. Selv Nav er en liten kunde overfor leverandører som Microsoft og Google.

6.4 Universitetet i Bergen

Universitetet i Bergen har rundt 18 000 studenter og vel 4000 ansatte som skal ha tilgang til IKT-tjenester. IT-avdelingen er organisert som del av universitetets sentraladministrasjon og skal levere stabile IT-tjenester av høy kvalitet til brukerne ved universitetet. Universitetet driver forskning på en rekke felt og deltar i globale forskernettverk. Som del av sektoren for høyere utdanning og forskning er Universitetet i Bergen også underlagt statlige fellestjenester.

Direktoratet for IKT og fellestjenester i høyere utdanning og forskning (Unit) har ansvar for nasjonal samordning og har et overordnet forvaltningsansvar på IKT-området innenfor sektoren. Unit har myndighet til å treffe beslutninger innenfor sine hovedområder (Unit, 2020). En rekke fellestjenester som somordnet opptak, felles studentsystem, nasjonal vitnemålsdatabase og liknende leveres av Unit. Direktoratet leverer også en rekke administrative tjenester som økonomisystem og lønns- og personalsystem.

Organiseringen av IKT-tjenestene

IT-avdelingen ved Universitetet i Bergen har litt over 100 ansatte. I tillegg brukes studenter som IT-assistenter. Virksomheten har et behov for tjenester over et bredt spekter og har organisert disse ved å ta i bruk ulike typer infrastruktur.

Universitetet har et eget datasenter med servere og mulighet for tungregning (HPC). Data som universitetet mottar fra CERN, og som benyttes innen forsking i partikkelfysikk, mates inn i en tungregnemaskin som utnyttes opp

mot 100 prosent. Den høye utnyttelsesgraden gjør det rimelig for virksomheten å drifte maskinen selv framfor å kjøpe regnekapasitet av andre. Universitetet har også funnet det billigere å ha lagringskapasitet på egne servere. I et eget drevet anlegg kan data som ikke er i bruk, men som man skal ta vare på, flyttes til enklere lagringsmedia og til slutt legges over på tape. Dette er en veldig kostnadseffektiv måte å lagre data på, som for eksempel Amazon bruker.

For å kunne tilby en kostnadseffektiv skytjeneste har Universitetet i Bergen og Universitetet i Oslo samarbeidet om å lage en egen skytjeneste med bruk av egne servere for sine brukere. Dette er en løsning som gir universitetet god kontroll med data. Tjenesten leveres fra infrastruktur ved UiB og/eller UiO, og det er mulig å velge mellom disse. Tjenesten kalles UH-IaaS og leveres i samarbeid med Uninett. Virksomhetene behøver ikke betale for opp- eller nedlasting av data, og data forlater ikke Norge. IT-direktøren mener dette gir forskere enkel, kostnadseffektiv tilgang på skytjenester som har vist seg å være effektiv. Forskerne får også god kontroll over sin forskningsinfrastruktur ved å ha den nær seg, og det er lett å ringe IT-tjenesten hvis noe skjærer seg.

Universitetet i Bergen har valgt å kjøpe tjenester der volumet er stort. Microsoft 365 leveres som skytjeneste med tilknyttet skylagring. Det er praktisk for forskere som samhandler i et internasjonalt nettverk, å benytte tjenester som leveres for eksempel fra Google og Dropbox. Dette er skytjenester universitetet har mindre styring med, og den enkelte forsker må dermed være påpasselig med at personvern og sikkerhet ivaretas.

Etter diskusjon om sikkerheten ved lagring på Microsofts skytjeneste valgte Universitetet i Bergen å ta egen backup av denne skytjenesten for å sikre brukerne mot tap av data. Microsoft 365 Exchange Cloud er ikke satt opp for å håndtere gjenfinning av slettede data (data recovery) (Gartner, 2020). Det kan derfor være nødvendig å ta backup med tredjepartsløsninger for å hindre at data går tapt, for eksempel ved uforvarende sletting eller fiendtlige angrep (hackere, illojale ansatte eller feil bruk av tredjeparts programvare).

IT-direktøren mener Universitetet i Bergen har begrenset bruk av konsulenter. Konsulenter blir brukt der det trengs spisskompetanse eller i forbindelse med større prosjekter, blant annet prosjekter som gjennomføres i samarbeid med Direktoratet for forvaltning og økonomistyring (DFØ).

Sourcingstrategi

Kunnskapsdepartementet la i 2017 fram en digitaliseringsstrategi for universitets- og høyskolesektoren (Kunnskapsdepartementet, 2017). På bakgrunn av denne har Unit laget en handlingsplan for digitalisering i høyere utdanning og forskning (Unit, 2019). Denne handlingsplanen legger føringer på hvordan universiteter og andre institusjoner i kunnskapssektoren, inkludert helsesektoren og forskningsinstituttene, skal går fram for å realisere statens og Kunnskapsdepartementets strategi. Handlingsplanen krever at virksomhetene tar i bruk skytjenester «[n]år det ikke foreligger spesielle hindringer» (Unit, 2019, s. 7). Det understrekes samme sted at offentlige virksomheter skal outsource tjenester «som markedet kan gjøre bedre og mer effektivt». Som andre kunnskapsvirksomheter må Universitetet i Bergen forholde seg til disse føringene. Samtidig er staten opptatt av å bygge ut fellestjenester i egen regi for å drifte sine virksomheter mer rasjonelt. Også dette påvirker universitetets handlingsrom og veivalg innenfor IKT-området.

Universitetet i Bergen har vedtatt en sourcingstrategi for perioden 2019–2022 (Universitetet i Bergen, u.å.). Strategien omfatter administrative og tekniske tjenester og er utformet som en veiledning for beslutninger om hvorvidt tjenester skal utføres med interne ressurser, skaffes gjennom tjenestekjøp eller organiseres gjennom et samarbeid med en ekstern virksomhet.

Sourcingstrategien legger noen rammer for de vurderingene som må gjøres i forbindelse med et valg om sourcing, og peker på forhold som må vurderes og begrunnes som del av beslutningsgrunnlaget. Som del av rammeverket inngår blant annet krav stilt av myndigheter og andre statlige organer med styringsrett (Unit) samt statlige fellesanskaffelser som kan bli styrende. Det understrekes også at Universitetet i Bergen skal være en seriøs aktør ved anskaffelser og blant annet stille krav til lønns- og arbeidsvilkår. De forholdene som skal vurderes og begrunnes i forbindelse med en beslutning, er blant annet

- primærvirksomheten: tjenestens betydning for universitetets primærvirksomhet
- kapasitet og kvalitet
- tidshorisont
- hyllevare eller skreddersøm
- velfungerende leverandørmarked
- helhetlig leveranseansvar
- sikkerhetskrav
- risiko
- hensyn til ansatte og samfunnsansvar

- kostnad

Sourcingstrategien sier at tillitsvalgte og vernetjenesten skal tas med så tidlig som mulig i beslutningsprosessen.

IT-direktøren ved universitetet peker på at den tekniske utviklingen går mot sammenkobling av IT-tjenester, og at mer eller mindre åpne standarder gjør det mulig å kombinere og kjøpe tjenester nesten uavhengig av hvor i verden de finnes. Dette er en sentral driver som påvirker hvilke valg som tas. Universitetet i Bergen skal prioritere sine IT-ressurser inn mot primærvirksomheten. Dette er det grunnleggende. Det er viktig at tjenestene sikrer at universitetet har kontroll på det som inngår i kjernevirksomheten, der forsknings- og undervisningsdata er det primære. Det er der verdiene ligger, og de må beskyttes (intervju 9.1.2020).

Det er en utfordring å ivareta datasikkerheten og personvernreglene (GDPR) på IKT-området når det er mange brukere som arbeider på ulike plattformer. Sikkerheten ivaretas ikke bare gjennom kontroll med leverandørsiden. Også brukerne må forholde seg til sikkerhet og personvernregler. Dette krever opplæring og kompetanse i virksomheten.

7 Organiseringen av IKT i fire kommuner

Kommunene og fylkeskommunene utgjør en betydelig del av offentlig sektor i Norge. Det kommunale selvstyret har lange tradisjoner. Det gir seg utslag i betydelig variasjon i IKT-driften kommunene imellom. Varierende størrelse og befolkningssammensetning gjør også at behov og muligheter varierer. Mange kommuner har i tillegg søkt å samarbeide om IKT-driften for å få en rasjonell og kostnadseffektiv drift. Samtidig gjør samhandling mellom kommunene og mellom kommuner og statlige virksomheter det i økende grad nødvendig å samordne IKT-tjenestene. Dette er med å påvirke kommunenes valg og strategier.

De fire kommunene som er valgt ut til denne undersøkelsen, representerer ulike størrelser og beliggenheter. Oslo og Bergen er de to største bykommunene i landet, mens Bodø og Fauske kan beskrives som en middels stor og en liten bykommune. Beliggenheten og størrelsen påvirker tilgangen til kompetanse og ressurser, og kommunene har utviklet seg noe forskjellig på IKT-feltet.

Beskrivelsen av de enkelte kommunene bygger på intervjuer og tilgjengelig informasjon fra dokumenter og nettsider. Teksten er ment å presentere kommunens erfaringer og er ikke en analyse eller fullstendig beskrivelse av kommunenes IKT-drift.

7.1 Bergen kommune

Bergen kommune har ansatte som utfører rundt 15 000 årsverk, og en befolkning på over 280 000. Kommunen har en parlamentarisk styreform.

Enhet for digitale driftstjenester er plassert under byråd for finans, innovasjon og eiendom og er underlagt kommunaldirektøren for HR, digitalisering og eiendom. Enheten har en konsernfunksjon, det vil si at den har ansvar for IT-driften i hele kommunen. Den skal levere infrastruktur, fagsystemer, databaser og lokalt IKT-utstyr som pc-er og liknende. Målet er å levere tek-

nologi som dekker brukernes behov for stabilitet, tilgjengelighet og tilfredsstillende kapasitet. Kommunen har en rekke brukergrupper som arbeider med personsensitivt materiale, og derfor legges det stor vekt på sikkerhet (Bergen kommune, u.d.).

Bergen kommune legger stor vekt på å digitalisere arbeidsprosesser og samordne bruken av digitale verktøy (Bergen kommune, 2018, ss. 32, 364).

