DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering:

Master i samfunnssikkerhet

Vårsemesteret, 2022
Åpen / ~~Konfidensiell~~

Forfatter:
Sofie Sagedahl Høydal

Sofie Sagedahl Høydal
.....
(signatur forfatter)

Fagansvarlig: Ole Andreas Hegland Engen

Veileder(e): Kenneth Arne Pettersen Gould

Tittel på masteroppgaven: En sky av usikkerhet – en case-studie av datasuverenitet i en norsk kommunes arbeid med skytjenester

Engelsk tittel: A cloud of uncertainty – a case study of data sovereignty in one Norwegian municipality's work with cloud computing

Studiepoeng: 30

Emneord:
Suverenitet, datasuverenitet, skytjenester, offentlig sektor, kommune, datalagring

Sidetall: 92

+ vedlegg/annet: 118

Stavanger, 13.juni 2022
dato/år

En sky av usikkerhet

En case-studie av datasuverenitet i en norsk kommunes arbeid med skytjenester

Microsoft Word stock photos

Masterstudium i samfunnssikkerhet

Universitetet i Stavanger

Juni 2022

Sofie Sagedahl Høydal

Forord

Denne oppgaven markerer slutten på mine to år som masterstudent i samfunnssikkerhet ved UiS.

Temaet datasuverenitet kom jeg over ved en tilfeldighet i desember 2021. Jeg var på leting etter et masteroppgavetema som både ville inkluderte teknologi, og som ville være relevant å undersøke i det offentlige Norge, som jeg interesserer meg svært mye for. Jeg oppdaget fort at datasuverenitet som tema trengte mer forskning, spesielt i norsk kontekst. Jeg har derfor utfordret meg selv til å skrive om et tema og felt som jeg før oppgavens start visste tilnærmet ingenting om. Det har vært utfordrende, men på den andre siden utrolig givende, å utforske et tema som er svært dagsaktuelt og etter min mening burde blitt fokusert mer på.

Takk til alle som har bidratt, både privat og faglig, til at denne oppgaven ble til. I forbindelse med denne oppgaven har jeg vært i kontakt med mange personer som har gitt meg innspill og bedre forståelse for datasuverenitet og skytjenester som felt, og dyktige og engasjerte informanter som har gitt verdifulle innspill til oppgaven.

Spesielt takk til min veileder, Kenneth Arne Pettersen Gould, som har utfordret meg til å se det store bildet, og veiledet på en måte som har gitt meg stort eierskap til egen oppgave.

Sofie Sagedahl Høydal

Stavanger, 13. juni 2022.

Sammendrag

Utviklingen av skytjenester har ført til at måten data blir flyttet, behandlet og lagret på, nå går på tvers av landegrenser i større grad enn med tradisjonell datalagring. Dette medfører nye utfordringer for de som er ansvarlige for at dataen holdes sikker. Etter hvert som dataen krysser landegrenser, oppstår også en ny utfordring med å vite hvilken jurisdiksjon dataen ligger under, og hvordan dette påvirker sikkerhet. Norske kommuner lagrer store mengder betydningsfull data, og har i stor grad tatt i bruk skytjenester.

I denne oppgaven undersøkes ivaretakelse av datasuverenitet i en kommunes arbeid med skytjenester, og hvilke utfordringer som eksisterer i dette arbeidet. Formålet med oppgaven er å se på en utvalgt kommunes arbeid med skytjenester, hvordan dette arbeidet ivaretar karakteristikker for datasuverenitet, og hvilke utfordringer arbeidet møter på.

For å besvare oppgaven undersøker jeg organisering av, og arbeid med, skytjenester i kommunen. Dette gjøres gjennom å studere offentlige dokumenter og dybdeintervju om skytjenester med informanter fra kommunen, en rådgivende organisasjon og en markedsaktør.

Oppgaven baseres på utarbeiding av et teoretisk rammeverk om datasuverenitet, ettersom det ikke eksisterer et allment akseptert rammeverk. Gjennom å identifisere karakteristikker for datasuverenitet i kommunens arbeid med skytjenester, drøftes det hvordan disse karakteristikkene ivaretas og hvilke utfordringer kommunen møter på i dette arbeidet.

Undersøkelsen av hvordan kommunen ivaretar datasuverenitet i sitt arbeid med skytjenester viser at det er store variasjoner i hvordan arbeidet blir strukturert og fulgt opp i kommunen, som påvirker ivaretakelse av datasuverenitet. Det er avdekket at det er mer fokus på relevante karakteristikker av datasuverenitet når dataen som skal lagres oppfattes som persondata og er underlagt GDPR.

De største identifiserte utfordringene for ivaretakelse av datasuverenitet i kommunens arbeid med skytjenester er knyttet til mangel på gjennomføring av dataklassifisering, for lite kompetanse om hvordan skytjenesters IT-arkitektur bør tilpasses data og ønsket sikkerhetsnivå, mangel på relevante rutiner for anskaffelser og oppfølging av skytjenester, og kjennskap til disse rutinene, og ikke minst for få ressurser til avtaleforvaltning. Som følge av disse utfordringene er ivaretakelse av datasuverenitet i kommunens arbeid med skytjenester preget av tilfeldigheter og sterk avhengig av leverandørens egne initiativ.

INNHOLD

TABELL OG FIGUROVERSIKT

Figuroversikt

Tabelloversikt

1. Innledning

I 2020 ga Nasjonal sikkerhetsmyndighet ut rapporten «Sikkerhetsfaglige anbefalinger ved bruk av tjenesteutsetting og skytjenester», der det påpekes at en av de mest betydningsfulle trendene innenfor digitalisering er tjenesteutsetting, blant annet bruk av skytjenester (Nasjonal sikkerhetsmyndighet, 2020c, s. 7). De siste tiårenes vekst i skytjenester har ført til at både private og offentlige virksomheter i økende grad har gått fra å ha egne servere, operativsystem eller programvarer, til å gå over til skytjenester (Seip, 2020, s. 21). I 2018 benyttet hele 85,4 % av de norske kommunene seg av skytjenester for datalagring (Statistisk sentralbyrå, 2019, s. 3).

Digitaliseringen og den økte bruken av skytjenester har ført til at digitale verdikjeder i større grad krysser landegrenser, og på denne måten utfordres nasjonale myndigheters kontroll ved at det er etablert gjensidige avhengighetsforhold på tvers av landegrenser (Departementene, 2019, s. 9). Fordi data krysser nasjonale landegrenser utfordres også det tradisjonelle suverenitetsbegrepet tilknyttet landterritorier, og det blir vanskeligere å fastsette hvem som faktisk er ansvarlig for, eier og skal ha tilgang til data. Denne tvetydeligheten vil også påvirke virksomheter som lagrer data i sky, slik som norske kommuner.

Usikkerheten rundt eierskap og overføring av data ble fokuset i Schrems II-dommen fra 2020, der EU-domstolen avsa en prinsipiell dom som omhandlet overføring av personopplysninger ut fra EU og EØS (Digdir, u.å.). Dommen omhandlet personvernaktivisten Max Schrems fra Østerrike, som klaget til det irske datatilsynet. Schrems mente at personopplysningene hans ikke var godt nok beskyttet i USA, etter at Facebook Irland informasjonen til Facebook Inc USA. For å overføre personopplysninger utenfor EU/EØS trengs det et overføringsgrunnlag som samsvarer med GDPR-bestemmelsene. Kjernen for dommen var at den amerikanske lovgivningen gir amerikanske myndigheter svært vide hjemler for behandling av personopplysninger samt overvåkning, på en måte som er i strid med det europeiske personvernregelverket fastsatt i GDPR. Dommen kom frem til at overføringsgrunnlaget brukt i Facebook Inc var i strid med kravene til tilstrekkelig beskyttelsesnivå fra GDPR. Dommen førte til at «Privacy Shield», en sertifiseringsordning for virksomheter i USA i samarbeid med EU og USA som ble brukt som overføringsgrunnlag, ikke lenger var gyldig (Digdir, u.å.).

Til tross for at dommen satt fokus på rettigheter til dataens tilhørighet og eierskap, og er omtalt og diskutert i Norge, er det fremdeles lite fokus på datasuverenitet i offentlig diskurs.

Datasuverenitet handler svært forenklet om kontroll over og rettigheter til egne data, også data som ikke er persondata eller sensitive data, uavhengig av plassering. Det mangler fremdeles et helhetlig rammeverk, og den forskningen som eksisterer er i stor grad basert på enkle definisjoner. Enighet om hva datasuverenitet som fenomen bør og skal innebære er ikke etablert. Litteraturen som eksisterer på nåværende tidspunkt er derfor svært fragmentert, og er i stor grad begrenset til korte definisjoner som er vanskelig å skille fra liknende sikkerhetsbegrep som informasjonssikkerhet og cybersikkerhet.

Datasuverenitet vil være betydningsfullt for norske kommuner, ettersom de drifter en enorm mengde tjenester og systemer, og dermed er avhengige av å lagre store mengder data. Informasjonssikkerhet, personvern og digital beredskap er en forutsetning for at kommunene skal kunne drive gode innbyggertjenester (KS, u.å). Overgangen til skytjenester knyttes til positive faktorer som reduserte kostnader og økt tilgang til kompetanse (Departementene, 2019, s. 6), men kan også ha fått betydning for hvilken kompetanse det offentlige trenger for å ta beslutninger om IKT-sikkerhet, samt kostnader forbundet med løsningene som er tilgjengelig (Seip, 2020, s. 21). Det offentlige er ofte avhengige av private aktører i offentlig-privat samarbeid når det kommer til utvikling av digitale tjenester og produkter som skytjenester. Derimot fører skytjenester, på grunn av digital lagring og forflytning over grenser, med seg en ny type problematikk: hvor dataen faktisk befinner seg, hvem som har tilgang til den, og hvilken lovgivning den faller under. Det kan dermed være mer uklart hvem som har kontroll over og makt over dataen, og hvilke plikter eierskap over data medfører.

2. Problemstilling og avgrensning

Med bakgrunn i den teknologiske og juridiske utviklingen som har skjedd de siste årene, ønsker jeg å undersøke hvordan skytjenester påvirker datasuverenitet i en norsk kommune. Skytjenester som teknologi er spesielt interessant, fordi de potensielt kan være svært kostnadsbesparende sammenliknet med lokal lagring og intern drift, samtidig som lagringen kan påvirket av lovgivning i flere land fordi den spres over flere datasentre etter kapasitet.

Fordi datasuverenitet er et begrep uten enighet om innhold og forståelse, vil det benyttes underliggende karakteristikker ved begrepet for å undersøke tilstanden i kommunen.

Formålet med studien er derfor å undersøke hvordan én utvalgt kommune, arbeider med anskaffelse og bruk av skytjenester, og om dette arbeidet ivaretar karakteristikker for datasuverenitet for digitale data i kommunen, samt hvilke utfordringer arbeidet møter på. Det er dermed ikke nødvendigvis det tekniske innholdet i en skytjeneste som er interessant for

oppgaven, men heller hvordan de ulike informantene arbeider med og forholder seg til skytjenester gjennom ulike virkemidler og prosesser.

Følgende problemstilling danner grunnlaget for studien:

Hvordan ivaretas karakteristikker for datasuverenitet i en norsk kommunes arbeid med skylagring, og hva er de sentrale utfordringene i dette arbeidet?

For å besvare problemstillingen er de følgende to forskningsspørsmålene utarbeidet:
Forskningsspørsmål 1: *Hvordan er arbeidet med skytjenester organisert i kommunen, og hvilke faktorer vektlegges i dette arbeidet?*

Forskningsspørsmålet søker å beskrive hvordan kommunen organiserer sitt arbeid med anskaffelse og bruk av skytjenester, samt om det er likhet i forståelsen av hvordan dette arbeidet skal gjøres på tvers av aktører og avdelinger. Systemperspektivet blir fremtredende ved at det kan undersøkes om organiseringen fremmer en helhetlig oversikt over arbeidet, eller om det arbeides i siloer og mangler oversikt.

Forskningsspørsmålet søker også å undersøke hvilke faktorer som vektlegges i dette arbeidet, for å få et innblikk i om for eksempel karakteristikker for datasuverenitet eller øvrige faktorer som et systems funksjonalitet vektlegges i dette arbeidet.