Organiseringen av IKT-tjenestene

Bergen kommune har startet en rekke programmer for å følge opp arbeidet med digitalisering og har etablert Program for digital fornyelse for å samordne prosjektene og sikre en helhetlig implementering av dem (Bergen kommune, 2018, s. 364). Tidligere hadde Bergen kommune et driftsmiljø for IT i hver etat, men kommunen har over tid arbeidet målrettet for å samle driften av IKT i en konsernfunksjon. Selv om de ulike byrådsavdelingene har et tjenesteansvar for fagsystemene i sine etater, er driftsfunksjonen samlet i enhet for digitale driftstjenester på konsernnivå. Dette er ment å åpne for bedre integrasjon av fagsystemer og tjenesteområder.

Kommunen har et eget datasenter hvor kommunens systemer driftes samlet. Det som fysisk skal driftes av Bergen kommune, samles her. På systemsiden har dette ført til at kommunen nå har ett sak- og arkivsystem, ett innkjøpssystem, ett HR-system og ett økonomisystem, som er felles for hele kommunen. Enhet for digitale driftstjenester har et overordnet ansvar blant annet for informasjonssikkerhet, personvern, virksomhetsarkitektur og utvikling av de digitale tjenestene.

Bergen kommune har også et driftssamarbeid med andre kommuner i regionen og et digitaliseringsrettet samarbeid med sikte på å følge opp myndighetenes krav til digitalisering av sektoren, blant annet innenfor e-helse.

Sourcingstrategi

Bergen kommune har ikke en fastlagt sourcingstrategi. Hvis kommunen følger et prinsipp for drift og innkjøp av digitale tjenester, kan det kalles en multisourcingstrategi, påpeker IT-direktøren. Kommunen vurderer fra sak til sak hvilke løsninger som er de beste. Selv om mye driftes av kommunen selv i dag, er det ifølge IT-direktøren ikke et mål i seg selv at kommunen skal fortsette driftingen: «Vi har en pragmatisk holdning til om fagsystemer eller andre leveranser havner i skyen eller ender på bakken» (intervju 9.1.2020). Det som er styrende, vil være de faglige kravene til informasjonssikkerhet, arkitektur og dataflyt og integrasjon.

IT-direktøren peker på at det er lett å se på sourcingstrategi utelukkende i lys av det tradisjonelle skillet mellom å drifte selv eller kjøpe inn som tjeneste. For kommunen er utviklingen og etableringen av de nye fellestjenestene i offentlig sektor en viktig del av bildet. I forholdet mellom stat og kommune er det en rekke fellesprosjekter som gjør at kommunens tjenester kanskje vil bli driftet av e-helsedirektoratet eller av KS, eller at drift for alle kommuner i Vestland legges ett sted. Digitaliseringen av sammenhengende tjenester vil være en sentral faktor i avgjørelsen av hvordan Bergen kommune og andre kommuner vil drifte sine systemer i framtiden.

Utviklingen av skytjenester vil, ifølge IT-direktøren, være en av de viktige driverne for endring i tiden som kommer. Bergen kommune har i mange år hatt driftssystemer som har vært driftet med små endringer. Dette systemet utfordres nå av mer dynamiske systemer som leveres via sky og oppdateres og utvikles kontinuerlig. Forventninger til informasjonssikkerhet, inntrengingssikkerhet og personvern vil også være styrende for hvordan kommunen arbeider med de digitale tjenestene, mener han. Arbeidet i datarommene bli endret uavhengig av hvilken sourcingstrategi man i dag tror er den rette. Skytjenestene vil ikke bety at kommunene fratas ansvar. De store økosystemene som bygges, krever at leverandørene forstår hvilken bransje de leverer til, og hvilke behov kommunene har, samtidig som kommunen som kunde ikke blir fri for ansvar.

En av utfordringene for kommunene er at leverandører ikke alltid har nok kunnskap om kommunene og forståelse for kommunal drift og hvilke behov det offentlige har. Det er derfor viktig at kommunene selv har god kompetanse både ved innkjøpsprosessen og i dialogen med eksterne leverandører. Ved kjøp av såkalt hyllevare ser kommunene også at store leverandører gjør endringer som kommunen som kunde ikke kan påvirke. Det kan i tillegg være vanskelig for små kunder, som for eksempel en kommune, å få til endringer i leveransen. Dette begrenser fleksibiliteten ved innkjøp av hyllevare.

Bergen er en universitetsby, og kommunen er stor. Dette er ifølge IT-direktøren med på å gjøre kommunen til en attraktiv arbeidsgiver med tilgang til god kompetanse selv om arbeidsmarkedet er stramt. Bergen kommune har god innkjøpskompetanse, et stort IT-miljø og mange faglige utfordringer å jobbe med. Kommunens verdigrunnlag og det å jobbe i offentlig sektor kan også virke positivt for kommunen når den skal tiltrekke seg IT-kompetanse, påpeker IT-direktøren.

IT-direktøren peker på at organisering av IKT i en konsernmodell, slik Bergen har gjort, gjør det lettere å sikre samhandling mellom ulike aktører både i kommunen og mellom kommunen og eksterne aktører. Kommunen har stor

kompleksitet i oppgaveløsningen, og digitaliseringen av tjenester og nye måter å løser oppgaver på gjør at samordning blir viktig. Myndighetene stiller også krav om at kommunesektoren skal opptre enhetlig. Et eksempel er e-helse-området, der digitale tjenester skal sikre felles journal og bedre samhandling mellom kommunene og mellom kommunene og de statlige helseinstitusjonene. Det gjør at kommunene må opptre mer enhetlig (intervju 14.1.2020). Kravene til sikkerhet og til personvern og kravene til integrasjon og utvikling av tjenester tilsier også at systemene blir mer sårbare hvis du har miljøer som er splittet opp. Organiseringen av IT-funksjonen i en konsernmodell i kommunen kan gjøre det lettere å ivareta et helhetlig perspektiv på digitaliseringen, ifølge IT-direktøren.

Foreløpig er kostnadene for lagring i skyen stor sammenliknet med å drifte egne servere, påpeker IT-direktøren. Men over tid vil integrasjonen i systemene og utviklingen av tjenesten trolig føre til at drift av egne servere blir uhensiktsmessig eller kostbart, og kommunens data vil ligge andre steder enn i Bergen. Det er funksjonaliteten som kommer til å bli avgjørende. Kommunen har hatt diskusjoner om hvor data skal lagres. Det har blitt stilt krav om lagring i EØS-området, men det har også blitt stilt spørsmål om ikke data bør lagres i Norge. Beslutninger om hvor data skal lagres, må tas fra sak til sak og fra område til område, mener IT-direktøren, som tror det vil være lite hensiktsmessig å ha én strategi, selv om mer og mer havner i skyen. Det vesentlige for kommunen er å få gode prosesser for styringen av personopplysninger.

For Bergen kommune har det vært krevende å forholde seg til arkivloven som skal sikre at viktig informasjon lagres for ettertiden eller for forvaltningsmessig dokumentasjon. Teknologiutviklingen går fortere enn denne type lovgivning som for eksempel ikke skiller mellom ulike typer kommunikasjon. Det kan for eksempel være vanskelig å etterleve kravene i arkivloven for chatter og tekstmeldinger og overføre disse på en meningsfull måte til et arkiv. Det er ikke tilrettelagt for automatisk overlevering til arkivet, og det må i tilfelle skje manuelt. Da mister man funksjonaliteten digitale tjenester skal gi, mener IT-direktøren.

7.2 Bodø kommune

Bodø er en kommune med rundt 52 000 innbyggere og over 6000 ansatte. Digitaliserings- og IKT-kontoret er underlagt administrasjonsavdelingen. Hovedmålene for digitalisering, som listes opp på kommunens nettside, er en forenklet innbyggerdialog, å gi medarbeiderne digital kompetanse og gi tjenesteproduksjonen digital støtte (Bodø kommune, u.å.).

Organiseringen av IKT-tjenestene

Bodø kommune har en egen serverpark for lagring av kommunens data og eier selv den digitale infrastrukturen. Kommunen har valgt å lease maskinparken i serverrommet i stedet for å kjøpe egne servere, for å ha fleksibilitet og fordi skyteknologien endres raskt. Kommunen bygger selv ut en fysisk infrastruktur med bredbånd og trådløst nett til sine bygg og der det er behov.

Kommunen har de siste 15–20 årene satt bort drift av hele IT-systemet til en driftspartner. For noe tid siden skiftet kommunen driftspartner. Bodø bruker også en konsulentvirksomhet som tredjepart for å vurdere om driftspartneren følger avtalen og leverer etter faglige standarder. Gjennom å bruke en tredjepart til å revidere driftspartneren forsøker kommunen å følge etablert «beste praksis», påpeker IKT-sjefen. Ettersom selve driften er satt bort, klarer Digitaliserings- og IKT-kontoret seg med fem–seks ansatte som forvalter kommunens IKT for rundt 10 000 brukere (intervju 8.1.2020).

I tillegg til egen serverpark har kommunen tatt i bruk enkelte applikasjoner som skytjeneste for å lære om utfordringer dette gir. Kommunen bruker blant annet Microsoft 365. I tillegg har Atea en ASP-server som Bodø kommune bruker. Evry leverer saks- og arkivsystemet Elements som en ASP-løsning, men har signalisert at de ønsker å levere dette i skyløsningen på Microsofts Azure-plattform.

Sourcingstrategi

Kommunens digitaliseringsstrategi angir noen overordnede mål og generelle prinsipper for digitalisering, men gir ingen konkrete retningslinjer for sourcing (Bodø kommune, u.å.). Kommunen har lang erfaring med å sette ut driften av IKT til en driftspartner. I forbindelse med skifte av driftspartner i 2017 opplevde kommunen betydelige problemer. Undertegning av kontrakten med ny driftspartner ble utsatt i over et år fordi det oppsto konflikt mellom kommunen og tidligere driftspartner (Atea, 2017). Det oppsto også diskusjoner med den nye driftsoperatøren om hvorvidt kommunens serverpark og øvrige infrastruktur hadde den standarden som var forutsatt. Kommunen måtte gjennom en løpende drøfting med driftspartneren om hva som lå inne i kontrakten, og hva som var et eventuelt mersalg.
IKT-plattformen med servere og nettverk ble betydelig oppgradert i tiden etter skiftet av driftspartner, noe som ga bedre stabilitet og responstid for kommunens brukere (Bodø kommune, 2018).

En av utfordringene med utsetting av tjenester er kompetansebehovet. I prosessen med anbud på drift av kommunens IT-anlegg opplevde kommunen stort behov for merkantil kompetanse. Selv om kommunen hadde god teknisk

kompetanse, var utformingen og forvaltningen av avtaler utfordrende, ifølge IKT-sjefen.

IKT-sjefen mener at leasing av maskinparken gjør kommunen mer fleksibel dersom det blir behov for å gjøre endringer, for eksempel å ta i bruk skytjenester. Kommunen følger utviklingen av skytjenester og kommer til å vurdere om den skal ha en egen infrastruktur, eller om den skal kjøpe skytjenester for lagring av data og drift av systemer (intervju 8.1.2020). Ettersom alle de store leverandørene, som Evry og Visma, flytter applikasjonene og tjenestene ut i skyen, vil kommunen kunne lære mer om dette. Det kan gjøre at det blir unødvendig å ha egne datarom.

Et spørsmål kommunen må vurdere når den velger sourcingstrategi, er sikkerheten. Det er ikke sikkert Bodø kommune og andre kommuner klarer å holde den samme sikkerhetsstandarden som Microsoft eller andre større leverandører, påpeker IKT-sjefen. Personvern er likevel en utfordring når man beveger seg utenfor brannmuren og ut i skyen. Det gjelder både når fagsystemene legges ut i sky, og når den enkelte ansatte bruker programmer som opererer utenfor brannmuren. Kompetansen til de enkelte brukerne er en kritisk faktor. IKT-sjefen viser til et tilfelle i kommunen der passord i en av Microsofts tjenester ble kompromittert. Microsoft fanget opp dette, men det ble ikke fanget opp i kommunens egne systemer (intervju 8.1.2020).

Et spørsmål for framtiden er om alle kommuner skal opptre hver for seg, eller om det tvinger seg fram et samarbeid. Skal det utvikles en felles plattform, må noen ta ansvar for dette. Bodø kommune har et samarbeid med andre kommuner i regionen. Kommunen har et vertskommunesamarbeid med Hamarøy, Røst og Rødøy kommuner og drifter IKT for dem til selvkost. Selv om mindre kommuner klarer å drifte systemene sine, får de utfordringer når digitaliseringen øker, påpeker IKT-sjefen. Mange har ikke engang egne IKT-ansatte.

Bodø kommune bruker hyllevare. På noen felt er det et begrenset antall leverandører, for eksempel innenfor fagsystemer i helsesektoren. Det er ikke alltid enkelt å skifte ut store tunge fagsystemer, påpeker IKT-sjefen, som mener anskaffelsesregimet i offentlig sektor bidrar til å gjøre dette krevende og kostbart. Et større samarbeid mellom kommuner og mellom kommunene og det statlige helsevesenet er kanskje en løsning.

Digitalisering dreier seg ifølge IKT-sjefen først og fremst om endrede arbeidsformer. Selve teknologien har ikke endret seg så veldig, men måten den griper inn i arbeidsprosessene på, er ny. Mange arbeidsprosesser blir fullautomatisert, og teknologisk kan man møte nesten ethvert behov de kommunale tjenestene måtte ha. Det ligger likevel en utfordring i å få folk til å ta i

bruk teknologien. Det er ikke nok å kjøpe inn ny programvare. IKT-sjefen peker på at det er krevende å få organisasjonen til å stå i den kampen som kreves for å få innført nye systemer. Helsesektoren er en sektor der det skjer mye i Bodø kommune. Nå kommer fjernovervåkning og bruk av nettbrett i styringen av tjenestene. IKT-sjefen tror ikke at lovgivningen som legger begrensninger på hvor data kan lagres, har noen særlig betydning for utviklingen.

De ulike skyløsningene har fordeler og ulemper. Oppdateringer i ASP-løsningen[6] Bodø kommune bruker på saks- og arkivsystemet, blir kjørt for hver kommune. Det gir den enkelte kommune noen valgmuligheter, men er også en omstendelig prosess. Hvis saks- og arkivsystemet legges til skyplattformen Azure, vil all oppgradering skje fortløpende og felles for alle. Det gir stordriftsfordeler, men kan begrense den enkelte kommunes valgmulighet. Det kan også gjøre det vanskeligere for kommunene å stille krav til leverandørene i tjenesteavtalene (SLA)[7]. Når én stor aktør skal levere til mange mindre kunder, krever leverandørene at det benyttes standardavtaler. Hver kommune kan ikke stille egne krav til for eksempel oppetid dersom alt kjøres på en felles plattform.

En annen utfordring ved tjenester som leveres på store felles plattformer, er endringstakten. Det skjer kontinuerlige endringer og produktutvikling som brukerne må forholde seg til med en gang. Det er ikke alltid like lett å forberede organisasjonen på endringene og sikre opplæring til riktig tid, ifølge IKT-sjefen.

En fordel med skyløsninger er imidlertid at de virker over alt. Man trenger en nettadresse (URL), og så er systemet oppe og går. Det gjør det lett for de enkelte enhetene i en kommune selv å bestemme hvilke systemer de ønsker å bruke, og bestille dette, ifølge IKT-sjefen. Noen tjenester har imidlertid ingen løsning hvis kommunen trenger å ta ut ekstrakt av data. Det kan være et problem, ifølge IKT-sjefen, som peker på at kravene som stilles til offentlig virksomhet, og samspillet med kommunenes andre systemer, ikke alltid er ivaretatt i digitale tjenester.

Bodø kommune har vurdert kostnader ved ulike systemer. Ulike måter å prise tjenestene på kan gi svært forskjellige kostnader. Skytjenester er ofte priset ut fra antall brukere, enten de bruker det mye eller lite. Det gjør det

[6] Application service provider (APS) er en virksomhet som tilbyr databaserte tjenester til kunder over et nettverk. Slike tjenester kalles også «Software as a service (SaaS)».
[7] Det inngås en tjenesteavtale (Service level agreement – SLA) mellom kommunen og tjenesteleverandør som sier hvilke tjenester som skal leveres, og hvilken kvalitet disse skal ha.

dyrt for kommunene å gi flest mulig tilgang til tjenestene. Begynner man å begrense tilgangen til tjenesten, vil nytten av systemet kunne bli redusert. For kommunen er funksjonalitet og sikkerhet det viktigste. Teknologien bør ikke bli premissgiver, mener IKT-sjefen, som viser til at det er vanskelig å foreta prisberegninger og også beregne kostnadene ved å drifte tjenester selv. Han mener leverandørene må utfordres til å gi et kostnadsbilde for tjenestene. For Bodø kommune er målet med sourcingstrategien for IT å gå stegvis fram og sikre en god anbuds- og innkjøpsprosess som ivaretar kommunens behov.

7.3 Fauske

Fauske kommune ligger i Nordland og har litt under 10 000 innbyggere og rundt 1300 ansatte. IKT-avdelingen er plassert i rådmannens stab under personal- og organisasjonstjenester og har fem ansatte og tre lærlinger.

Organiseringen av IKT-tjenestene

Fauske kommune har eget serverrom og drifter egne tjenester fra dette. Programmene kommunen bruker, er stort sett hyllevare. Noen systemer, som økonomisystemet, har blitt levert fra samme leverandør i mange tiår. Kommunen har også en egenutviklet webplattform som gir tilgang til tomteinformasjon.

Fauske kommune leier fibernett av en privat leverandør for å sikre nettilgang i alle tjenestestedene i kommunen. Der det ikke er lagt kabel, benytter kommunen i dag 4G-nett.

Sourcingstrategi

Mens mindre kommuner ofte har satt ut sine IT-tjenester, har Fauske kommune foreløpig valgt å drifte disse selv. Sourcingstrategier for IKT har vært drøftet i kommunen, men det foreligger ingen vedtatt sourcingstrategi, ifølge driftsansvarlig for IKT. Pris er i noen tilfeller avgjørende. Det kan være billigere å drifte systemer selv framfor å kjøpe tjenester. En annen utfordring er kompatibilitet mellom de systemene kommunen bruker i dag, og nye skyløsninger. Det sak- og arkivsystemet kommunen bruker, passer for eksempel ikke sammen med Googles desktop-produkter. Slike forhold gjør det vanskelig for kommunen å gjøre endringer.

Kommunen vurderer å sette ut IT-tjenester der det er hensiktsmessig. En fordel kan være at det minker belastningen på IT-avdelingen. En ulempe ved å kjøpe IT-tjenester kan være at kommunen mister kontroll over data og hvor

de befinner seg, påpeker driftsansvarlig for IKT, og det kan være vanskelig å hente ut den informasjonen man har behov for. Driftsansvarlig for IKT er også bekymret for at responstiden for feilretting kan bli svekket.

Fauske kommune har et samarbeid med andre kommuner. Kommunen har siden 2007 driftet fagsystemer for andre kommuner. Det gjelder blant annet IT-system for barnevern og for sosialtjenester knyttet til Nav. Dette har, slik driftsansvarlig IKT vurderer det, fungert godt.

Også i Fause er man opptatt av at kommunene må forholde seg til de standardkontraktene de store leverandørene bruker. Dersom det offentlige kan lage en markedsplass eller en ordning for innkjøp der reguleringen kan være felles, ville dette være interessant for Fauske kommune, tror driftsansvarlig for IKT. Alle kommuner har behov for de samme tjenestene. Å ha en markedsplass som ivaretar sikkerhetsaspektet og tilgjengelighet og sikrer forutsigbare priser og kostnader, ville være fint, påpeker driftsansvarlig for IKT.

Digitaliseringen av Fauske kommune skal bidra til å gjøre arbeidshverdagen bedre for de ansatte og gi innbyggerne bedre tjenester. Det skjer mye innenfor velferdsteknologi, sykehjem og hjemmetjenesten, for eksempel bruk av sensorteknologi og styring via nettbrett. Dette vil få betydning også for Fauske kommune, mener driftsansvarlig for IKT, men han påpeker at dette ikke bare handler om ny teknologi. Bruk av slike digitale tjenester krever at de ansatte får opplæring og økt kompetanse.