Forskningsspørsmålet er beskrivende, og knyttes til det empiriske arbeidet som må gjøres for å svare på problemstillingen i diskusjonen. Med dette forskningsspørsmålet søker jeg dermed å danne en grunnleggende forståelse som kan brukes for å knytte empirien opp mot teorien i diskusjonen, og det vil således besvares i gjennomgang av empirien alene.

Forskningsspørsmål 2: *Hvilke karakteristikker for datasuverenitet kan identifiseres i kommunens arbeid med skytjenester?*

Dette andre forskningsspørsmålet søker å identifisere hvilke karakteristikker for datasuverenitet som er, og dermed ikke er, til stede i kommunenes arbeid med skytjenester.

Sammenlagt vil disse to forskningsspørsmålene søke å besvare problemstillingen i sin helhet, ved å se på hvordan organiseringen av skytjenester, og også de identifiserte karakteristikkene, eller mangler derav, påvirker datasuverenitet i kommunen.

2.1 Avgrensning

Datasuverenitet kan i stor grad tilknyttet nasjonalstater, og nasjonal sikkerhet, gjennom statenes generelle suverenitet. Nasjonalstater, og andre territoriale fellesskap, slik som EU, vil

igjen kunne påvirke datasuverenitet via lovverket som etableres og setter ramme for digitalisering og datalagring. I denne oppgaven vil det ikke være fokus på datasuverenitet i nasjonal forstand, men avgrenses til kommunene. Kommunene kan knyttes til datasuverenitet, fordi de er statens utøvende ledd. Hva kommunene gjør, vil kunne få følger for den nasjonale suvereniteten, men det er også interessant å undersøke datasuverenitet i kommunene i seg selv.

Datasuverenitet i norske kommuner er interessant å undersøke som et isolert fenomen, fordi kommunene produserer og behandler store mengder data både om innbyggerne og kommunen som virksomhet, og er leverandører av kritisk infrastruktur og tjenester som forvaltes via digitale løsninger slik som skytjenester. Disse løsningene kan påvirke datasuverenitet, som både vil påvirke kommunen som virksomhet, og dens innbyggere.

I denne oppgaven vil jeg derfor undersøke datasuvereniteten i den utvalgte kommunen, men det vil ikke være fokus på hvordan ulik grad av datasuverenitet i kommunen, kan påvirke den nasjonale suvereniteten og derfor nasjonal sikkerhet.

Oppgaven vil også begrenses til å identifisere karakteristikker for datasuverenitet og hvordan disse ivaretas i kommunen, samt hvilke utfordringer kommunen møter i dette arbeidet. Oppgaven vil derimot ikke vurdere i hvilken grad datasuvereniteten i kommunen er god eller dårlig. Fordi det ikke eksisterer et rammeverk for datasuverenitet, og dette er utviklet i oppgaven, er det også er mangler på metoder eller kriterier for å måle datasuverenitet. Karakteristikkene og underkarakteristikkene kan identifiseres, men med bakgrunn i den eksisterende litteraturen er det vanskelig å måle grad av datasuverenitet. Det kan derimot pekes på mangler av eller tilstedeværelse av karakteristikkene, og hvordan endring av arbeid med datasuverenitet kunne påvirket tilstedeværelse av disse.

3. Kontekst

Før datasuverenitet som begrep og fenomen gjennomgås, er det nødvendig med en gjennomgang av bakgrunnsfaktorer som får betydning for skylagring og datasuverenitet. Det følgende kapittelet vil derfor danne et bakteppe for resten av oppgaven, ved å se på verdien i digitale data, ulike metoder for datalagring, hva skytjenester er og lovverk som berører datalagring i kommunen.

3.1 Hva er digitale data, og hvorfor har de verdi?

Essensielt for datasuverenitet, er det faktum at det er snakk om digitale data. Data tilknyttet individer, bedrifter eller offentlig sektor utgjør store verdier for samfunnet. Eierskap og forvaltning av data er derfor viktig, både om det er snakk om persondata eller andre data (Skogli et al., 2019, s. 3).

Fra et økonomisk perspektiv kan en peke på at data har tre hovedegenskaper, som er tett sammenvevde: 1) data er et ikke-rivaliserende gode, som betyr at dataen kan gjenbrukes uten at verdien synker, men som også kan bety at det er vanskelig å avklare rettighetene til dataen, 2) data kan generere positive eksternaliteter, som viser til at dataens verdi kan bli større av å sammenkobles med andre data, og dermed ha mer verdi for samfunnet enn den som søker å kontrollere dataen, 3) storskalafordeler som kommer av anvendelse av data, eksempelvis fordelene som medfølger av å slå sammen datasett i større datasett (Skogli et al., 2019, s. 5).

Samtidig som den norske regjeringen oppfordrer til økt deling av åpne data for å styrke næringslivet, spesifiserer de også at de vil:

> […] legge til rette for ansvarlig dataøkonomi i Norge, og arbeide for at bruken av data skjer på en rettferdig, etisk og ansvarlig måte. Sikkerheten og personvernet må ivaretas. Forbrukernes rettigheter må sikres, og det må legges til rette for rettferdige konkurranseregler for norske og internasjonale aktører. Kunstig intelligens og stordataanalyse kan bidra til at tjenester blir bedre tilpasset den enkelte. Samtidig er det viktig å forhindre diskriminering, manipulasjon av informasjon og misbruk av informasjon. Åpenhet, likebehandling og rettssikkerhet er viktige demokratiske verdier som også må gjelde i dataøkonomien. (Meld. St. 22 (2020–2021), s. 6).

Stortingsmeldingen viser til at fordi data har verdi, må det også finnes tiltak som kan kontrollere og beskytte tilgang til data, selv om deling av data kan være fordelaktig for dataøkonomien. Store mengder av denne dataen behandles i skytjenester, og for mange virksomheter er bruken av skytjenester en forutsetning for at verdien i dataen skal kunne utnyttes til det fulle, fordi tjenestene muliggjør bruk av ressurser som ikke er tilgjengelig lokalt (Meld. St. 22 (2020–2021), s. 9).

3.2 Datalagring – fra lokale servere til skyen

Globalisering og den digitale utviklingen har fått betydning for handel av tjenester. Der handel av varer har vært betydningsfullt i mange år, er det et nyere fenomen at handel med tjeneste øker betydningsfullt i volum (Seip, 2020, s. 32). Fordi salget at disse tjenestene skjer over nett, kan ulike deler av verdikjeden befinne seg på tvers av landegrenser. Virksomheten kan befinne seg ett sted mens datasenteret er et annet sted. Dette har ført til en endring i både markedet, reguleringer og ikke minst mulighetene for kontroll (Seip, 2020, s. 32).

Tradisjonelt sett har data, også i kommunene, blitt lagret lokalt på lokale servere, såkalt on-premise. On-premise datalagring innebærer at alt fra servere til software, infrastruktur og arbeidskraft for vedlikehold befinner seg lokalt (Boillat & Legner, 2013). Denne formen for datalagring baserer seg dermed på handel av varer, det vil si både det tekniske utstyret som trengs for å bygge opp det lokale tilbudet, og løsningen som er ønsket. On-premise løsninger krever at brukeren installerer og driver tjenesten fra eget lokalt IT-miljø (Boillat & Legner, 2013, s. 41).

3.2.1 Skytjenester – definisjon, tjenestemodeller og leveransemodeller

Skytjenester har vokst frem som et alternativ til å drifte eget system på lokale servere og infrastruktur. Moderne skytjenester ble introdusert tidlig på 2000-tallet av Amazon, tett fulgt opp av Google og Microsoft, som alle tre fremdeles er blant de største skytjenesteleverandørene (Seip, 2020, s. 28-29). I 2019 kunne SSB vise til at «samtlige kommuner med mer enn 30.000 innbyggere benyttet en eller flere nettskytjenester» mens de mindre kommunene med færre enn 5.000 innbyggere hadde en prosentvis bruk på 75,4 prosent (Statistisk sentralbyrå, 2019).

Skytjenester defineres av den norske regjeringen etter definisjonen av den amerikanske standardiseringsorganisasjonens NIST (National Institute of Standards and Technology). NIST viser til at skytjenester har en rekke kjennetegn: de er behovsbaserte, de leveres over nett, leverandøren kan fordele sine dataressurser mellom ulike kunder etter behov, det er rask fleksibilitet for å skalere tjenestene, og betalingen skjer etter faktisk bruk (Mell & Grance, 2011, s. 2).

Skytjenester kan videre deles inn i tre ulike typer tjenestemodeller, og fire typer leveransemodeller. Tjenestemodellene deles inn i 1) programvare som tjeneste (SaaS), 2) plattform som tjeneste (PaaS) og 3) Infrastruktur som tjeneste (IaaS) (Mell & Grance, 2011, s. 2-3). Leveransemodellene deles inn i 1) allmenn sky, 2) gruppesky, 3) privat sky og 4) hybrid

sky, som er en kombinasjon av de to første (Mell & Grance, 2011, s. 3). De allmenne skyløsningene er tjenester som selges på det åpne markedet, og tilbyr som regel standardiserte løsninger. Store leverandører som Google, Microsoft og Amazon tilbyr blant annet slike løsninger (Kommunal- og moderniseringsdepartementet, 2016, s. 8-9). Private skyløsninger tilbyr derimot en lukket skytjeneste, og denne er helt avgrenset til virksomheten(e) som kjøper tjenesten. Er tjenesten avsatt til flere virksomheter kalles den gruppesky. En kombinasjon av disse to løsningene der en bruker både allmenn sky og lokalt driftet IKT-system, privat sky eller gruppesky, kalles på sin side for hybrid sky (Kommunal- og moderniseringsdepartementet, 2016, s. 8-9).

Differensiering mellom de ulike typene er aktuelt for norske kommuner, som oppbevarer både viktig og kritisk informasjon, samt drifter kritiske tjenester for sine innbyggere. Store allmenne tjenester kan tilby store driftsfordeler og større kapasitet, mens å drifte egen sky eller sette data i privat sky vil kunne gi større garantier for eksempelvis hvor dataen er lagret, eller at kritisk info har tilstrekkelig med sikkerhetstiltak (Kommunal- og moderniseringsdepartementet, 2016, s. 9).

3.3 Lovverk som berører datalagring i kommunen

Departementene har som overordnet mål at «norske virksomheter digitaliserer på en sikker og tillitsvekkende måte, og har bedre evne til egenbeskyttelse mot uønskede digitale hendelser» (Departementene, 2019, s. 13). Ansvaret for å ivareta digital sikkerhet ligger hovedsakelig hos den enkelte virksomhet, men myndighetene skal legge til rette for arbeidet med å beskytte seg mot ønskede digitale hendelser, da dette vil gi høyere samlet robusthet i samfunnet (Departementene, 2019, s. 13). Myndighetene stiller i tillegg krav til at både offentlige og private virksomheter som eier kritisk digital infrastruktur, må gjennomføre tiltak for å sikre at det er forsvarlig sikkerhet i denne infrastrukturen (Departementene, 2019, s. 15).

Norges lovgivning er tilpasset EUs reguleringer angående salg av tjenester og regulering av personvern (Seip, 2020, s. 32). I Norge finnes det flere lover og forskrifter som på en eller annen måte omhandler sikkerhet rundt digitale data: personopplysningsloven, ekom-loven, helseregisterloven, pasientjournalloven, arkivloven, sikkerhetsloven, forvaltningsloven, personopplysningsforskriften, eForvaltningsforskriften og forskrift om objektsikkerhet. Mest sentrale er likevel sikkerhetsloven, arkiv loven, bokføringsloven og personopplysningsloven (GDPR), når det kommer til hvor data skal lagres (Kommunal- og moderniseringsdepartementet, 2016, s. 19).

Selve datasenterbransjen er ikke underlagt noen sektorer eller særegne lovverk. Det er derfor kun krav til forretningsvirksomhet som per i dag regulerer datasenteraktører (Nasjonal sikkerhetsmyndighet, 2022, s. 5). Det er derfor opp til den enkelte kunde å sette krav til kommersielle aktører ved kontraktsinngåelse (Nasjonal sikkerhetsmyndighet, 2022, s. 5).