Fauske kommune har virksomhet spredt mange steder i kommunen. De fleste installasjoner i kommunen skal være knyttet til nett, enten det er vannrensing, kloakk eller en boenhet. I dag blir IT integrert når man går i gang med nye prosjekter, så man slipper å sette opp IT-løsninger i ettertid. IT-konsulenten mener det med de plattformene kommunen bruker i dag, blir mye jobb med bytte av utstyr og nye oppkoblinger når noen flytter internt i et bygg eller til en annet sted i kommunen. De som bruker fagprogrammer, er tilknyttet ulike nettverk og må kobles opp manuelt. Med en annen teknisk løsning, som skyløsninger, ville det være mulig å la tilgangen følge bruker, ikke den enkelte arbeidsstasjonen. Kommunen har som mål å gå i den retningen (intervju 8.1.2020).

Fauske kommune har ikke fast bruk av konsulenter, men har en opsjonsavtale som benyttes når kommunen trenger kompetanse eller økt kapasitet. Konsulenter ble blant annet brukt ved etableringen av ny velferdsteknologi. For øvrig gjør bruk av hyllevare det enklere å håndtere drift og feilretting selv. Da har som oftest andre opplevd feilen før, og det går greit å søke etter svar.

En fordel med å drifte anlegget selv er at kommunen ikke blir avhengig av leverandører for support. IT-avdelingen i kommunen har god kompetanse og

kan løse problemer raskt, påpeker IT-konsulenten. Eksterne konsulenter eller leverandører sitter ofte i Oslo, og det tar tid å få hjelp. En annen utfordring er, ifølge IT-konsulenten, at kommunens egne IT-ansatte ikke alltid får med seg hva som skjer, når hjelpen leveres som fjernhjelp. Da lærer de ikke hvordan problemer skal løses, og kommunen kan bli mer avhengig av leverandøren med de kostnader som følger av det. IT-konsulenten peker på at det er viktig å ha kompetanse i kommunen, og at noen vet hvordan programmer og systemer skal brukes. De kan gi opplæring, og noen må gå foran og vise hvordan systemene kan brukes til å gi best mulig tjenester.

7.4 Oslo

Oslo kommune har 680 000 innbyggere og litt over 51 000 ansatte som står for 41 956 årsverk (Oslo Kommune, u.å.). Kommunen styres etter en parlamentarisk styringsmodell, og Oslo kommune har både kommunale og fylkeskommunale funksjoner.

Utviklings- og kompetanseetaten er Oslo kommunes interne tjenesteleverandør for IKT. Etaten ivaretar virksomhetsovergripende utviklings-, forvaltnings- og driftsoppgaver, som skal støtte kommunens serviceytelser til innbyggere og næringsliv. Tjenestespekteret omfatter blant annet IT (sluttbrukertjenester som sak- og arkivtjenester, HR, økonomi, mobilitet, samhandling samt IKT-driftstjenester), anskaffelser og konsulenttjenester innen organisasjonsutvikling, prosjektledelse, tjenestedesign og anskaffelser. Etaten er underlagt byrådsavdeling for finans og har rundt 350 ansatte (Oslo kommune, u.å.).

Organiseringen av IKT-tjenestene

Utviklings- og kompetanseetaten har ifølge etatsdirektøren bred kompetanse og leverer IT-tjenester til alle de 50 virksomhetene (etater, foretak og bydeler) i Oslo kommune. Utviklingen har gått i retning av å samle IT-kompetansen i denne etaten, samt i Oslo Origo (etat for digitalisering og utvikling av innbyggertjenester), men flere andre virksomheter har fortsatt egne IT-medarbeidere og egne systemdriftsmiljøer.

Oslo kommune har tidligere eid all infrastrukturen selv, men for noen år siden inngikk kommunen en avtale med Sopra Steria der hensikten var å gjøre tjenestekjøp og at Oslo kommune ikke skulle eie infrastrukturen selv. Det er en omfattende transformasjonsprosess som er i gang. Skytjenester er så smått tatt i bruk for nyutviklede tjenester, mens eldre fagsystemer fortsatt driftes i privat sky.

I 2017 signerte kommunen en avtale med Facebook om å bruke Workplace som verktøy for internkommunikasjon. I løpet av året var rundt 41 000 medarbeidere knyttet opp til plattformen.

Sourcingstrategi

Da Oslo kommune valgte å gå over fra å eie infrastrukturen selv til å gå i retning av tjenestekjøp, var målet å utvikle en multisourcingstrategi med flere skyleverandører. En grunn til dette var at de enkelte etatene har stor frihet, og at mange etater allerede hadde kjøpt seg inn i ulike skytjenester uten at dette følger en samlet strategi. Med flere skyleverandører var målet å fange opp flere av de innkjøpene som allerede var gjort, og imøtekomme ulike behov i etatene. Direktøren for Utviklings- og kompetanseetaten peker imidlertid på at det kan bli utfordrende å operere med mange skyleverandører. Det er vanskelig å sette krav til standardisering, og det kan bli mer kostbart, fordi man må forholde seg til flere grensesnitt. I praksis viser det seg også at leverandørene er ganske like, og det gir ikke kommunen mer funksjonalitet å operere med flere (intervju 13.1.2020).

Kommunen har i dag flere hundre fagsystemer og anser at det i utgangspunktet er lite å tjene på å flytte gamle fagsystemer ut i skyen. Så lenge kommunen fortsatt benytter disse systemene, vil det være mest kostnadseffektivt å drifte dem i privat sky (i eget datasenter eller hos kommunens driftsleverandør). Ved permanente og stabile systemer, der det er lite behov for å ta kapasiteten opp og ned, får man ikke utnyttet alle fordelene med skytjenester, og de kan derfor egne seg for å ha i privat sky.

Mange av fagsystemene er hyllevare, og når de etter hvert blir skiftet ut, vil kommunen vurdere å erstatte dem med en skytjeneste (Saas) hvis det leveres. Det vil gjøre det lettere i å oppgradere og endre systemene i framtiden, påpeker etatsdirektøren. I dag opplever kommunen å være låst til flere av de store programpakkene som ble kjøpt for noen år siden. Leverandørene vil ikke alltid utføre endringer i disse, og det kan være vanskelig å få hentet data ut av systemene. I framtiden vil det være viktig å sikre tilgjengelighet til data og mulighet for kobling av data.

Personvern og informasjonssikkerhet spiller også inn når kommunen vurderer bruk av skytjenester. Men her er det ifølge etatsdirektøren ikke alltid lett å se hva som er best. Hun peker på at eksperter mener at det er like sikkert eller sikrere å ha data i en offentlig, profesjonelt drevet skytjeneste. Oslo kommune har en fortløpende diskusjon og vurderer hva som kan legges ut i sky. Microsoft 365 er et eksempel på en tjeneste der noen kommuner har hatt

utfordringer, og Oslo kommune ser på hva andre kommuner har gjort, og forsøker å lære (intervju 13.1.2020).

Direktøren for Utviklings- og kompetanseetaten i Oslo kommune peker på at det er viktig å være bevisst når man kjøper skytjenester og legger data ut i skyen. Det er ikke nødvendigvis billig, og det kan være dyrt og vanskelig å trekke seg ut. Strategien til Oslo kommune er å lage en tjenestekatalog som kommunens virksomheter kan velge fra. Behov fra systemutviklingsmiljøene ivaretas spesielt. For kommunen er det viktig å sikre at virksomhetene får gode, sikre og kostnadseffektive digitale tjenester. Det er ikke et mål i seg selv å begrense valgmulighetene.

Oslo kommune har mye kompetanse, men opplever at det er vanskelig å rekruttere mange nok teknologer. Konsulentbruken er gått noe ned, men er fortsatt høyere enn ønskelig. Imidlertid ser det ut som det har løsnet litt de siste månedene når det gjelder rekruttering av etterspurt kompetanse i markedet, som arkitekter og utviklere.

8 Har vi en strategi for IKT i offentlig sektor?

Gjennomgangen av de fire statlige virksomhetene og de fire kommunene viser at det er stor forskjell på hvordan IKT-tjenestene er organisert, og i hvilken grad disse virksomhetene har lagt en strategi for framtidig innkjøp og drift av IKT-tjenester.

8.1 Organisering og drift av IKT-tjenester

De fleste virksomhetene vi har med i denne undersøkelsen, har egen drift av hele eller deler av dataanleggene. Forsvaret, Meteorologisk institutt og Universitetet i Bergen har egne driftsmiljøer. Det samme har kommunene Fauske, Oslo og Bergen. Nav har et voksende IKT-miljø, men her rettes oppmerksomheten først og fremst mot utvikling av tjenestene, mens selve driften av datasenteret kan skje gjennom tjenestekjøp. Bodø kommune har i mange år hatt en modell der hele driften av kommunens eget leasede anlegg har vært satt bort til en tjenesteleverandør. Kommunen klarer seg med rundt fem IKT-ansatte. Oslo kommune ønsker også å sette ut driften av dataanlegget.

Det er stor forskjell på de ulike applikasjonene eller programmene som brukes i en stor virksomhet. Meteorologisk institutt og Universitetet i Bergen driver til dels med spesialisert forskning og datamodellering som krever særskilte ressurser. Nav har spesialiserte programmer for ulike trygdeberegninger og velferdstjenester. Kommunene kan ha i bruk flere hundre ulike fagsystemer for å drifte ulike tjenesteområder som helse, vann og avløp eller brannvarsling. Noen av disse programmene er lette å få tak i som såkalt hyllevare, mens andre er spesialiserte med bare et lite antall mulige leverandører. Mens alle virksomhetene i denne undersøkelsen kjøper eller er positive til å kjøpe skytjenester som er hyllevare, for eksempel Microsoft 365, Google Suite eller kontorstøttesystemer, ser de driften av fagsystemene som mer kritisk. Universitetet i Bergen og Meteorologisk institutt legger vekt på at virksomheten må ha kontroll både over datalagring, drift og utvikling der dette

omfatter kjernevirksomhet. Undersøkelsen viser at det er variasjon mellom virksomhetene i måten IKT driftes på, og hvilke deler av IKT-driften som virksomheten mener lett kan og/eller bør settes ut som skytjenester, og hvilke deler virksomhetene mener den bør drifte selv eller på annen måte skjerme fra allmenne skytjenester. Driftsmodellen kan også variere internt i de enkelte virksomhetene.

8.2 Sourcingstrategier og utviklingstrekk

Virksomhetene i denne undersøkelsen har i ulik grad utformet egne sourcingstrategier for IKT. Ingen av kommunene har utformet en skriftlig sourcingstrategi, men enkelte har formulert en utviklingsretning gjennom svært generelle formuleringer. De målene som er satt opp for framtidig utvikling av IKT, varierer også i detaljnivå. Gjennomgangen av virksomhetene viser likevel at det er noen felles utviklingstrekk bak de tankene som er formulert i strategier, og de synspunktene som kommer til uttrykk gjennom intervjuene som er gjennomført.