3.3.1 Sikkerhetsloven

Etter den nye sikkerhetsloven kom i 2019 ble det presisert at departementene har ansvar for å identifisere grunnleggende nasjonale funksjoner innenfor sitt område, men det er den enkelte virksomhets leder som har ansvar for det forebyggende sikkerhetsarbeidet på virksomhetsnivå (Sikkerhetsloven, 2019). Sikkerhetsloven stiller krav til hvordan virksomheter, og derfor kommuner, forvalter informasjonssystem som gjør at det ikke er hensiktsmessig å lagre informasjonen hos leverandører utenfor Norge (Sikkerhetsloven, 2019).

Denne tilnærmingen tilsier at det er kommunene selv som må sikre informasjonssikkerhet ved skytjenester. Kommunene har også selvråderett på en rekke områder som gjelder egen kommune (Stortinget, u.d.). Både sikkerhetsloven og den kommunale selvråderetten bunner ut i at man lokalt sitter på mest kunnskap som angår nærområdet.

3.3.2 Arkivloven

Formålet med arkivloven er å beskytte arkiv som mulig kulturell eller forskningsmessig verdi, eller som inneholder dokumentasjon som er rettslig eller viktig forvaltningsmessig (Arkivloven, 1999). Denne informasjonen skal tas vare på og gjøres tilgjengelig for ettertiden. Det er flere unntak i loven som tillater å føre offentlige arkiv ut av Norge. Dersom det er nødvendig og midlertidig kan arkiv føres ut av landet, eksempelvis for at en saksbehandler tar med seg nødvendige dokumenter på tjenestereise. Oppbevaring av digitale kopier i utlandet er også tillatt, dersom det komplette arkivet er lagret i Norge (Arkivloven, 1999).

Loven berører datalagring fordi offentlige organer som ønsker å bruke skytjenester som befinner seg i utlandet, må ta hensyn til forbudet i loven som spesifiserer at man ikke kan føre arkiv ut av landet (Arkivverket, 2019). Frem til nå har bruk av skytjenester for lagring av offentlig arkiv blitt definert som å føre arkivene ut av Norge. Arkiv lagret i utlandet er heller ikke underlagt norsk lov, og kan komme til å bli påvirket av den gjeldende jurisdiksjonen der det er lagret. Det kan også være vanskelig å fastsette nøyaktig hvor dataene er lagret (Arkivverket, 2019).

3.3.3 Bokføringsloven

Bokføringsloven gjelder for alle som har regnskapsplikt etter regnskapsloven, deriblant kommunene, og inneholder bestemmelser for behandling og oppbevaring av regnskapsmateriale (Bokføringsloven, 2004). I loven finner man en rekke bestemmelser som kan påvirke datalagring i sky. Hovedregelen i bokføringsloven er at regnskapsmaterialet skal oppbevares i Norge, men unntak av dersom regnskapet føres i utlandet, virksomheten drives i utlandet eller elektronisk regnskapsmateriale kan oppbevares i nordiske land ved varsel til Skattedirektoratet (Bokføringsloven, 2004).

Bokføringspliktige er ansvarlige for å undersøke hvor serverne de benytter seg av befinner seg (Pedersen, 2019). Om disse serverne befinner seg utenfor Norden, må den enkelte virksomhet søke om dispensasjon til Skattedirektoratet for å kunne benytte lagringen. Denne dispensasjonen er derimot ikke enkel å få. Vanlige unntak er at lagring i utlandet tillates fordi det er en felles regnskapsløsning i et større konsern. Likevel kan søknaden avvises fordi en ikke har opplysninger om hvor serverne befinner seg. At virksomheten har innsikt i hvor serveren som benyttes befinner seg, er derimot problematisk, da flere leverandører ikke ønsker å oppgi eksakt plassering av serverne med hensyn til sikkerhet (Pedersen, 2019).

3.3.4 General Data Protection Regulation og personopplysningsloven

General Data Protection Regulation (GDPR) er en forordning som skal styrke personvernet ved behandling av personopplysninger innenfor den Europeiske Union (EU), men som også omhandler behandling av persondata utenfor EU eller overføring av personopplysninger ut av EU (GDPR.EU, u.å). Forordningen trådte i kraft i 2018, og ga like regler for alle næringsdrivende i EU. Fordi GDPR er en forordning har den direkte virkning i alle medlemslandene i EU, og krever ingen særskilt nasjonal lovgivning (GDPR.EU, u.å). I Norge trådte GDPR i kraft 20. juli 2018 som personopplysningsloven (Personopplysningsloven, 2018).

I personopplysningsloven er det 6 overordnede prinsipper for praksis av databehandling: 1) personopplysninger skal behandles på en lovlig, rettferdig og åpen måte, 2) dataen skal samles inn for spesifikke, berettigede formål, 3) de skal være adekvate, relevante og begrenset til formålets nødvendighet, 4) de skal være korrekte og nødvendig oppdaterte, 5) måten de lagres på skal sørge for at personer ikke kan identifiseres i lengre perioder enn nødvendig for formålet og 6) dataen skal behandles på en slik måte at det sikres tilstrekkelig sikkerhet for personopplysningene (Personopplysningsloven, 2018).

Virksomheter som behandler personopplysninger, har plikter de må oppfylle etter personvernregelverket (Personopplysningsloven, 2018). De må fastsette formål for å samle inn personopplysninger og ha et rettslig behandlingsgrunnlag for å være lovlig. Videre må de gi informasjon om hvordan de behandler personopplysningene på en kort og forståelig måte. Virksomheten må også legge til rette for at kunder eller brukere kan benytte sine rettigheter overfor dataene på en enkel måte. Det må også legges til rette for at den som får registrert data om seg selv kan rette og slette disse. Det er også krav til at visse virksomheten har et personvernombud. Videre må virksomheten gjøre vurderinger av personvernkonsekvenser for å sikre at personvernet til de som er registrert ivaretas. Løsningene som benyttes må ivareta personvern i alle utviklingsfaser, og det må sikres at personopplysningene beskyttes tilfredsstillende. Det skal føres protokoll over alle behandlingsaktiviteter der virksomheten behandler personopplysninger, og virksomheten som benytter seg av en underleverandør er pliktige til å ha databehandleravtaler med disse som sikrer at personopplysningene behandles i samsvar med regelverket. Dersom det oppstår avvik. må disse håndteres og rapporteres til Datatilsynet. Ved tilfeller der personopplysninger skal føres ut av EØS kreves det særskilt grunnlag for at dette skal være lovlig (Datatilsynet, u.å.-b; Personopplysningsloven, 2018).

For tjenesteutsetting av datalagring og behandling er artikkel 28 om databehandler i personopplysningsloven som er spesielt relevant. Artikkelen tar for seg bruk av databehandleravtaler mellom behandlingsansvarlige og databehandler (Personopplysningsloven, 2018).

En databehandleravtale er en avtale mellom en databehandler og en behandlingsansvarlig (Datatilsynet, u.å.-a). Avtalen spesifiserer hvordan personopplysninger skal behandles. Avtalens formål er å sikre at personopplysningene blir behandlet i samsvar med regelverket, og utgjør en klar ramme for hvordan databehandleren kan behandle de opplysningene som innhentes. Avtalen regulerer forholdet mellom den behandlingsansvarlige virksomheten og databehandleren (Datatilsynet, u.å.-a). Krav som spesifiseres i kontraktene, og verifikasjon av disse, utgjør et bindeledd mellom de behovene som virksomheten har, og tjenesten som tjenestetilbyderen leverer (Nasjonal sikkerhetsmyndighet, 2020c, s. 17).

Databehandleravtalene skal bidra til at både databehandleren og den behandlingsansvarlige forstår de forpliktelsene og ansvaret de har (Datatilsynet, u.å.-a). Det er likevel den behandlingsansvarliges ansvar at det kun brukes databehandlere som kan gi tilstrekkelige garantier for at tiltak som gjennomføres er egnede både teknisk og organisatorisk. Den behandlingsansvarlige har derfor ansvar for at databehandleren oppfyller kravene i

personopplysningsloven (Personopplysningsloven, 2018). Dette medfører at kommunene fortsatt har ansvar for dataene de setter i sky, selv om tjenesten kjøpes av en annen virksomhet.

3.3.4.1 Datalagring utenfor EU/EØS – motstridende eller usikker jurisdiksjon

Dersom persondata skal overføres innenfor EU-/EØS-land er det tilstrekkelig at det inngås en databehandleravtale. Dersom dataen skal overføres til land utenfor EU/EØS kan det inngås en EU Model Clause-avtale, også kalt standardkontrakter, om overføring av data utenfor EU/EØS (European Commission, 2021).

Der EU- og norsk lovgivning er skapt for å beskytte data og kontrollere dataflyt, spesielt vedrørende persondata, kan man ved bruk av skytjenester oppleve at ulik lovgivning i land utenfor EU fører til andre krav overfor de lagrede dataene (Seip, 2020, s. 37). Når en skytjeneste skaper dataflyt over landegrenser, kan dette føre til usikkerhet om hvilket som har jurisdiksjon overfor dataen (Seip, 2020, s. 37). Data som lagres slik at det kommer inn under et annet lands jurisdiksjon, kan føre til at norske virksomheter potensielt mister kontrollen over denne dataen. Det er blant annet slike hensyn som ligger bak lovgivning for overføring av persondata i EU, samt arkivloven og bokføringsloven (Seip, 2020, s. 37).

I etterkant av Schems II-dommen har det europeiske personvernrådet (EDPB) vedtatt to veiledere som følge av resultat i dommen (Datatilsynet, 2020). Veilederne skal brukes av alle som planlegger å overføre personopplysninger til land utenfor EØS. Den første veilederen omhandler hvilke vurderinger man må gjennomføre før man kan overføre personopplysninger utenfor EU. Den andre veilederen omhandler vurdering av beskyttelsesnivået i landet man skal overføre personopplysningene til, samt vurdering av om det finnes overvåkningslover som kan svekke personvernet i forhold til EØS-reglement (Datatilsynet, 2020).

Der GDPR og Schrems II-dommen har fokus på databehandlers plikt til å beskytte persondata lagret på vegne av behandlingsansvarlig, har andre jurisdiksjoner lovgivning som skal sikre innsyn i data. I 2018 ble Cloud Act vedtatt i USA (Seip, 2020, s. 37). Loven ble utformet for at amerikanske myndigheter skulle kunne, etter rettslig avgjørelse, kreve at selskaper som behandler data- og kommunikasjon måtte utlevere data de lagret for kunder, til myndighetene. Denne utleveringen vil gjelde for alle servere selskapene eier, både i USA og i utlandet (Seip, 2020, s. 37). Problemet med bruk av de markedsdominerende nettskyleverandørene Amazon Web Services, Google Cloud og Microsoft Azure, er derfor at uansett hvor mye databeskyttelse de lover, kan de få et rettslig pålegg om å utlevere kundenes data (Seip, 2020).

Hensynet til usikkerhet ved jurisdiksjon er grunnlaget for de strenge reglene i EU for overføring av persondata utenfor EU og EØS (Seip, 2020, s. 38).

For andre typer data enn persondata, foruten data som faller under annen lovgivning spesifisert i denne gjennomgangen, er det derimot i stor grad opp til den enkelte dataeier og behandlingsansvarlig virksomhet å innføre passende sikkerhetstiltak.

4. Teoretisk rammeverk

Det teoretiske rammeverket er essensielt i oppgaven for å tolke dataen som samles inn. Oppgaven er basert på et systemperspektiv, og jeg har utviklet et rammeverk av karakteristikker for datasuverenitet som kan anvendes for å undersøke ivaretakelse av datasuverenitet i kommunens arbeid med skytjenester. For å forstå datasuverenitet som begrep, er det også nødvendig å gjennomgå øvrige sikkerhetsbegrep tilknyttet data, og skille disse fra datasuverenitet.

4.1 Systemperspektiv

Kommunen er en del av et større og komplekst system som strekker seg fra den enkelte innbygger til Norge som stat. Kommunen kan også beskrives som å bestå av flere mindre systemer, som utgjør kommunen som system. Denne kompleksiteten er viktig å ta med i beregningen når en arbeider med samfunnssikkerhet. Njå og kolleger viser til at utformingen av komplekse systemer krever gode prosesser, og at dette er krevende. Derimot er det ikke et enkelt svar på hva som utgjør en god prosess (Njå et al., 2020, s. 130).