1) Strategisk bruk av IKT

Mens datadrift i stor grad tidligere har blitt sett på som en støttefunksjon til virksomhetens tjenesteproduksjon, ses den nå i økende grad som en integrert del av de tjenestene virksomheten ønsker å tilby. Dette er et utviklingstrekk som går igjen i alle virksomhetene. IKT-strategien i Forsvaret understreker dette. Informasjonsinnhenting og sammenstilling av informasjon er blitt en sentral del av forsvarets aktivitet og blir også integrert i våpensystemene. Dette gjør at utvikling og bruk av IKT er en sentral del av Forsvarets IKT-strategi.

Også kommunene legger vekt på at digitalisering av tjenestene er et av de sentrale målene for framtidig IKT-drift. Å bygge smarte byer og kommuner er blitt et uttalt mål mange steder i landet (Agenda Kaupang, 2019). I Fauske kommune blir for eksempel dataavdelingen nå tatt med på planleggingsstadiet når nye tjenester skal utvikles og kommunen skal gjøre endringer i sin organisasjon. Målet er at IKT-driften skal bli bedre integrert med kommunens øvrige operasjoner.

I Nav har dataavdelingen fått en mer sentral rolle i utviklingen av etatens tjenester gjennom samarbeid i autonome tverrfaglige team. Teamene skal ta brukernes problemstillinger som utgangspunkt for utviklingen av tjenester, og målet er at digitaliseringen blir en integrert del av de tjenestene Nav leverer.

2) Sentralisering

Etter hvert som IKT har fått en mer sentral plass i virksomhetenes drift, har det foregått en økende sentralisering av IKT-driften. Dette er særlig tydelig i de store kommunene Oslo og Bergen. Disse har tidligere hatt egne driftsmiljøer for data i de ulike etatene med ansvar for etatenes egne fagsystemer. Dette er nå under endring, og kommunene samler ansvaret for IKT i egne enheter med stabsfunksjon. Dette skal åpne for bedre integrasjon av fagsystemer og tjenesteområder. Bergen har kommet noe lenger enn Oslo i denne prosessen, men utviklingen er den samme.

Nav har også en sentral IT-avdeling som har vokst de siste årene. Også her er målet å sikre en samlet og integrert utvikling av tjenestene. Sentraliseringen er likevel ikke entydig. Den nye arkitekturen som nye IT-systemer skal bygges etter, åpner for at datasystemene kan utvikles i mindre biter, som byggeklosser. Det har gjort det mulig å etablere selvstendige utviklingsteam som jobber tett med brukere og Navs egne ansatte om å utvikle tjenestene.

Også Forsvaret har en sentralisert enhet som drifter og leverer IKT-tjenester: Cyberforsvaret. Forsvarsdepartementet skal ha en styrende rolle. Men Forsvaret er en stor og sammensatt organisasjon, og gjennomgang av organisasjonen viser at IKT-miljøet oppfattes som fragmentert og at funksjoner og kompetanse dupliseres. IKT-strategien i Forsvaret legger derfor opp til å etablere en styringsmodell som kan styrke den sentrale koordineringen fra departementet. Målet er at modellen gir «tydeligere rammer og prinsipper for IKT og etterlevelse av strategiske føringer» (Forsvarsdepartementet, 2019, s. 49).

3) Oppmerksomhet rettet mot kjernevirksomheten

Et tredje trekk ved sourcingstrategiene i virksomhetene som er undersøkt, er at virksomhetene retter oppmerksomheten og egen datadrift mot kjernevirksomheten. Dette er særlig framtredende i de statlige virksomhetene som utfører spesialiserte oppgaver.

Meteorologisk institutt er en av virksomhetene som klarest har etablert et skille mellom kjerneoppgaver, der drift og utvikling skal håndteres av virksomhetens egne IT-ansatte, og støtteoppgaver som er satt ut til tjenesteleverandører som leverer disse som skytjenester. E-post, økonomisystem, og sak- og arkivprogram er blant tjenestene som i dag leveres som skyløsninger til Meteorologisk institutt.

Også Universitetet i Bergen uttrykte et klart mål om å konsentrere egen IKT-kompetanse rundt drift og lagring av data knyttet til forskning og undervisning. Dette kan universitetet i dag gjøre billigere enn eksterne tilbydere av

tjenester. Dessuten representerer data knyttet til forskning og undervisning svært store verdier som må beskyttes. Å opprette og drifte egne skyløsninger, delvis i samarbeid med andre universiteter, har vært en prioritert oppgave for Universitetet i Bergen, blant annet for å ivareta den nødvendige sikkerheten og beskytte data mot ulike former for spionasje.

Også flere av kommunene og Nav har rettet oppmerksomheten mot kjernevirksomhet. Disse virksomhetene har definert kjernevirksomheten som tjenesteyting og utvikling av tjenestene mer enn lagring og prosessering av data. Både Nav, Oslo kommune og Bodø kommune har valgt å sette ut hele eller deler av IKT-driften til en tjenesteleverandør, mens målet for disse virksomhetene er å bruke egne ressurser på å utvikle og støtte tjenesteytingen slik at den kan utvikles gjennom å ta i bruk nye digitale løsninger.

I Forsvaret må kjernevirksomhet forstås på en egen måte. Dels vil data og prosessering knyttet til de enkelte våpnene og våpensystemene være del av kjernevirksomheten. Her foregår ikke beregningene i en sentral datamaskin, men i våpenet selv eller nært knyttet til våpenet (edge computing). Samtidig er innsamling av informasjon og sammenstilling av informasjon en del av Forsvarets kjernevirksomhet. Dette vil foregå i nettverk og i sentrale enheter. Et uttrykk for denne dobbeltheten finner vi i Forsvarets IKT-strategi der et av målene for styring beskrives som «koordinert og delegert» (Forsvarsdepartementet, 2019, s. 48).

4) Staten krever samordning

Selv om statlige virksomheter og kommuner i noen grad selv kan bestemme hvilke IKT-løsninger de vil velge, og myndighetene oppfordrer til å velge skyløsninger fra markedsaktører, krever også myndighetene samordning av IKT-løsningene på visse områder. Digitaliseringsrundskrivet fra regjeringen pålegger statlige virksomheter å bruke nasjonale fellesløsninger som digital postkasse og Altinn. Flere av kommunene var opptatt av at statens krav til samordning innenfor visse områder vil legge føringer for IKT-politikken i framtiden. Et eksempel på et slikt område er e-helse, der det nå i Akson-prosjektet jobbes med å etablere et felles elektronisk journalsystem for dokumentasjon av helsehjelp og pasientadministrasjon (Direktoratet for e-helse, u.å.).

Statlige virksomheter kan oppleve et samordningspress når det gjelder digitale løsninger for håndtering av drift og økonomi. Innenfor universitets- og høyskolesektoren er det igangsatt samordningsprosjekter som blant annet omfatter HR, saksbehandling og arkiv, samordnet studentopptak og sikkerhetssatsing. Slikt samarbeid kan utfylle det samarbeidet som allerede finnes

innenfor universitets- og høyskolesektoren, men kan også innskrenke institusjonenes handlingsrom i IKT-spørsmål. Arbeidet med å etablere standardiserte arbeidsprosesser og utvikle felles digitale økonomisystemer for sektoren peker i retning av samordning og sterkere sentral styring.

Eksemplene viser at kommuner og statlige virksomheter på flere felt møter et krav om samordning, enten om å ta del i nasjonale fellesløsninger eller å bli del av et felles økonomi- og styringssystem innenfor den enkelte sektoren. Dette trekket ved utviklingen peker i en annen retning enn det statlige kravet om å bruke markedet for å finne digitale løsninger. Det kan dermed ligge en spenning mellom statlig styringsbehov og fritt valg av markedsløsninger som kan gjøre det vanskelig for statlige virksomheter og kommuner å legge en enhetlig sourcingstrategi.

5) Krav om outsourcing og skydrift

Det er liten tvil om at virksomhetene i denne undersøkelsen opplever et krav fra politisk og overordnet myndighet om å etablere skydrift for ulike tjenester. Dette har blitt understreket av myndighetene i flere år gjennom digitaliseringsrundskrivet. Virksomhetene har forsøkt å følge opp dette pålegget. Både i kommunene og i de statlige virksomhetene var det enighet om at der det fantes hyllevare og konkurranse mellom flere leverandører, kunne dette være en god løsning. Microsoft 365 i skyløsning var i bruk i flere virksomheter, og en rekke statlige virksomheter (sykehus, Norges Bank, politiet, Nav og Skatteetaten) er på jakt etter leverandører av skytjenester på ulikt nivå (abc nyheter, 2019).

Når det gjelder lagring av større mengder data, var de fleste virksomhetene litt tilbakeholdne med bruk av kommersielle allmenne skyløsninger. Dels setter gammel infrastruktur og dataprogrammer skranker for dette, dels var det også noen som uttrykte reservasjon når det gjaldt sikkerhet og hvordan sikkerhetsspørsmål i tilfelle skulle håndteres. For flere av virksomhetene var det også et kostnadsspørsmål. Flere virksomheter pekte på at å lagre data i allmenne skyløsninger var dyrt.

Alle virksomhetene hadde egne servere og tilgang på private eller delte skyløsninger, mens Bodø og Oslo hadde satt driften ut til en leverandør. Flere av virksomhetene ga uttrykk for at det var viktig å ha god kontroll på data som var kritisk for kjernevirksomheten, og at egne servere eller privat sky kunne ivareta dette behovet. Det var likevel ingen av virksomhetene som mente det var enkelt å fastslå hvilken type lagring som ga best sikkerhet over tid.

Forsvaret er inne i en prosess der de ønsker å etablere et samarbeid med en leverandør og anskaffe IKT som en tjeneste fra sky i stedet for eller som supplement til egne dataanlegg. Høsten 2019 inngikk Forsvaret en avtale med Microsoft om levering av skytjenester etter at Microsoft dro i land en omfattende avtale med det amerikanske forsvaret (FriFagbevegelse, 2019; IT-avisen, 2019). Microsoft driver en omfattende markedsføring for å få hånd om skytjenestene til forsvars- og etterretningsbyråer og tilbyr hjelp til å forbedre både forsvar og etterretning gjennom bruk av selskapets dataanalyser og maskinlæring (Microsoft, u.d.).