Videre viser de til at alle vurderinger av skjer i en kontekst av «…et system i den virkelige verden, hvor det kan være målformuleringer, rammebetingelser og t sett av virkemidler som utgjør et hele av funksjoner» (Njå et al., 2020, s. 130). På samme måte vil denne oppgaven peke på hvordan datasuverenitet i kommunene inngår i et stort system, der målformuleringer slik som interne strategier, rammebetingelser slik som lovgivning, og virkemidler slik som for eksempel databehandleravtaler, får betydning for datasuvereniteten i sin helhet, sammen med flere andre faktorer som inngår i norske kommuner som system.

Oppgaven vil likevel ikke anvende noen konkrete systemteorier som teoribasis for empirien, da utredelse av og fastsettelse av karakteristikker for datasuverenitet som fenomen, vil utgjøre teoridelen av oppgaven.

4.2 Datasuverenitet

I den følgende delen vil ulike definisjoner av datasuverenitet gjennomgås, og differensieres fra andre likende begrep, og andre sikkerhetsrelaterte begrep som informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet. Til slutt vil innhold i datasuverenitet som begrep gjennomgås, for å skille ut karakteristikker ved begrepet som vil anvendes i empirien og diskusjonen.

4.2.1 Suverenitetsbegrepet

Den moderne forståelsen av suverenitet varierer fra fokus på det kollektive, til det individuelle. Det er et konsept som blir brukt av svært forskjellige aktører med ulike perspektiver. Overordnet kan suverenitet defineres som en form for øverste myndighet over en politisk enhet (Couture & Toupin, 2019, s. 2308). Philpott definerer fire prinsipp for suverenitet: 1) det inkluderer autoritet, 2) autoriteten stammer fra en gjensidig anerkjent kilde til autoritet, 3) autoriteten er den høyeste makten, og 4) autoriteten er over et bestemt territorium (Philpott, 2003). Hollis bemerker midlertidig at disse territoriene ikke nødvendigvis trenger å bli begrenset til landområder, men at de også kan inkludere luftområder, infrastruktur eller ressurser slik som olje (Hollis, 2012). Denne tanken er spesielt interessant i en diskusjon om bruk av skytjenester og datasuverenitet, der tradisjonelle territorier i større grad er visket ut av den digitale infrastrukturen og overføring av data over tradisjonelle territoriale grenser.

Suverenitetsbegrepet koblet til det digitale kan omhandle flere aspekter, fra statsoverhoder til sosiale bevegelser og teknologikollektiv med anarkifokus. Disse aktørene konseptualiserer suverenitetsbegrepet forskjellig, og har forskjellige mål (Couture & Toupin, 2019, s. 2306). Regimer rundt om i verden har begynt å se på data som en viktig handelsvare som det er nødvendig å ha eierskap til, kontrollere og beskytte. Data utgjør viktig kapital, og skiller seg dermed ikke fra andre verdier slik som geografisk eiendom som tradisjonelt forbindes med suverenitetsbegrepet (Elms, 2021, s. 4). Tradisjonelle konsepter for territorialitet og jurisdiksjon kan derfor anvendes for å sette avgifter og krav til lokalisering av dataflyt over grenser (Elms, 2021, s. 4).

Jurisdiksjon er spesielt interessant når det kommer til dataflyt. Jurisdiksjon omhandler retten eller autoriteten til å tolke og anvende loven (Merriam-Webster, u.å). Denne autoriteten følger med en suveren makt til å styre og danne lovverk, og å utøve denne autoriteten. Jurisdiksjon er tilknyttet et territorium eller grenser innenfor hvor jurisdiksjonen kan utøves (Merriam-

Webster, u.å). En suveren enhet, for eksempel stat, delstat eller by, kan ha jurisdiksjon-, doms- og tvangsmyndighet i det avgrensede området de tilhører (NUPI, u.å). Jurisdiksjonen kan komme i konflikt med lovgivning i hjemlandet til behandlingsansvarlig av dataen, eventuelt interne krav som går utover lovgivning.

4.2.2 Definisjoner - datasuverenitet og liknende begrep

Det finnes flere liknende begreper til datasuverenitet, slik som digital suverenitet, teknologisk suverenitet, dataautonomi, og cybersuverenitet. Felles for alle disse begrepene er at det ikke er enighet om felles forståelse av dem.

Floridi beskriver datasuverenitet som kontroll av data, software, standarder og protokoller, samt prosesser, tjenester og infrastruktur som er digital (Floridi, 2020, s. 370). Liknende denne definisjonen er Posch sin definisjon av digital suverenitet, som han beskriver som evnen til å ha full kunnskap og kontroll over hvem som kan ha tilgang til dataen og hvor dataen overføres (Posch, 2017). Ved disse svært forenklede definisjonene av datasuverenitet og dataautonomi, kan begrepene se ut til å i stor grad omhandle samme fenomen.

Peterson definerer på sin side omfanget av problematikken rundt datasuverenitet som et mål om å begrense plasseringen av data innenfor presise geografiske grenser, og at denne begrensningen hører sammen med autentisering for tilgang (Peterson et al., 2011, s. 1).

Polatin-Reuben og Wrights definisjon er derimot mer rettet mot nasjonalstater, og definerer datasuverenitet som de tilnærmingene en stat bruker for å kontrollere data generert i, eller som passerer gjennom, nasjonal internettinfrastruktur. De setter en kobling til cyberdomenet der cybersuverenitet defineres som underkastelsen av cyberdomene til lokal jurisdiksjon (Polatin-Reuben & Wright, 2014, s. 1). Polatin-Reuben og Wrights definisjon av datasuverenitet harmonerer med definisjonen av Nugraha og Sastrosubroto som definerer begrepet som tiltak som nasjonalstater anvender på nasjonal flyt av sensitiv data over landegrenser (Nugraha & Sastrosubroto, 2015, s. 1).

I følge artikkelgjennomganger gjennomført av Baezner og Robin (2018) og Couture og Toupin, omhandler datasuverenitet kontroll av dataflyt via nasjonale jurisdiksjoner (Couture & Toupin, 2019). Svært interessant er det at Couture og Toupin påpeker at diskurs om datasuverenitet i USA ofte har negative konnotasjoner, mens det fra utenfor USA som oftest har positive konnotasjoner (Couture & Toupin, 2019, s. 2313). Det er også forskjeller i utøvelsen av datasuverenitet, der eksempelvis Kina bruker suverenitet som grunnlag for å kontrollere og sensurere data i eget intranett, mens sosiale bevegelser bruker

suverenitetsbegrepet for å beskytte mot en slik statlig eller kommersiell kontroll (Couture & Toupin, 2019, s. 2318). Dette viser til at datasuverenitet som begrep er svært kontekstavhengig og sterkt knyttet til nasjonstater og deres lovgivning, som igjen kan vise til vanskeligheter med å utvikle et felles rammeverk.

For norske kommuner vil forståelsen av datasuverenitet antakeligvis både innebære elementer av personlig suverenitet for innbyggerne, ved at de kan stole på at deres data blir behandlet og lagret på en tilfredsstillende måte, men også en kollektiv suverenitet slik som å beskytte nasjonale sikkerhetsinteresser (Couture & Toupin, 2019).

Sterk datasuverenitet på nasjonalt nivå innebærer beskyttelse av nasjonale interesser, nasjonal sikkerhet og innbyggeres data, mens svak datasuverenitet innebærer at privat sektor er den som tar initiativer for databeskyttelse (Kaloudis, 2021, s. 6). Denne todelingen likner på Polatin-Reuben og Wrights definisjon av dataautonomi, der svak dataautonomi karakteriseres av at den private sektoren leder initiativ for å beskytte data, mens sterk datasuverenitet karakteriseres av en statlig ledet tilnærming med fokus på å beskytte nasjonal sikkerhet (Polatin-Reuben & Wright, 2014, s. 1). Denne måten å se på dataautonomi trekker linjer til avhengighetsforholdet det offentlige setter seg i når det private leder initiativene for databeskyttelse. Når kommunene lagrer data hos andre aktører enn statlige, fører det til en avhengighet av disse aktørene. Avhengigheten påvirker både om dataene er tilgjengelige, men også om de er sikre fra målrettede angrep som hacking og statlig etterretning. Det kan virke som om svak datasuverenitet henger sammen med lav grad av digital autonomi. Dataautonomi, ofte omtalt sammen med digital autonomi og digital suverenitet, omhandler å sikre at digitale funksjoner ikke er avhengige av enkeltfunksjoner eller enkeltselskaper (Seip, 2020, s. 40). Digital autonomi skal på sin side sikre teknologisk uavhengighet (Stach, 2020), slik som de overnevnte definisjonene av datasuverenitet påpeker at kan være problematisk.

Der datasuverenitet som begrep har fokus på selve dataen og dataflyten, beskrives teknologisk suverenitet av Kaloudis som forståelsen av og evalueringen av hvor relevant spesifikke teknologier er for økonomien, samfunnet og politikk, og at man må finne en måte å bruke disse teknologiene på som så langt som mulig er sikrer suverenitet uten avhengighet og påvirkning fra andre aktører (Kaloudis, 2021, s. 7). På denne måten kan man opprettholde muligheten til uavhengige handlinger og beslutninger (Kaloudis, 2021, s. 7). Couture og Toupin definerer derimot teknologisk suverenitet som å være i opposisjon av markedsdominerende teknologileverandører, slik som de USA-baserte private teknologibedriftene Google, Amazon, Facebook, Apple og Microsoft (Couture & Toupin,

2019, s. 2317). Likevel vil valg av type skytjeneste, for eksempel privat eller offentlig, samt valg av leverandør, grunnet avhengighet og jurisdiksjon i virksomhetens land, kunne være relevant for også datasuverenitet, fordi det berører hvor stor kontroll man har over dataen og dataflyt.

Datasuverenitet handler ikke kun om å beskytte innbyggernes rettigheter via deres egne data, men kan ses på som et reguleringstiltak for å styrke egne innenlandske firmaer og sektorer slik som teknologisektoren. Denne formen for datasuverenitet kan gå på bekostning av fri flyt av varer og tjenester (Elms, 2021, s. 19).

4.2.3 Datasuverenitet sammenliknet med informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet

Datasuverenitet som begrep har også flere likheter, og ulikheter, til mer etablerte sikkerhetsbegrep. I den følgende delen vil derfor begrepene informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet gjennomgås. Det vil gjøres en sammenlikning av de tre begrepene, før det gjennomgås hvordan datasuverenitet henger sammen med disse.

4.2.3.1 Informasjonssikkerhet

Informasjonssikkerhet defineres som beskyttelsen av informasjon og dens kritiske element (von Solms & van Niekerk, 2013, s. 98). Denne beskyttelsen inkluderer systemene og maskinvare som behandler, oppbevarer eller overfører informasjon. Informasjonssikkerhet er dermed en prosess, og ikke et produkt eller en teknologi (von Solms & van Niekerk, 2013, s. 98).

Denne prosessen er rettet mot å oppnå karakteristikker som sikker informasjon burde ha (von Solms & van Niekerk, 2013, s. 98). Informasjonssikkerhet beskrives derfor ofte, og også i norsk sammenheng, som opprettholdelse av de tre karakteristikkene konfidensialitet, integritet og tilgjengelighet. Informasjon er konfidensiell når den er beskyttet fra å bli eksponert eller delt av individer eller systemer som ikke er autoriserte. Kun de med rettigheter til å få tilgang til informasjon skal få tilgang. Dersom disse autoriserte personene eller systemene har tilgang, anses dataene som tilgjengelige. Integritet kan oppnås dersom informasjonen er hel, komplett og ikke korrupt. Dataens integritet kan påvirkes både under lagring og overføring (DSB, 2016, s. 64; Whitman & Mattord, 2021, s. 11-15).

4.2.3.2 IKT-sikkerhet

IKT-sikkerhet omhandler beskyttelse av teknologibaserte system som lagrer og overfører informasjon (von Solms & van Niekerk, 2013, s. 98). Konseptet er tett knyttet til

informasjonssikkerhet, da IKT-sikkerhet defineres som alle aspekter relatert til å definere, oppnå og opprettholde konfidensialitet, integritet, tilgjengelighet, ikke-fornektelse, ansvarlighet, autentisitet og pålitelighet til informasjonskilder (von Solms & van Niekerk, 2013, s. 99).