8.3 Skytjenester og virksomhetenes erfaringer

Skytjenestene framstilles som svært attraktive, både av leverandører og i de offentlige dokumentene som staker ut en digital framtid for Norge og rettleder offentlige virksomheter i de valg de må ta. Hvordan opplever virksomhetene påstandene om skytjenestene, og hva er fordeler og ulemper?

- Skytjenester gir tilgang til avanserte programmer.

Ja, mange av programmene som leveres som skytjenester, er attraktive og gode tjenester som virksomhetene gjerne vil ta i bruk. Microsoft 365 er et eksempel på et program mange velger. Virksomhetene opplever imidlertid at skytjenester ofte er kostbare. Det er ikke uvanlig at leverandører av attraktiv programvare leverer rimelige eller gratis versjoner til utdanningsinstitusjoner. Studenter og universiteter drar fordel av dette, men venner seg også til å bruke og etterspørre programvare som kan være svært kostbar for andre virksomheter å skaffe når studentene kommer ut i yrkeslivet.

- Man betaler etter bruk.

Dette er som oftest en sannhet med modifikasjoner. Mange av skytjenestene faktureres som abonnementstjenester, og man betaler for antallet brukere tilknyttet tjenesten, enten de bruker den mye eller lite. Programmer, som tidligere ble kjøpt som en vare med en anskaffelsespris, kunne så brukes uten nye kostnader over flere år. Skytjenester faktureres som oftest fortløpende som et abonnement. Programvare som tidligere ble solgt til kommuner og priset ut fra antallet innbyggere i kommunen, blir som skytjeneste priset ut fra antall brukerkontoer i kommunen, med månedlig eller årlig fakturering. Det kan gjøre det svært kostbart å gjøre programvaren bredt tilgjengelig for kommunalt ansatte som bruker programmet bare periodevis. Betalingsmodellene kan dermed gi høye kostnader, eller nytten av programmene/tjenesten kan reduseres fordi bruken begrenses.

- Det er lett tilgang til skytjenester fra nettleser hvor som helst.

Skytjenester er som oftest lette å ta i bruk og krever i utgangpunktet lite av den enkelte arbeidsstasjonen. De kan nås på nettbrett, pc eller mobiltelefon og lett tilpasses mange brukersituasjoner. Det kan likevel være begrensninger i tilgang og nedlasting av data. En kommune hadde opplevd problemer med å hente ut ekstrakter eller biter av data fra skysystemene, og individuell tilpasning er ikke alltid mulig å få i allmenne skytjenester. Opplasting av data er rimelig og kan også være gratis innenfor visse rammer. Nedlasting av større mengder data har derimot i noen tilfeller vært dyrt og kan også være komplisert å få til.

- Skytjenester kan skaleres opp og ned etter behov.

For noen av virksomhetene i denne undersøkelsen kan skytjenestenes mulighet til å skalere opp og ned tjenesten være en fordel. Nav foretar sine beregninger periodevis, for eksempel hver måned eller hver 14. dag. I stedet for å sitte med egne datamaskiner med regnekraft for å gjennomføre beregningene som fortas bare noen ganger i måneden, kan virksomheten kjøpe dette som skytjeneste og dermed dele utgiftene til regnekapasitet med andre som bruker skytjenesten. Et annet eksempel er utbygging av en tjeneste over tid. En kommune kan for eksempel starte med et prøveprosjekt og så bygge ut etter hvert, uten at kapasitetshensyn påvirker utbyggingen.

Virksomhetene i denne undersøkelsen pekte imidlertid på at det også kunne være utfordringer med opp- og nedskalering av skytjenester. For det første peker en virksomhet på at innkjøpsreglene for offentlige virksomheter kan begrense nytten av skaleringsmulighetene. Anskaffelsesregimet har betydelige omkostninger. Det kan være vanskelig å utforme avtaler med tjenesteleverandører slik at avtalen omfatter framtidig utvikling og oppskalering eller endring, uten at dette utløser krav til ny utlysning av tjenesteleveransen. Dette kan i noen tilfeller hemme og forsinke utviklingen av IKT i offentlig sektor, blir det påpekt.

Muligheten til å skalere tjenesten opp og ned gjør det ikke automatisk enkelt å skifte tjenesteleverandør. Flere virksomheter påpeker at det er lett å komme i en situasjon der man blir låst til en tjenesteleverandør («lock-in»). Det kan i noen tilfeller vise seg vanskelig og kostbart å skifte leverandør og programvare. Det kan være dyrt å gi opplæring og implementere et nytt system, og det kan være vanskelig å få overført data til et nytt system, slik at kontinuitet kan opprettholdes. Dette er ikke unikt for skytjenester, men viser at også disse kan ha sider som utvikler «teknisk gjeld».

- Kontinuerlig oppdatering og utvikling.

I de fleste tilfeller vil det være en stor fordel at skytjenester vanligvis oppdateres og utvikles kontinuerlig. Dette gjøres gjennom små og hyppige endringer. Som bruker er det lett å ta i bruk siste versjon av programmet, og ofte er denne tilgjengelig uten behov for nye kjøp. Men det kan også være en ulempe å dele programvare med andre virksomheter. Både de statlige virksomhetene og kommunene pekte på at de som oftest bare måtte godta standardkontrakter, og dermed mistet innflytelse og mulighet for å tilpasse tjenesten. Offentlige virksomheter kan ha særegne behov som ikke er lagt inn i programvaren, eller krav til et høyere servicenivå enn det de store leverandørene vil gi i sine standardkontrakter.

8.4 Samarbeid og kompetanse

Denne undersøkelsen av fire statlige virksomheter og fire kommuner viser at de offentlige virksomhetene har organisert sin IKT-drift på ulike måter, og at sourcingstrategiene varierer. De fleste virksomhetene har tatt i bruk skytjenester på ett eller flere felt. I noen tilfeller er det få gode alternativer. Skytjenestene har vist seg å være enkle å bruke, og de utvikles ofte sømløst underveis slik at brukeren alltid har siste versjon av tjenesten. De store internasjonale selskapene har ressurser som gjør det mulig å utvikle tjenestene raskt og ivareta høy grad av sikkerhet. Dersom offentlige virksomheter skal etablere og drifte egne systemer i konkurranse med markedet, krever det trolig et utstrakt samarbeid. Noen statlige virksomheter har valgt en slik strategi innenfor spesialiserte områder, for eksempel innenfor høyere utdanning. Et annet eksempel er Meteorologisk institutt, som har valgt å delta i et nordisk samarbeid.

Virksomhetene vurderer sikkerheten ved bruk av skytjenester og lagring i skyen i lys av den type data som skal lagres, og legger stor vekt på at personvernreguleringen (GDPR) følges opp. Her er spørsmålet om hvor data lagres, viktig. Enkelte av informantene ga likevel uttrykk for at det kan være krevende å vurdere sikkerheten ved ulike typer tjenester, og at det kan være ulike synspunkter på hvordan datasikkerhet best ivaretas.

Å besitte tilstrekkelig kompetanse er en forutsetning for å kunne ta gode avgjørelser og kunne opptre som en uavhengig virksomhet. I forbindelse med byggingen av den statlige tyske skytjenesten – Die Bondescloud – bruker tyskerne uttrykket «digital autonomi». Digital autonomi skal sikres ved at staten ikke gjør seg avhengig av store internasjonale selskaper, og gjennom at den

tyske staten selv tar ansvar for å lagre sine data. Bør en nasjonal strategi for digitalisering og sourcing legge vekt på at virksomheter og det offentlige som helhet bør ha digital autonomi?

Det er kanskje et strengt krav, men i en verden som raskt endres gjennom digitalisering, er det verd å ofre spørsmålet en tanke. De fleste virksomhetene i denne undersøkelsen ga uttrykk for at de merket mangelen på kompetanse innenfor IT-teknologi. Det var mulig å få ansatt arbeidstakere, men det kunne være utfordrende å få tak i den ønskede kompetansen. I alle de statlige virksomhetene ble det understreket at det er veldig viktig å ha kompetanse som kjenner til hva virksomheten driver med. For Meteorologisk institutt og Universitetet i Bergen gjorde den begrensede tilgangen på IT-kompetanse at virksomhetene fant det nødvendig å forsøke å utnytte kompetansen best mulig inn mot kjernevirksomheten. Hvis Norge skal ligge langt framme innenfor visse fagområder, er det avgjørende, påpekte virksomhetene, at Norge kan håndtere data selv og foreta kjøringer som er kritiske for virksomhetene. Det genererer kompetanse og kontroll.

Både de statlige virksomhetene og kommunene hadde søkt samarbeid med andre for å styrke kompetansen og nå virksomhetenes mål. For små kommuner er det helt avgjørende. Men også de store aktørene i universitets- og høyskolesektoren har lang erfaring med samarbeid innenfor IKT og har på nasjonalt nivå vært foregangsinstitusjoner i å ta internett i bruk og gjøre det tilgjengelig for offentlig sektor. Men etter hvert som skytjenestene blir mer og mer utbredt, vil basistjenester bli levert automatisk. Mens det tidligere var mye arbeid med å sette opp en pc, installere programvare og foreta oppdateringer, kan alt dette nå gjøres automatisk over nett. Store offentlige virksomheter har kunnet ta ut stordriftsfordeler ved å gjøre dette selv. Den fordelen forsvinner. Utviklingen har imidlertid gjort data verdifulle, slik at eierskap og kontroll over data er blitt det aller viktigste. Det gjør det ekstra viktig for de offentlige virksomhetene å sikre at de har IKT-kompetanse innenfor sin kjernevirksomhet, og mulighet til å utvikle denne. Her kan internasjonalt bransjesamarbeid og nasjonale fellesløsninger bidra til å sikre gode drifts- og utviklingsmiljøer som er uavhengige og en motvekt til de kommersielle tjenestene. I Nederland skrev rektorer ved 14 universiteter under på et åpent brev til avisen *de Volkskrant* i desember 2019 og uttrykte bekymring for at universitetene vil bli avhengige av de internasjonale storselskapene, og at dette kunne underminere forskningens og utdanningens frihet. Rektorene foreslo blant annet å etablere et nasjonalt og europeisk samarbeid for å skape en felles politikk når det gjaldt innkjøp fra kommersielle aktører og håndtering av data. De mente dette var viktig for å sikre utdanning som et fritt tilgjengelig

offentlig gode, og at data generert av det offentlige skulle forbli på offentlige hender (de Volkskrant, 2019).

I Norge har regjeringen lagt til rette for å organisere en offentlig innkjøpsordning eller markedsplass for skytjenester (Difi, 2018). Dette er et skritt på veien for å sikre billigere skytjenester og en felles håndtering av kontraktsmessige sider ved sikkerhet og personvern. Tiltaket har også til hensikt å gjøre det lettere for kommuner med utilstrekkelig kompetanse å gå til anskaffelse av skytjenester (Difi, 2018, s. 8). Ut over dette tiltaket, som beskrives som en markedsplass, har regjeringen ikke lagt til rette for et samarbeid om offentlig datalagring eller etablering av et felles datasenter for statlig eller offentlig sektor, men heller understreket at det offentlige ikke skal opprette egne tjenester dersom disse kan leveres like godt i markedet. 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. Kanskje er det tid for å starte en debatt om dette. I framtiden vil eierskap og kontroll over data legge grunnlag for store verdier. Det vil også være en vei til makt og innflytelse. Derfor er det viktig å drøfte hvordan vi skal regulere disse verdiene, og hvordan vi skal forvalte de verdiene som skapes i det offentlige.

Litteraturliste

abc nyheter. (2019, 12 16). *Nasjonal sikkerhetsmyndighet (NSM) bekymret over Forsvarets IT-planer*. Hentet 03 06, 2020 fra abcnytheter.no: https://www.abcnyheter.no/nyheter/norge/2019/12/16/195634118/nasjonal-sikkerhetsmyndighet-nsm-bekymret-over-forsvarets-it-planer

Agenda Kaupang. (2019). *Smarte byer og kommuner i Norge - en kartlegging*. Kommunal- og moderniseringsdepartementet. Hentet 03 03, 2020 fra https://www.regjeringen.no/contentassets/d6fa05005d5d4ea3a45f62286c2ba2fe/kartlegging_av_smarte_byer.pdf

Arbeids- og velferdsdirektoratet. (2019). *Årsrapport 2018*. Oslo: Arbeids- og velferdsdirektoratet.

Atea. (2017, 01 05). *Pressemelding. Avtale mellom Bodø kommune og Atea endelig undertegnet*. Hentet 01 30, 2020 fra atea.no: https://www.atea.no/om-atea/nyhetsarkiv/pressemeldinger/2017/avtale-mellom-bodo-kommune-og-atea-endelig-undertegnet/

Ball, J. (2019, 11 01). *What's really behind the US's Huawei ban?* Hentet 07 2020 fra newstatesman.com: https://www.newstatesman.com/spotlight-america/cyber/2019/11/whats-really-behind-uss-huawei-ban

Bergen kommune. (2018). *Bergen kommune. Årsmelding 2018*. Bergen kommune. Hentet fra https://www.bergen.kommune.no/politikere-utvalg/api/fil/1727862/Bergen-kommune-Arsmeldingen-2018

Bergen kommune. (u.d.). *Enhet for digitale driftstjenester*. Hentet 01 26, 2020 fra bergen.kommune.no: https://www.bergen.kommune.no/omkommunen/avdelinger/enhet-for-digitale-driftstjenester

Bodø kommune. (2018). *Årsmelding 2018. Interne tjenester*. Hentet 01 30, 2020 fra bodo.kommune.no: https://bodo.kommune.no/interne-tjenester/category2439.html

Bodø kommune. (u.å.). *Digitaliseringsstrategi for Bodø kommune*. Hentet 01 30, 2020 fra bodo.kommune.no: https://bodo.kommune.no/digitaliseringsstrategi/category2388.html

BOTT Universitetssamarbeidet. (u.d.). *Prosjekt: Økonomi og lønn*. Hentet 03 06, 2020 fra bott-samarbeidet.no: https://www.bott-samarbeidet.no/okonomi/

Broadbandsearch. (u.d.). *Mobile Vs. Desktop Usage (Latest 2020 Data)*. Hentet 4 6, 2020 fra broadbandsearch.net: https://www.broadbandsearch.net/blog/mobile-desktop-internet-usage-statistics#post-navigation-0

CICA. (2019, 06 17). *Alert (AA19-168A). Microsoft Operating Systems BlueKeep Vulnerability*. Hentet 02 28, 2020 fra us-cert.gov: https://www.us-cert.gov/ncas/alerts/AA19-168A

Dagens Næringsliv. (15.2.2020). Forsvaret unngikk kryptoutstyret Kongsberg solgte til andre. *Dagens Næringsliv*.

Datatilsynet. (2018, 6 23). *Skytjenester*. Hentet 02 28, 2020 fra datatilsynet.no: https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/skytjenester/

de Volkskrant. (2019, 12 22). *Digitalisering bedreigt onze universiteit. Het is tijd om een grens te trekken*. Hentet 03 08, 2020 fra de Volkskrant: https://www.volkskrant.nl/columns-opinie/digitalisering-bedreigt-onze-universiteit-het-is-tijd-om-een-grens-te-trekken~bff87dc9/

Departementene. (2019). *Tiltaksoversikt til nasjonal strategi for digital sikkerhet.* Oslo: Departementenes sikkerhets- og servicorganisasjon.

Difi. (2018). *Innkjøpsordning/markedsplass for skytjenester. Forprosjekt.* Oslo: Direktoratet for forvaltning og ikt. Hentet 12 17, 2019 fra https://www.difi.no/sites/difino/files/innkjopsordning-markedsplass-for-skytjenester-difi-rapport-2018-6.pdf

Digitaliserngsdirektoratet. (2015). *Veileder i kompetanse- og kulturutvikling innen informasjonssikkerhet. Hvorfor*, Sist endret 3.7.2019. Hentet 02 29, 2020 fra difi.no: https://www.difi.no/fagomrader-og-tjenester/informasjonssikkerhet/veiledere/kompetanse-og-kulturutvikling/hvorfor

Direktoratet for e-helse. (2020, 07 03). *Akson – felles kommunal journal og helhetlig samhandling.* Hentet 07 2020 fra ehelse.no: https://ehelse.no/strategi/akson

Direktoratet for e-helse. (u.å.). *Akson*. Hentet 08 05, 2020 fra ehelse.no: https://ehelse.no/tema/Akson

Direktoratet for e-helse. (u.å.). *Nasjonale kunnskapsbehov på e-helseområdet.* Oslo: Direktoratet for e-helse. Hentet 01 29, 2020 fra https://ehelse.no/publikasjoner/nasjonale-kunnskapsbehov-pa-e-helseomradet

eSam. (20.9.2019). Kompletterande information om. *PM*. Sverige. Hentet 3 1, 2020 fra http://www.esamverka.se/download/18.4c1250a116d1bb3a3f094fe1/1568977769756/Kompletterande%20information%20om%20molnfr%C3%A5gan%202019-09.pdf

eSam. (23.10. 2018). Rättsligt uttalande om röjande och molntjänster. *Rättsligt uttalande VER 2018:57*. Sverige. Hentet 3 1, 2020 fra http://www.esamverka.se/download/18.290a0225166bfafb714c0c7a/1542007824143/eSam%20-%20Ra%CC%88ttsligt%20uttalande%20om%20ro%CC%88jande%20och%20molntj%C3%A4nster.pdf

Evry. (u.d.). *Mulighetene er uendelige i en skybasert verden*. Hentet 02 27, 2020 fra every.com: https://www.evry.com/no/jobbe-sammen/tjenester/sky-og-infrastruktur/?gclid=CjwKCAiA7t3yBRADEiwA4GFlI1oorJT3AjOhpbxhwkD6eJXjnEW7PrA8VVCBW1ZwjrPQz7DsjIcl1xoC8CAQAvD_BwE

Forsvaret. (2017, 09 19). *Forsvarsmateriell tar form*. Hentet 08 04, 2017 fra forsvaret.no: https://forsvaret.no/aktuelt/forsvarsmateriell-tar-form

Forsvaret. (u.å.). *Organisasjon*. Hentet 07 29, 2020 fra Forsvaret.no: https://forsvaret.no/fakta/organisasjon

Forsvarsdepartementet. (2019). *IKT-strategi for forsvarssektoren. Hoveddokument.* Oslo: Forsvarsdepartementet. Hentet fra https://www.regjeringen.no/contentassets/5818cac9676c45bba69b46f610816267/ikt-strategi-for-forsvarssektoren---hoveddokument.pdf

Fri Fagbevegelse. (11.2.2020). *Nå får tyskerne sin egen skytjeneste for lagring av all offentlig informasjon*. Hentet 2 17, 2020 fra frifagvevegelse.no: https://frifagbevegelse.no/ntlmagasinet/na-far-tyskerne-sin-egen-skytjeneste-for-lagring-av-all-offentlig-informasjon-6.158.678855.cdeb734c7a

FriFagbevegelse. (2019, 11 22). *Forsvaret er på vei over i en datasky levert av Microsoft. Det gjør de ansatte veldig urolige*. Hentet 03 06, 2020 fra frifagbevegelse.no: https://frifagbevegelse.no/forside/forsvaret-er-pa-vei-over-i-en-datasky-levert-av-microsoft-det-gjor-de-ansatte-veldig-urolige-6.158.662694.651ffdc7b8

Gartner. (2020, January 16). *Use Third-Party Solutions to Fill Backup and Data Recovery Gaps in Office 365*. Hentet fra gartner.com: https://www.gartner.com/en/documents/3839166/use-third-party-solutions-to-fill-backup-and-data-recove

Høyesterett. (2019). HR-2019-610-A Tidal Music AS mot Påtalemyndigheten. *lovdata.no*.

Internet Word Stats. (2020). *Internet usage statistics - Mid-Year 2019*. Hentet 02 26, 2020 fra internetworldstats.com: https://www.internetworldstats.com/stats.htm

IT-avisen. (2019, 10 26). *Microsoft vant skykontrakt verdt 91 milliarder kroner*. Hentet 03 06, 2020 fra itavisen.no: https://itavisen.no/2019/10/26/microsoft-vant-skykontrakt-verdt-91-milliarder-kroner/

Kommunal- og moderniseringsdepartementet. (2016). *Najonal strategi for bruk av skytjenester.* Oslo: Kommunal- og moderniseringsdepartementet.