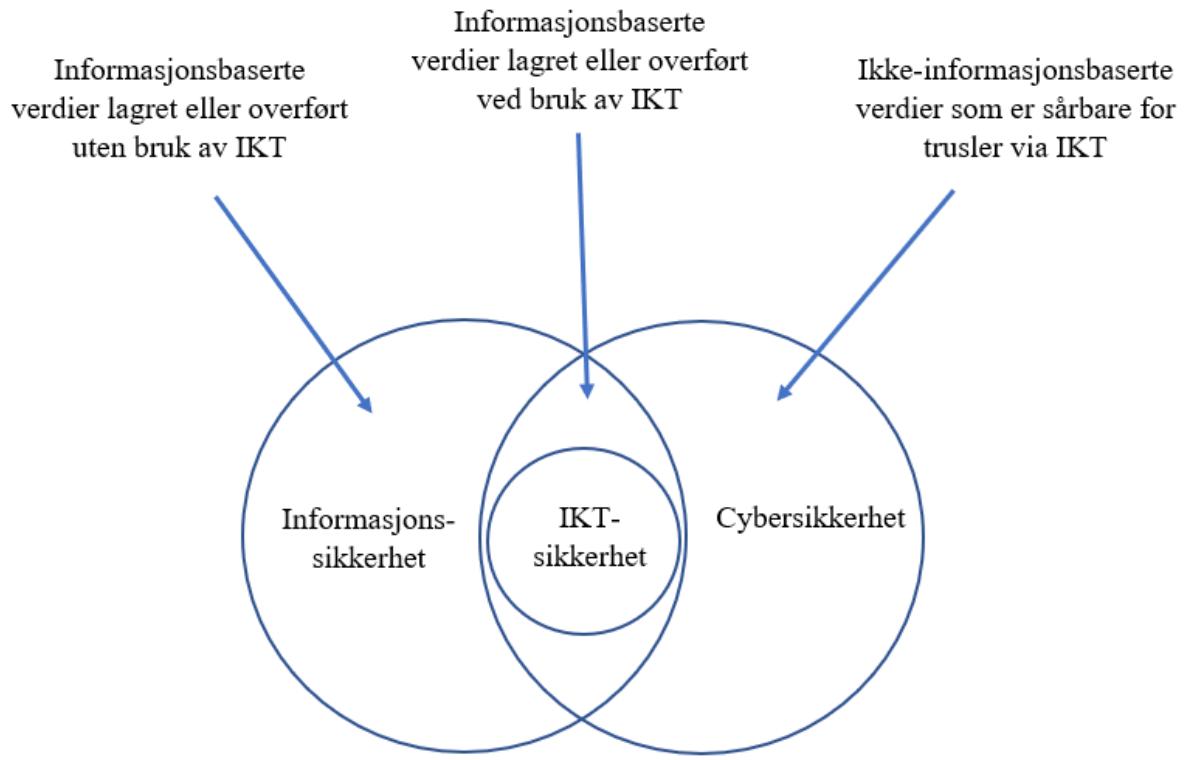
IKT-sikkerhet kan ses på som en underkomponent av informasjonssikkerhet, fordi det inkluderer beskyttelse av de underliggende informasjonsressursene (von Solms & van Niekerk, 2013, s. 98). IKT-sikkerhet er derfor i stor grad knyttet til hvor pålitelig sikkerheten er i selve informasjonssystemet som dataen befinner seg i (von Solms & van Niekerk, 2013, s. 99). Sikker informasjons- og kommunikasjonsteknologiressurser er oppsummert ikke mer en sikker informasjonsressurs som befinner seg inne i et informasjonsteknologisystem (von Solms & van Niekerk, 2013, s. 99). En kan derfor si at IKT er infrastrukturen som prosesserer, lagrer og kommuniserer informasjonen, som en ønsker at skal være beskyttes. (von Solms & van Niekerk, 2013, s. 99)

4.2.3.3 Cybersikkerhet

Cybersikkerhet har forskjellige definisjoner med varierende kompleksitet. En omfattende definisjon satt av The International Telecommunications Union definerer cybersikkerhet som:

> Samlingen av verktøy, policyer, sikkerhetskonsepter, sikkerhetstiltak, retningslinjer, risikostyringstilnærminger, handlinger, trening, beste-praksiser, forsikring og teknologi som kan brukes for å beskytte cybermiljøet og organisasjons- og brukerkapital. Cybersikkerhet streber etter å sikre oppnåelse av og opprettholdelse av sikkerhetsegenskapene til en organisasjons- og brukerkapital mot relevante sikkerhetsrisikoer i cybermiljøet. (International Telecommunication Union, 2008, s. 2, fritt oversatt fra originalspråk).

I likhet med informasjonssikkerhet, kan de generelle sikkerhetsmålene beskrives som å være tilgjengelighet, integritet og konfidensialitet (von Solms & van Niekerk, 2013, s. 98). Grensene til cybersikkerhet går derimot breiere enn informasjonssikkerhet, fordi det også inkluderer beskyttelse av kapital som ikke er informasjonsbasert. Derimot inkluderer ikke cybersikkerhet analoge data, slik som informasjonssikkerhetsbegrepet gjør.



Figur 1. Forskjellen i verdier for IKT-sikkerhet, informasjonssikkerhet og cybersikkerhet (Tilpasset fra von Solms & van Niekerk, 2013 s. 101)

I figur 1 vises det til at informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet har flere fellesområder og likheter når det kommer til hvilke verdier som er i fokus (von Solms & van Niekerk, 2013). Figuren er konsentrert rundt hvilken type verdi de ulike fenomenene omhandler. Informasjonssikkerhet omfatter både digital informasjon ved bruk av informasjons- og kommunikasjonsteknologi, og analog informasjon. Informasjonssikkerhetsbegrepet omfatter derfor hele IKT-sikkerhetsbegrepet som omhandler informasjon som lagres eller overføres ved hjelp av informasjons- og kommunikasjonsteknologi. Det omfatter også den delen av cybersikkerhet som omhandler digital informasjon. Cybersikkerhet omhandler derimot også ikke-informasjonsbaserte verdier som er sårbare for trusler via IKT (von Solms & van Niekerk, 2013).

Ved IKT-sikkerhet er det den underliggende informasjonsteknologien og tilhørende infrastruktur som må beskyttes, til forskjell fra informasjonssikkerhet, der definisjonen inkluderer beskyttelse av informasjonen i seg selv, samt at det også inkluderes sikkerhet rundt informasjon som ikke lagres i IKT-systemer (von Solms & van Niekerk, 2013, s. 100). Cybersikkerhet skiller seg ut ved at det også beskytter kapital som ikke er tilknyttet data eller

et IKT-system, men tilhørende elementer slik som personer, samfunnsinteresser og kritisk infrastruktur, som kan være sårbart gjennom IKT-systemer (von Solms & van Niekerk, 2013, s. 100).

4.2.3.4 Behovet for datasuverenitet som eget sikkerhetsbegrep

Det er mange likheter mellom de presenterte begrepene og datasuverenitet, eksempelvis at de alle omhandler å sikre informasjon eller informasjonsrelaterte verdier, samt at det er en trussel om personer som ikke skal ha tilgang får tilgang til informasjonen. For å forstå behovet for datasuverenitet som eget sikkerhetsbegrep, må vi se på hvordan det skiller seg fra de øvrige sikkerhetsbegrepene definert over.

I tabell 1 presenteres min forståelse av de største forskjellene på informasjonssikkerhet, IKT-sikkerhet, cybersikkerhet og datasuverenitet.

Tabell 1. De største forskjellene på informasjonssikkerhet, IKT-sikkerhet, cybersikkerhet og datasuverenitet

	Informasjons-sikkerhet	IKT-sikkerhet	Cybersikkerhet	Datasuverenitet
Verdi	Analoge og digital data	IKT-systemet	Digitale data og verdier som kan nås via IKT	Digitale data, og verdier som påvirkes av bortfall av data
Fokus	Beskytte analoge og digitale data	Beskytte IKT-systemet for å beskytte digitale data	Beskytte data og tilstøtende verdier	Eierskap til og kontroll over egne digitale data
Trussel	Ondsinnede aktører	Ondsinnede aktører	Ondsinnede aktører	Jurisdiksjon

Forskjellene er delt inn i kategoriene «verdi», «fokus» og «trussel». Som presentert i figur 1 er verdiene i informasjonssikkerhet både analoge og digitale data, mens IKT-sikkerhet omhandler de fysiske komponentene som utgjør IKT-systemet som digitale data lagres i, mens cybersikkerhet omhandler digitale data og andre verdier som kan nås via IKT-system (von Solms & van Niekerk, 2013). Datasuverenitet omhandler kun digitale data som verdi (Hummel et al., 2021, s. 7), men fordi disse dataene, spesielt i lys av skytjenester, brukes for å drifte systemer og tjenester, vil begrepet også påvirke andre verdier. Det omhandler derimot ikke verdier som kan nås via IKT-systemet slik som cybersikkerhet, men vil i større grad konsentrene seg om hva som skjer dersom de digitale dataene, for eksempel et system som brukes til kritisk infrastruktur, faller bort.

Selv om alle begrepene til en viss grad handler om tiltak for å sikre data eller tilknyttede verdier, vil jeg argumentere for at informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet i stor grad omhandler å beskytte disse verdiene. For å beskytte verdiene settes det opp mottiltak som skal hindre ondsinnede aktører å påvirke i negativ forstand (Humayun et al., 2020). For datasuverenitet er det derimot eierskap til egne data og kontroll over denne, som er i sentrum (Hummel et al., 2021). Hvem som eier dataen og har rettigheter til denne, kan påvirkes av motstridende jurisdiksjon (Hummel et al., 2021). Det trenger altså ikke være ondsinnede aktører, men ulikheter i lovgivning og jurisdiksjon, som truer datasuverenitet. Intensjonen til andre suverene aktører slik som stater, kan derimot være lik enten de anses som trusler for cybersikkerhet eller datasuverenitet. Statlige aktører kan på den ene siden være ondsinnede aktører, for eksempel gjennom statlig sponsede cyberangrep. På den andre siden kan de benytte jurisdiksjon for å få innsyn i den samme dataen. Selv om målet, for eksempel verdien som finnes i data, kan være det samme, er metodene og virkemidlene annerledes ettersom det er cyberangrep eller jurisdiksjon som benyttes. Intensjonen bak å benytte jurisdiksjon for å få innsyn i data trenger heller ikke være ondsinnet, for eksempel om en nasjon hevder at innsyn i dataen vil være nyttig for å føre en rettssak tilknyttet enten dataen eller databehandler. Eksempelvis kan amerikanske selskaper risikere å måtte utlevere data i skytjenester med bakgrunn i en dom, uavhengig av om selve lagringsstedet befinner seg i USA, slik som vist til i oppgavens kontekstkapittel om Cloud Act. Derimot vil teknisk svikt kunne være en trussel for både datasuverenitet og de øvrige begrepene.

Selv om det er forskjeller mellom de fire begrepene, vil det også være likheter i hvordan arbeidet med å styrke dem ser ut. Eksempelvis vil arbeid med informasjonssikkerhet for å styrke konfidensialitet, integritet og tilgjengelighet, tidligere påpekt som trekk ved informasjonssikkerhet (DSB, 2016, s. 64; Whitman & Mattord, 2021, s. 11-15), kunne være positivt for datasuverenitet, fordi en arbeider for å begrense tilgang til dataene, sikre at de er korrekte og tilgjengelige for det de skal brukes til. Å hindre at uvedkommende, for eksempel unødvendig innsyn fra leverandørens side, har tilgang til data, er også en del av alle fire begrepene. Felles for alle begrepene er dermed også at brudd på datasuverenitet, informasjonssikkerhet, IKT-sikkerhet eller cybersikkerhet vil alle føre til tap av integritet, konfidensialitet og tilgjengelighet (von Solms & van Niekerk, 2013).

Uansett hvor mange sikkerhetstiltak, redundante løsninger og optimalisering av de tekniske systemene som er gjort, vil det ikke kunne sikre at lovgivning og jurisdiksjon overstyrer retten til innsyn i data. Selv om GDPR som lovgivning har medført at man skal sette krav til hvor

dataen lagres og potensielt hvor databehandler hører til (Personopplysningsloven, 2018), er dette ikke en del av informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet som konsepter. Det er derimot blitt en praksis gjennom fokus på disse begrepene sammen med personvern, men det mangler et overordnet fokus som ser på slike faktorer for all data, ikke kun persondata. Her er det plass for datasuverenitet som et nytt sikkerhetsbegrep, der både nasjoner og virksomheter kan sette overordnede eller egne krav til eierskap og rettigheter til egne data.