Kommunal- og moderniseringsdepartementet. (2019, 12 20). *Digitaliseringsrundskrivet*. Hentet 02 06, 2020 fra regjeringen.no: https://www.regjeringen.no/no/dokumenter/digitaliseringsrundskrivet/id2683652/

Kommunal- og moderniseringsdepartementet. (2019, 12 20). *Digitaliseringsrundskrivet, nr. H-5/19*. Hentet 01 29, 2020 fra Regjeringen.no: https://www.regjeringen.no/no/dokumenter/digitaliseringsrundskrivet/id2683652/

Kommunal- og moderniseringsdepartementet. (2019). *Én digital offentlig sektor. Digitaliseringsstrategi for offentlig sektor 2019–2025*. Oslo: Kommunal- og moderniseringsdepartementet.

Kommunal- og moderniseringsdepartementet. (2020, 03 3). *Oppretter ekspertgruppe for datadeling i næringslivet*. Hentet 02 10, 2020 fra regjeringen.no: https://www.regjeringen.no/no/aktuelt/oppretter-ekspertgruppe-for-datadeling-i-naringslivet/id2688682/?utm_source=www.regjeringen.no&utm_medium=epost&utm_campaign=nyhetsvarsel%20Veke%207&utm_content=Statlig%20forvaltning

Kunnskapsdepartementet. (2017). *Digitaliseringsstrategi for universitets- og høyskolesektoren 2017-2021*. Oslo: Kunnskapsdepartementet. Hentet fra regjeringen.no: https://www.regjeringen.no/contentassets/779c0783ffee461b88451b9ab71d5f51/no/pdfs/digitaliseringsstrategi-for-universitets--og-hoysk.pdf

Letouzey, J.-L., & Whelan, D. (2019, 12 23). *Introduction to the Technical Debt Concept*. Hentet fra agilealliance.org: https://www.agilealliance.org/wp-content/uploads/2016/05/IntroductiontotheTechnicalDebtConcept-V-02.pdf

Meld. St. 27 (2015–2016). (u.d.). Digital agenda for Norge. Norge: Kommunal- og moderniseringsdepartementet.

Meld. St. 27. (2015–2016). Digital agenda for Norge. IKT for en enklere hverdag og økt produktivitet.

Meteorologisk institutt. (2018). *Strategisk plan 2019 – 2021. Vi sikrer liv og verdier, med tjenester i verdensklasse.* Oslo: Meteorologisk institutt. Hentet fra https://www.met.no/om-oss/_/attachment/inline/99f52f7b-33b4-40a5-a41e-c28d56589e26:3cfe9315bc30512ed49f51ab9e1f286b665d8264/Strategisk%20plan%202019-2021.pdf

Meteorologisk institutt. (2019). *Sourcingstrategi - IT-området 2019–2021.* Oslo: Meteorologisk institutt.

Meteorologisk institutt. (2020, 01 02). *MetCoOp*. Hentet fra met.no: https://www.met.no/en/projects/metcoop

Microsoft. (2017). Microsoft Cyber Defense Operations Center. Strategy brief. Microsoft Corporation. Hentet 3 2, 2020 fra https://www.microsoft.com/nb-no/security/business/operations?market=no

Microsoft. (u.d.). *Hjelp forsvars- og etterretningsbyråer å fremme en tryggere verden*. Hentet 03 06, 2020 fra microsoft.com: https://www.microsoft.com/nb-no/industry/government/defense-and-intelligence

Nasjonal sikkerhetsmyndighet. (2018). *NSMs grunnprinsipper for IKT-sikkerhet, versjon 1.1.* Sandvika: Nasjonal sikkerhetsmyndighet. Hentet 02 28, 2020 fra https://www.nsm.stat.no/globalassets/dokumenter/nsm_grunnprinsipper_for_ikt-2018.pdf

Nasjonal sikkerhetsmyndighet. (2020, 01 14). *NSM oppfordrer til rask oppdatering av Microsoft Windows*. Hentet fra nsm.stat.no: https://www.nsm.stat.no/aktuelt/nsm-oppfordrer-til-rask-oppdatering-av-microsoft-windows/

New York Times. (24.10.2018). *When Trump Phones Friends*. Hentet 02 29, 2020 fra nytimes.com: https://www.nytimes.com/2018/10/24/us/politics/trump-phone-security.html?fallback=0&recId=1C3gl9VHzJELvNvi441GAB3MGZo&locked=0&geoContinent=EU&geoRegion=02&recAlloc=most_popular&geoCountry=NO&blockId=most-popular&imp_id=827967306&action=click&module=Most%

Nexia International. (2015). *Kartlegging og analyse av landskapet for offentlige dtasentre i norge 2015. Utarbeidet for Kommunal- og moderniseringsdepartementet.* Oslo: Nexia International. Hentet 02 27, 2020 fra https://www.regjeringen.no/contentassets/2c6b31ece2504399bb23ca5e83b9b6ed/nexia_off_datasentre.pdf

NSC. (2020, 01 02). *About NSC*. Hentet fra nsc.liu.se: https://www.nsc.liu.se/about/

Oslo kommune. (2019, 09 20). *Oppgradering av kommunens største arbeidsflate*. Hentet 12 16, 2019 fra https://nyhetsbrev.ukeoslo.no/: https://nyhetsbrev.ukeoslo.no/ny-citrix-versjon/

Oslo Kommune. (u.å.). *Ansatte i Oslo kommune*. Hentet 02 03, 2020 fra https://www.oslo.kommune.no/: https://www.oslo.kommune.no/statistikk/kommunal-okonomi-og-forvaltning/ansatte-i-oslo-kommune/

Oslo kommune. (u.å.). *Utviklings- og kompetanseetaten*. Hentet 02 27, 2020 fra oslo.kommune.no: https://www.oslo.kommune.no/etater-foretak-og-ombud/utviklings-og-kompetanseetaten/

Petrov, C. (2019, 3 22). *Big Data Statistics 2020*. Hentet 4 7, 2020 fra techjury.net: https://techjury.net/stats-about/big-data-statistics/

Punke, M. (29.5.2019). Oppklaring rundt AWS og Cloud act. *digi.no*. Hentet 2 6, 2020 fra https://www.digi.no/artikler/kommentar-oppklaring-rundt-aws-og-cloud-act/463582

Ringnes, I. F. (2018, 10 16). *Infotrygd 40 år: Fortsatt lenge igjen til pensjonering*. Hentet January 17, 2020 fra memu.no: https://memu.no/artikler/infotrygd-40-ar-fortsatt-lenge-igjen-til-pensjonering/

Room, S. (2020, 07 16). *Europe's Top Court Collapses The Privacy Shield In Facebook Data Transfer Case.* Hentet 07 2020 fra forbes.com: https://www.forbes.com/sites/stewartroom/2020/07/16/europes-top-court-collapses-the-privacy-shield-in-facebook-data-transfer-case/#1e0e02dd2a1c

Stach, Heike. (2020). *Data storage as a federal responsibility – The Bundescloud. eForvaltningskonferansen 2020*. Hentet fra youtube.com: https://www.youtube.com/watch?v=hzx2MIRQYBs

Statistisk sentralbyrå. (u.d.). *Fakta om internett og mobil*. Hentet 4 7, 2020 fra ssb.no: https://www.ssb.no/teknologi-og-innovasjon/faktaside/internett-og-mobil

The Globe and Mail. (11.10.2018). *U.S. senators urge Trudeau to block Huawei from 5G*. Hentet 02 29, 2020 fra theglobeandmail.com: https://www.theglobeandmail.com/politics/article-us-senators-urge-trudeau-to-block-huawei-from-5g/

The Guardian. (u.d.). *The Cambridge Analytica Files*. Hentet 3 2, 2020 fra theguardian.com: https://www.theguardian.com/news/series/cambridge-analytica-files

U.S. Department of Justice. (2019). Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act. *White Paper*. Hentet 3 1, 2020 fra https://www.justice.gov/opa/press-release/file/1153446/download?utm_medium=email&utm_a=govdelivery

Unit. (2019). *Handlingsplan for digitalisering i høyere utdanning og forskning 2019-2021*. Hentet januar 16, 2020 fra unit.no: https://www.unit.no/sites/default/files/media/filer/2019/10/Handlingsplan-digitalisering-2019.pdf

Unit. (2020, 01 15). *Units vedtekter, sist endret 30.9.2019*. Hentet fra unit.no: https://www.unit.no/units-vedtekter

Universitetet i Bergen. (u.å.). Kapasitet, kvalitet, kostnad og samfunnsansvar. Sourcingstrategi 2019-2022. Universitetet i Bergen.

Visma blogg. (2020, 05 13). *Øystein Moan: ERP i skyen aldri vært viktigere.* Hentet 05 22, 2020 fra https://www.visma.no/blogg/digitaliseringen-ma-motes-med-omstillingsvilje/

Washington Post. (11.2.2020). *National Security 'The intelligence coup of the century'. For decades, the CIA read the encrypted communications of allies and adversaries*. Hentet 2 29, 2020 fra washingtonpost.com: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

Watts, S., & Raza, M. (2019, 6 15). *SaaS vs PaaS vs IaaS: What's The Difference and How To Choose*. Hentet 4 7, 2020 fra bmc.com: https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

Wikipedia. (u.d.). *Cloud computing*. Hentet 4 7, 2020 fra https://en.wikipedia.org/wiki/Cloud_computing

yr.no. (2020, 01 02). *A new way to check the weather*. Hentet fra hjelp.yr.no: https://hjelp.yr.no/hc/en-us/articles/115005341865-A-new-way-to-check-the-weather

Sourcingstrategier for IKT i offentlig sektor

Denne rapporten handler om sourcingstrategier for IKT og bruk av skytjenester i offentlig sektor i Norge. Undersøkelsen bygger blant annet på intervjuer i fire statlige virksomheter og fire kommuner. 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. Hvilke vurderinger og veivalg gjør virksomhetene i offentlig sektor? De reiser blant annet spørsmål om sikkerhet, framtidig avhengighet av leverandører og tjenestenes tilpasning til offentlig sektor. Med et sideblikk til Tyskland, hvor staten har valgt ikke å ta i bruk allmenne skytjenester, men vil bygge opp en egen statlig skytjeneste, stiller rapporten spørsmål om det også i Norge bør tas en offentlig diskusjon om sikkerhet og digital autonomi.

Fafo

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

Fafo-rapport 2020:17
ID-nr.: 20752