4.2.4 Innhold i datasuverenitet som begrep

Der de to forgående delene har sett på enkle definisjoner av datasuverenitet som begrep, og hvordan dette skiller seg fra liknende begrep og andre sikkerhetsbegrep, vil den følgende delen se på selve innholdet i datasuverenitet som begrep. Fordi datasuverenitet er et begrep som foreløpig er uten enighet om felles forståelse, vil det kunne eksistere flere variasjoner av innhold i begrepet.

Utgangspunktet for denne delen er derfor en litteraturgjennomgang gjennomført i 2021. Hummel og kolleger har gjennomført en gjennomgang av 341 publikasjoner for å analysere hva begrepet datasuverenitet innebærer, sammenliknet med liknende begrep. Gjennomgangen deler begrepet inn i de fem kategoriene forståelse, agenter, kontekst, verdier og innhold (Hummel et al., 2021, s. 2).

Gjennomgangen viser at datasuverenitet som begrep var betydelig oftere nevnt med 680 av 1492 treff, enn liknende begrep slik som cybersuverenitet, digital suverenitet, og samlekategorien «other» som inneholdt blant annet nasjonal suverenitet (Hummel et al., 2021, s. 6).

Selve innholdet i datasuverenitetsbegrepet deles i artikkelgjennomgangen inn i forståelse av begrepet, utfordringer og ledelsesstrategier (Hummel et al., 2021). Artikkelgjennomgangen fant at det var seks ulike typer forståelse av begrepet datasuverenitet. Den første forståelsen ser på datasuverenitet som en reduksjon, der man kan bryte ned begrepet til mer spesifikke forhold og verdier. Eksempelvis kan denne formen ta for seg hvordan konfidensialitet blir ivaretatt ved bruk av skytjenester. Den andre forståelsen er datasuverenitet som en mulighet, eksempelvis muligheten til å ha full kontroll over egne data. Den tredje forståelsen ser på datasuverenitet som en rettighet, eksempelvis retten til at en nasjon samler og behandler egen data. Den fjerde innholdsforståelsen ser på datasuverenitet som resultatet av lovverk, der data blir underlagt lovverket i landet det er lokalisert i. Den femte forståelsen av datasuverenitets

innhold står i kontrast til den forrige, og ser på datasuverenitet som en kontrast til lovverk, der datasuverenitet kan bli sett på som mindre rigid og mer fleksibel enn lovverket. Den sjette og siste forståelsen av innholdet i datasuverenitet omhandler forholdet mellom datasuverenitet og suverenitet generelt. Datasuverenitet kan både bli sett på som en del av, forlengelse av eller forutsetning for nasjonal suverenitet (Hummel et al., 2021, s. 6-7).

Det er beskrevet fire ulike utfordringer ved datasuverenitet (Hummel et al., 2021, s. 7-8). Den første formen for utfordringer er grunnleggende trekk ved dataens natur. En slik utfordring kan være at ubeskyttet data kan multipliseres uten store kostnader og tap av kvalitet. Fordi data i sky er tilknyttet fysiske komponenter i form av IoT (internet of things) vil definisjonen av området av relevans, for eksempel lagringssted, for dataen, kunne være forskjellig fra den skybaserte løsningen til de fysiske komponentene. Den andre formen for utfordring gjelder tekniske design, der spesifikke tekniske design fremstilles som om de utfordrer datasuverenitet, eksempelvis design som øker kompleksiteten av dataprosessering. Den tredje formen for utfordring omhandler epistemiske problem, ved at det er svært mange usikkerheter rundt datasuverenitet, eksempelvis sikkerhet ved bruk av skylagring. Den fjerde formen problem spiller videre på den epistemiske usikkerheten, ved at det kan være uklart hvilken lovgivning som gjelder (Hummel et al., 2021, s. 7-8).

Artikkelgjennomgangen presenterer fire ulike ledelsesstrategier som kan brukes for å implementere og realisere datasuverenitet (Hummel et al., 2021, s. 8-9). Den første strategien går ut på å styrke grunnleggende komponenter av datasuverenitet tilknyttet dataens natur eller kontekst. Dette kan eksempelvis gjøres med å sette inn tiltak som gjør det vanskelig å kopiere data, og følge med på dataens kontekst altså hvor den befinner seg og hvilke lover den havner under. Den neste strategien går ut på å bruke en teknisk tilnærming, der en ser på hvilke rutiner og protokoller som må etableres, eksempelvis kryptering, dataovervåkning og tilsyn. Denne ledelsesstilen har fokus på at datasuverenitet kan bygges inn i IT-arkitekturen. Den tredje ledelsesstrategien omhandler de epistemiske utfordringene tidligere presentert, og innebærer derfor å hindre informasjonsmangler og forsterke transparens. Ved denne formen blir tydelig at folk skal vite hvilken data som samles inn om den, og hvordan den brukes. Den fjerde og siste ledelsesstrategien innebærer at lovverket i enkelte stater krever at spesifikke typer data holdes innenfor opphavslandet eller sted spesifisert i restriksjonene dersom data skal fraktes utover landegrensen (Hummel et al., 2021, s. 8-9). En kan kjenne igjen EUs GDPR-lovgivningen i denne ledelsesstrategien.

Artikkelgjennomgangen viser at ulike aktører forekommer med forskjellige forståelser av suverenitet (Hummel et al., 2021, s. 9). For datasuverenitet er forekomsten høy med aktørene *urbefolkning, bruker/forbruker* og *privatsektor organisasjoner*. Til sammenlikning har cybersuverenitet, digital suverenitet og internettsuverenitet høyere forekomst med aktøren *land* (Hummel et al., 2021, s. 9). For bruk av skytjenester er privatsektoren sterkt involvert, og en kommune som virksomhet vil ofte være forbruker av disse tilbudene for å støtte opp om egen drift. Urbefolkning som aktør er mindre relevant når en generelt ser på bruk av skytjenester i norske kommuner.

Datasuverenitet viser i artikkelgjennomgangen høy forekomst sammen med kontekstene *IT-arkitektur og lovgivning* (Hummel et al., 2021, s. 9). Cybersuverenitet viser på sin side høy forekomst sammen med kontekstene *forsvar, internasjonale forhold, lovgivning* og *overvåkning*, mens digital suverenitet har høy forekomst sammen med *IT-arkitektur* og *forsvar*. Datasuverenitet gjelder lovgivning når lovgivning begrenser grenseoverskridende dataoverføringer og generelle vanskeligheter med å innrette behandling etter lovlige krav (Hummel et al., 2021, s. 9), slik som en finner i GDPR. Lovgivning som kontekst har dermed også kobling til jurisdiksjon i andre land. For kommuner som benytter skytjenester, må de være observante på om dette kan være motstridende til egne ønsker og lovkrav. Koblingen til IT-arkitektur omhandler tilgang til informasjonsinfrastruktur, innhold og enheter med internettilkobling. Den viser også til at datasuverenitet som begrep omhandler digital informasjon som blir lagret i forskjellige varianter av IT-arkitektur (Hummel et al., 2021). IT-arkitekturen er derfor relevant å undersøke for skytjenester, fordi det finnes ulike former for tjenestetilbud som potensielt kan påvirke grad av datasuverenitet.

Datasuverenitet har høy kobling til verdiene *kontroll, makt* og *personvern*, samt normative konsepter *som overveielse* og *inkludering, sikkerhet* og *ikke-skadelighet* og *eierskap* (Hummel et al., 2021, s. 10). For overordnet bruk av skytjenester i norske kommuner er verdiene kontroll og makt mest interessante, og overveielse og inkludering (for eksempel av urbefolkning) vil ikke ses på i denne studien. Personvern, sikkerhet, og eierskap vil på sin side dekkes under flere andre punkter, og anvendes derfor ikke som verdi i det oppsummerte rammeverket under kapittel 4.2.5.

Den grundige gjennomgangen viser at datasuverenitet som begrep og konsept er knyttet til flere forskjellige, og til tider motstridende, forståelser. Det er et rikt begrep med flere dimensjoner. Det er likevel noen konnotasjoner som går igjen i de forskjellige områdene. Disse inkluderer at datasuverenitet omhandler en form for kontroll eller eierskap over data

eller infrastruktur tilknyttet data. Dataen er digital, og er ikke begrenset til personvern, selv om dette er et viktig aspekt av konseptet. Aktører som går igjen, er blant annet land og forbrukere. Begrepet går igjen i kontekstene IT-arkitektur og lovgivningen, og inkluderer ofte verdiene kontroll, makt, overveielse og inklusjon, samt personvern (Hummel et al., 2021, s. 11-12). De øvrige begrepene forholder seg hovedsakelig til land som aktører. Datasuverenitet har også sterkere kobling til samfunnsdiskurser enn de øvrige begrepene.

Det er likevel fremdeles problematisk at aktører som skriver om datasuverenitet ikke spesifiserer sin forståelse av datasuverenitet (Hummel et al., 2021, s. 12). Denne manglende forståelsen gjør det vanskeligere å svare på hva som kreves for å oppnå datasuverenitet, og hvilke mekanismer en kan iverksette for å forsterke det. Det kan også gjøre det vanskeligere å forstå hvem som har ansvar for å sikre datasuverenitet (Hummel et al., 2021, s. 14).

4.2.5 Oppsummering – karakteristikker for datasuverenitet til bruk i analysen

I denne delen vil funnene fra gjennomgangen av tidligere forskning på datasuverenitet oppsummeres for å utlede karakteristikker for datasuverenitet, som vil brukes i resten av oppgaven. Karakteristikkene vil brukes for å undersøke datasuverenitet i kommunen, i empiri- og analysedelen i oppgaven.

Utgangspunktet for tabellen er at det ikke er enighet om en felles forståelse for datasuverenitet som begrep eller konsept, ei heller hva begrepet innebærer i praksis. Karakteristikkene som er inkludert er valgt ut basert på å gå igjen i sammenheng med datasuverenitetsbegrepet.

Det er viktig å poengtere at enighet om begrepsforståelse ikke nødvendigvis vil gjøre datasuverenitet lettere å håndtere, styrke eller arbeide med. Det er likevel essensielt for oppgaven å legge en forståelse til grunnlag for empiri- og analysedelen av oppgaven. Karakteristikkene er forenklede, men vil inkludere ulike underkarakteristikker og deres kjennetegn som er fremtredende for datasuverenitet som konsept.

Fordi oppgaven spesifikt ser på bruk av skytjenester i norske kommuner, vil de utvalgte karakteristikkene og underkarakteristikkene være tilpasset dette arbeidet. Jeg har derfor ikke inkludert aspekter ved datasuverenitet som ikke er aktuelle for overordnet datalagring i skytjenester i norske kommuner, slik som eksempelvis urbefolkningsaspekter og samfunnsengasjement. Som vist til tidligere, vil avgrensningen også holdes til kommunen, og vil dermed ikke vie spesiell oppmerksomhet til det nasjonale aspektet av datasuverenitet som ser på datasuverenitet som viktig for nasjonal sikkerhet.

I tabell 2 presenteres de utvalgte karakteristikkene og underkarakteristikkene for datasuverenitet, koblet til arbeid med skytjenester i norske kommuner.

Tabell 2. Karakteristikker for datasuverenitet

Overordnet karakteristikk	Underaspekt av karakteristikken	Implikasjoner for analyse av skytjenester
Verdier	Kontroll - Hvor er dataen? - Eierskap og begrensing av tilgang Makt - Hvem har makt og autoritet over utvikling og data? - Avhengighet av tjenesteleverandør	Ved å undersøke disse to verdiene kan en se på om kommunene vet hva som skjer med dataen når den overlates til tjenesteleverandør, og om de har påvirkning på hvordan lagringen skjer.
Datatype	Digitale data Dataklassifisering - Persondata - Andre kritiske data Kollektiv vs individuell dimensjon – har dataen betydning for innbyggerne eller kommunen?	Hvilke data kommunen har fokus på, og hvordan datatype påvirker valg av tjeneste, vil være avgjørende for datasuvereniteten. Videre vil fokus på en individuell dimensjon (beskyttelse av persondata for innbyggere) skille seg fra en kollektiv dimensjon (løfter fokuset opp på data som er viktige for kommunen)
Kontekst	IT-arkitektur - Innsikt i tekniske aspekter ved skyløsningen Lovgivning - Lovgivning er avhengig av nasjonalstater og/eller internasjonale organ	De to ulike kontekstene gir mulighet til å undersøke hvordan rammer utenfor kommunen påvirker datasuverenitet.

	- Jurisdiksjon i andre land kan være motstridende til lovgivning i Norge	
Håndtering	Ledelsesstrategier - Hvordan tilnærmer kommunen seg datasuverenitet? Hvilke virkemidler har de tilgjengelig? - Interne og eksterne	Hvilken ledelsesstrategi kommunen har til aspekter ved datasuverenitet kan si noe om kommunens tilnærming til datasuverenitet er fordelaktig eller ei.
Utfordringer	Utfordringene kan være tilknyttet grunnleggende komponenter ved data, teknisk design, epistemiske utfordringer rundt usikkerhet, uklar lovgivning eller jurisdiksjon.	Utfordringene er interessante å undersøke for å få innblikk i hva som hemmer arbeidet med datasuverenitet.

Fra tabellen ser vi at den første overordnede karakteristikken «verdier» har de to underkarakteristikkene «Kontroll» og «makt». Kontroll omhandler hvor dataen befinner seg, eksempelvis hvor geografisk er datasentrene tilknyttet databehandler. Kontroll omhandler også å ha eierskap til egne data. Verdien omhandler også tilgangsstyring, både hos databehandler og behandlingsansvarlig. «Makt» omhandler på sin side hvem som har autoritet over både dataen i skytjenester, men også utvikling av teknologi og skytjenester som felt. Det er her likheter til kontroll, da autoriteten kan påvirke hvem som har størst eierskap til dataen.. Personvern er ikke inkludert som en verdi, fordi det naturlig inngår i neste karakteristikk som ser på ulike typer data.

Den andre overordnede karakteristikken er «data». Data viser til at dataene datasuverenitet omhandler er digitale, slik som i skytjenester. Dataklassifisering omhandler en prosess ved å definere dataen og bestemme følsomhetsnivå (Shaikh & Sasikumar, 2015, s. 494). Kommunen må gjennomføre dataklassifiseringer for å ha oversikt over hvilken type data de behandler, da datasuverenitet omhandler all data, ikke kun persondata og personvern. Data tilknyttet individuell dimensjon omhandler persondata som samles inn, for eksempel at kommunen må beskytte og ha kontroll over dataen de samler inn om sine innbyggere, og er dermed sterkt knyttet til personvern og rettigheter til egne data. Kollektiv dimensjon omhandler data som kan få betydning for kommunen som en helhet, og potensielt nasjonal sikkerhet, eksempelvis virksomhetskritisk informasjon eller økonomisk informasjon.

Den tredje overordnede karakteristikken for datasuverenitet er «kontekst», som deles inn i underkarakteristikkene «IT-arkitektur» og «lovgivning». IT-arkitektur som kontekst tillater oss å se på forholdet mellom private og offentlige aktører. For kommunene vil dette være spesielt relevant, fordi de som oftest benytter private tjenesteleverandører for skytjenester. Dette kan skape avhengigheter som kan påvirke kommunens tilbud. Avhengighets-aspektet henger sterkt sammen med verdien makt, og videre autoritet, da store markedsaktører dominerer skytjenestetilbudene, og det er begrenset hvor mye regulering gjennom lovverk endrer, da de private leverandørene driver den teknologiske utviklingen. Potensielt enda mer begrenset er hvor mye kommunene som virksomheter får endret og tilpasset leveransene. IT-arkitektur som kontekst henger også sammen med utformingen av tjenesten, henholdsvis om skytjenesten er offentlig, hybrid eller privat, og hvordan valgte løsning påvirker datasuverenitet. Eksempelvis vil kryptering av data og innsikt i datamodell kunne påvirke grad av suverenitet.

Lovgivning som underkarakteristikk er avhengig av hvilken nasjonalstat dataens eier befinner seg i, som i denne oppgavens tilfelle er Norge for de norske kommunene. Derimot vil også jurisdiksjon være en underkarakteristikk, fordi lovgivning i både lagringsland og databehandlers land vil kunne påvirke rettigheter til innsyn i dataene som lagres i skytjenester.

Den fjerde overordnede karakteristikken er «håndtering», som viser til underkarakteristikken «ledelsesstrategier». I litteraturgjennomgangen spesifiseres fire ulike ledelsesstrategier for å håndtere datasuverenitet: 1) Promotere grunnleggende komponenter – for eksempel faktorer ved dataens natur eller kontekst. 2) Teknisk tilnærming – protokoller, for eksempel forkryptering, dataovervåkning og tilsyn. 3) Epistemiske utfordringer – hindre informasjonsmangler, forsterke transparens, overfor de dataene samles inn om 4) Lovverk – krever at spesifikke data skal holdes innenfor opphavsland eller spesifisert sted dersom utenfor landegrenser. Ledelsesstrategi omhandler også hvilke interne og eksterne virkemidler man har tilgjengelig for å kunne gjennomføre disse.

Den femte overordnede karakteristikken for datasuverenitet er «utfordringer». Utfordringene kan være tilknyttet dataens natur, teknisk design, epistemiske utfordringer rundt usikkerhet, uklar lovgivning eller jurisdiksjon.

Flere av underkarakteristikkene er liknende på tvers av de overordnede karakteristikkene, og de må derfor sees i sammenheng. Eksempelvis kan lovgivning både være en utfordring om denne er uklar, men samtidig være en kontekst og i tillegg en del av en ledelsesstrategi.

Lovgivning og jurisdiksjon vil også påvirke hvem som har kontroll over dataen og hvem som har autoritet.

5. Forskningsmetode

Mitt valg av forskningsmetode, forskningsdesign og øvrige metodiske valg danner grunnlaget for denne oppgaven. For å sikre transparens og forståelse for valgene som er gjort, vil de begrunnes ved å redegjøre for forskningsdesign, datainnsamling, utvalg av informanter og gjennomføring av arbeidet med mål om å sikre kvalitet. Jeg har under arbeidet hatt fokus på å sikre kvalitet i studien og gjennomgått etiske refleksjoner som har vært viktige for oppgavens utforming.

5.1 Studiens formål

Bakgrunn for studien var et ønske om å få innsikt i hvordan systemet rundt datalagring og eierskap til egne data fungerer i norske kommuner. Kommunal sektor ble valgt ettersom de forvalter data på vegne av svært mange innbyggere, dataen er svært variert og de er ansvarlige for svært mange tjenester ut til befolkningen. Store mengder av denne dataen kan antas å være persondata, men en kommune vil også generere svært mange andre data som det potensielt kan være interessant å beskytte. Jeg hadde også en antakelse om at det ville være store variasjoner i kompetanse og ressurser i kommunene, som kunne påvirke arbeid med skytjenester og igjen datasuverenitet.

5.2 Kvalitativ forskningsmetode

Kvalitativ forskning brukes for å studere hvorfor noe skjer, i mindre utvalg (Krumsvik, 2015, s. 27). Ved kvalitativ forskning måler man et kjent fenomen, ved å undersøke fenomenet i sin naturlige kontekst, og/eller undersøke hvordan informanter opplever konteksten og fenomenet. I denne studien undersøkes datasuverenitet som fenomen i kommunens arbeid med skytjenester som kontekst.

Hovedmålet for den kvalitative forskeren er å få et innsideperspektiv på et fenomen, av hvordan individene tolker omverdenen (Krumsvik, 2015, s. 25). I denne studien er det derfor blitt intervjuet ansatte i kommunen som har en opplevelse eller formening av hvordan kommunen arbeider med skytjenester.

5.2.1 Abduktivt forskningsdesign

Studien anvender et abduktivt forskningsdesign. Et abduktivt design fokuserer ikke på generalisering til populasjon, men er opptatt av generalisering av teori (van Hoek et al., 2005,

s. 138). Det gjøres gjennom å tolke og kontekstualisere individuelle fenomen innen et rammeverk, for å forstå et fenomen på en ny måte innenfor dette rammeverket (van Hoek et al., 2005, s. 138).

Fordi det mangler konsensus om datasuverenitet som fenomen, var det nødvendig å gjøre en gjennomgang av eksisterende forskning for å etablere et rammeverk til bruk i oppgaven. De utvalgte artiklene ble valgt på grunn av kobling til informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet generelt, eller skytjenester spesielt. Innledningsvis er gjennomgangen fokusert rundt definisjoner av datasuverenitet, variasjoner mellom definisjonene, og hvordan disse kan skilles fra liknende begrep.

Hummel og kollegers gjennomgangsartikkel ble viet mye plass, ettersom de har gått gjennom 341 publikasjoner med fokus på å differensiere datasuverenitet, digital suverenitet og cybersuverenitet. Gjennomgangen viser til mangel på enighet om begrepets innhold, men viser samtidig til hvilke aktører, kontekster og verdier begrepet som oftest benyttes sammen med, og som på en eller annen måte relateres til en form for kontroll over og eierskap til data.

Artikkelen fungerte derfor som et utgangspunkt, sammen med definisjonsgjennomgangen, for å identifisere karakteristikker for datasuverenitet som ville være aktuelle for bruk rundt skytjenester. Fordi artikkelen også tar for seg vinklinger som ikke er relevant for arbeid med skytjenester i virksomheter, ble det nødvendig å lage en egen karakteristikk-oversikt som luket ut irrelevant informasjon. Eksempelvis ble datasuverenitet i lys av urbefolkningers rettigheter, eller sosiale bevegelser, utelatt fra de endelige karakteristikkene, da de ikke er relevante for hvordan en ordinær virksomhet, slik som kommuner, organiserer sitt arbeid med datasuverenitet på generelt nivå.

Utviklingen av karakteristikker og underkarakteristikker var også nødvendig fordi begrepet og fenomenet datasuverenitet fortsatt er relativt ukjent, og det antakelig eksisterer forståelser som ikke samsvarer helt med forståelsen lagt til grunn i denne oppgaven. Ved å benytte karakteristikker og underkarakteristikker kunne dermed de samme forholdene undersøkes, selv om informantene ikke hadde kjennskap til datasuverenitet på forhånd.

5.2.2 Case-studie

Selv om kvalitative data ikke kan tallfestes, er kvalitativ forskningsmetode svært egnet til å undersøke dybdeperspektiv (Krumsvik, 2015, s. 25). I denne studien er målet å undersøke fenomenet datasuverenitet i dybden i en gitt kontekst, som er et fenomen uten klar definisjon. Begrepet er derfor brutt ned i ulike karakteristikker som ofte beskrives i sammenheng med

begrepets definisjoner, for å danne et teoretisk rammeverk. Studien er derfor utformet som en case-studie med abduktiv logikk med mål om å danne en grundig forståelse for konseptet datasuverenitet i kommunens arbeid med skytjenester.

En case-studie er «en empirisk undersøkelse som undersøker moderne fenomen («casen») i dybden og innenfor den ekte konteksten, spesielt når grensene mellom fenomen og kontekst ikke nødvendigvis er tydelig» (Yin, 2014, s. 16, egen oversettelse).

I denne studien er det datasuverenitet ved bruk av skytjenester i én spesifikk kommune, som undersøkes. Kommunens arbeid med skytjenester vil både være kontekst for datasuvereniteten, men også del av fenomenet som studeres via informantene. På grunn av det manglende rammeverket, og behov for å utvikle dette selv for å etablere det abduktive forskningsdesignet, måtte det også settes en begrensning for oppgaven til å kun se på én kommune. Dette fordi utformingen av oppgavens teori opptok mye av tiden, som ledet til at case-studie ble valgt som undersøkelsesmetode. Dersom det allerede hadde eksistert et rammeverk og felles forståelse for datasuverenitet som begrep, ville det derimot vært mulig å utvide oppgaven til å omfatte flere kommuner med sikte på empirisk generalisering. Istedenfor sikter denne oppgaven på å se datasuverenitet som et fenomen i dybden i én case, i lys av det norske systemet.

I en strategisk caseutvelgelse ligger det potensiale for å avgrense et fenomen, velge konteksten det skal studeres i, og koble dette til et teoretisk potensiale. Det er dermed en underliggende ambisjon om å «utvikle konsepter, modeller og teori istedenfor å forklare fenomen med referanse til eksisterende konsepter, modeller og teorier» (Antonsen & Haavik, 2012, s. 71, egen oversettelse). Denne tilnærmingen er passende for datasuverenitet, fordi datasuverenitet ikke er forsket mye på tidligere, og spesielt ikke i norsk kontekst om skytjenester. Det er derfor viktig å gå i dybden før en generaliserer, fordi det her ikke eksisterte nødvendige forutsetninger for å generalisere ut fra teori.

Case-studien er derfor konsentrert rundt én kommune som er del av det norske systemet. I arbeidet har det vært nyttig å ha andre referansepunkter for å speile funnene, og det er derfor inkludert informanter fra en annen kommune, samt en rådgivende organisasjon.

5.3 Fremdrift i forskningsprosjektet

Den følgende tabellen vil nokså detaljert beskrive hvordan forskningsprosessen har vært. Prosessen har ikke vært lineær, og det har blitt endret fokus samt arbeidet med de forskjellige komponentene av prosjektet om hverandre.

Tabell 3. Oversikt over fremdrift i forskningsprosjektet

Når	Hva ble gjort	Mål	Utfordringer og begrensninger
Januar	Søkte etter og leste gjennom eksisterende forskning på datasuverenitet, samt offentlige dokumenter. Sendte søknad til NSD. Startet å ta kontakt med potensielle samarbeidskommuner.	Danne forståelse for datasuverenitet som konsept.	Oppdaget at det ikke er enighet om en forståelse for datasuverenitet som begrep. Måtte derfor utforme oppgaven slik at jeg selv skapte teoridelen av oppgaven, ved bruk av eksisterende forskning med varierende forståelser og definisjoner.
Februar	Fortsatte lesing om datasuverenitet. Utarbeidet problemstilling og intervjuguide og gjennomførte møte med potensiell samarbeidskommune.	Danne grunnlag for start av datainnsamling	Hørte ikke noe fra kommunen fra møtet i etterkant, og måtte derfor ta kontakt med andre kommuner.
Mars	Fikk godkjent NSD-søknad. Etablert kontakt med ny kommune og startet intervjuprosess der. Utviklet teoretisk rammeverk om datasuverenitet. Startet transkribering og påbegynt metode.	Etablere samarbeid med kommune. Samle inn data til oppgaven.	Måtte tilpasse intervjuguide og problemstilling til et nivå som gjorde at de kommunale deltakerne kunne bidra.
April	Gjennomførte møter og intervju med ny kommune, markedsaktør og rådgivende organisasjon. Transkribering.	Utfylle datagrunnlag med komplementerende aktører.	Måtte begrense antallet informanter til allerede gjennomførte intervju, på grunn av oppgavens tidsfrist. Besluttet derfor å gjennomføre studien som en case-studie.
Mai	Ferdigstilte transkribering. Kodet og tolket dataen, og skrev ferdig empiri. Fullførte oppgavens metodedel og startet på diskusjonen.	Sortere i datagrunnlaget og transformere dette til oppgavens empiridel.	Tidskrevende transkribering. Måtte omforme oppgavens empiridel for å bedre presentere dataen.
Juni	Fullførte oppgavens diskusjonsdel. Levering av førsteutkast i	Samle trådene og ferdigstille oppgaven.	Tidspress.

	begynnelsen av måneden. Brukte resten av perioden til å korrigere og rette, samt gjennomføre språkvask.		

Prosjektet ble i stor grad preget av at det tok lang tid å finne informanter, og at det videre arbeidet måtte tilpasses rundt når informantene var tilgjengelige. Tabell 3 er en forenklet versjon av fremdriften, og i realiteten ble prosessen karakterisert av mye frem og tilbake og tidvis kaotisk arbeid. Eksempelvis tok transkriberingen opp mye større del av perioden enn tenkt, som gjorde at det tok lenger tid før jeg fikk begynt på empirien og diskusjonen. Utfordringene som ble møtt underveis i prosjektet bidro til utformingen av den endelige oppgaven, da det var behov for endringer i hvert eneste steg.

5.4 Datainnsamling og triangulering

Datainnsamling viser til prosessen der observasjoner registreres, for så å bli samlet inn og tatt vare på. I denne studien anvendes semistrukturerte intervju og dokumentanalyse som datainnsamlingsmetode. Intervjuene er hovedbasisen for datainnsamling. Dokumentene er inkludert for å danne forståelse for en nasjonal tilnærming til skytjenester og datasuverenitet, og komplementerer intervjudataen ved å videre vise hvordan den nasjonale tilnærmingen påvirker kommunen lokalt.

Denne prosessen med å kombinere intervju og dokumentanalyse kan omtales som triangulering. I denne oppgaven vil triangulering følge hvordan Denzin beskriver begrepet, der det beskrives som å omhandle flere former for kvalitative metoder, slik som intervjuer og dokumentanalyse. Alternative forståelser av begrepet likner mer på «mixed methods», der både kvantitative og kvalitative metoder benyttes (Denzin, 2012, s. 82).

Den antatte fordelen med triangulering er å prøve å sikre dybdeforståelse for fenomenet som undersøkes. Å kombinere ulike metoder, empirisk materiale, perspektiver eller observanter har som formål å fungere som en strategi som tilfører bredde, dybde, rikdom og kompleksitet til en studie (Denzin, 2012, s. 82).

Dokumentene er i hovedsak benyttet for å få et utvidet systemperspektiv på hvordan tematikken utfolder seg på nasjonalt nivå, mens intervjuene har gitt innblikk i kommunen. Det er også fokusert på å få forskjellige perspektiv inn via intervjuene, ved å inkludere perspektiver fra både markedsaktører og rådgivende aktører. Informasjonen fra disse aktørene

vil være utfyllende for dataen fra de kommunale informantene, fordi de har arbeidet med eller for flere kommuner og individer enn det som er intervjuet i denne studien.

Jeg undersøkte også om studien skulle inkludere kommunale dokumenter, dersom det eksempelvis eksisterte strategier for informasjonssikkerhet, anskaffelser eller risikovurderinger tilknyttet skytjenester eller liknende felt. Det viste seg derimot at slike strategier ofte ikke eksisterte, var utdaterte eller var unntatt offentligheten. Jeg besluttet derfor å ikke inkludere kommunale dokumenter, men heller etterspørre kjennskap til om dette eksisterte i intervjuene.

I tabell 4 presenteres de utvalgte dokumentene.

Tabell 4. Utvalgte dokumenter fra offentlige kilder

Dokumentnavn	Type dokument	Opphav	Publisert år
Veileder i bruk av skytjenester til behandling av helse- og personopplysninger	Veileder	Direktoratet for e-helse	2020
Temarapport om norske datasentre og digital autonomi	Temarapport	NSM	2022
Sikkerhetsfaglige anbefalinger ved tjenesteutsetting	Temarapport	NSM	2020
Nasjonal strategi for bruk av skytjenester	Plan/strategi	Kommunal- og distriktsdepartementet	2016
Grunnprinsipper for IKT-sikkerhet 2.0	Råd og anbefalinger	NSM	2020
Nasjonal strategi for digital sikkerhet	Strategi	Justis- og beredskapsdepartementet Forsvarsdepartementet	2019
Landvurdering ved tjenesteutsetting av IKT-tjenester	Råd og anbefalinger	NSM	2019
Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data	Veiledning	European Data Protection Board	2020
Totalt antall dokumenter	8 dokumenter er inkludert i oppgavens empiridel		Dokumentene er fra perioden 2016-2022

Dokumentene er utarbeidet av offentlige aktører i både Norge og EU, og er en blanding veiledere, anbefalinger, rapporter og strategi. Hovedmålet med bruk av dokumentene er å undersøke om det finnes strategier eller vurderinger rundt skytjenester og datasuverenitet på et høyere systemnivå enn kommunene, som legger føringer for hvordan arbeidet i kommunene skal eller bør gjennomføres.

5.5 Semistrukturerte intervju

I studien er det brukt semistrukturerte intervju for å samle inn informasjon fra informantene. Et semistrukturert intervju er et intervju som er planlagt, men fleksibelt. Formålet med denne formen for intervju er å innhente beskrivelser av verdenen til informantene, for å videre kunne tolke meningen av et beskrevet fenomen (Kvale, 2012).

Intervjuguidene som brukes i intervjuene er basert på de kvalitative forskningsspørsmålene for å sikre god koherens i studien (Krumsvik, 2015, s. 125). Den kvalitative dataen som et slikt intervju henter inn, vil tolkes i lys av annen forskning eller teorier (Kvale et al., 2015). Intervjuguiden er derfor også basert på det teoretiske rammeverket utviklet i oppgavens teoridel, slik at å tolke svarene til teorien blir enklere å gjennomføre.

Semistrukturerte intervju følger prinsippene «scripting», der intervjuguiden fungerer som en skisse over tema, emne og forslag til spørsmål, og «tunneling», der generelle spørsmål blir fulgt opp av mer konkrete spørsmål (Krumsvik, 2015, s. 125). Fordi datasuverenitet er et lite brukt begrep i Norge, er det nødvendig å undersøke fenomenet ved bruk av andre formuleringer og begrep som er tilknyttet datasuverenitet som underkarakteristikker, og derfor mer kjent. Dermed var det behov for å kunne følge opp innspill og tanker fra informantene om nærliggende felt og erfaringer. Det ga også mulighet for å klargjøre hva informanten mente med ulike kommentarer og opplevelser.

5.5.1 Informanter og intervjugjennomføring

Informantene i denne studien er utvalg som del av et strategisk utvalg. Informantene er valgt ut på basis at de enten har kjennskap til eller er ansvarlig for skytjenester i en kommune, eller tilbyr skybaserte tjenester for salg, eller tilhører en organisasjon med rådgivende funksjon for norske kommuner.

En oversikt over informantene er presentert i tabell 4.

Tabell 5. Informanter

Informantkode	Stilling	Arbeidsplass	Intervjuform

Informant A	IKT-rådgiver	Hovedkommune	Fysisk
Informant B	Personvernombud	Hovedkommune	Fysisk
Informant C	Digitaliseringsrådgiver	Hovedkommune	Fysisk
Informant D	Kommunalteknikk, systemansvarlig	Hovedkommune	Fysisk
Informant E	Driftssjef IKT	Hovedkommune	Fysisk
Informant F	Seksjonsleder kommunalteknikk, systemeier	Hovedkommune	Fysisk
Informant G	Rådgiver velferdsteknologi	Hovedkommune	Fysisk
Informant H	Prosjektleder velferdsteknologi	Hovedkommune	Virtuelt
Informant I	Head of Strategic differentiation programs	IT-selskap	Virtuelt
Informant J	Personvernombud/IKT-rådgiver	Kommune 2	Virtuelt
Informant K	Utviklingsleder	Kommune 2	Virtuelt
Informant L	Daglig leder	Rådgivende organisasjon for kommuner	Virtuelt
Informant M	Sikkerhetsanalytiker	Rådgivende organisasjon for kommuner	Virtuelt

Det var et mål å rekruttere informanter med ulike roller og erfaringsnivå fra forskjellige områder i kommunen, for å få et mest mulig balansert informantutvalg. Ingen av de kommunale informantene hadde detaljert kjennskap til datasuverenitet som konsept, men har innsikt i en eller flere skybaserte løsninger, eller en oversikt over liknende prosesser. Det var ikke et kriterium at informantene skulle ha tekniske stillinger eller inngående forståelse for skytjenester som system, dette fordi karakteristikkene til datasuverenitet i mindre grad går innom den faktiske tekniske utformingen.

5.5.1.1 Bakgrunn for informantutvalg

Informant A til H er ansatt i en kommune med rundt 25.000 innbyggere som beskriver seg selv som en mellomstor kommune. Kommunen har betydningsfulle mengder industri og næringsliv innenfor sine grenser. Kontakt med kommunen ble opprettet gjennom mail, og jeg kjenner til kontaktpersonen (informant B) via tidligere kort arbeidsforhold som kollegaer. Kommunen stilte med åtte informanter fra forskjellige avdelinger i kommunen. Det var fokus på å få representanter fra forskjellige avdelinger og nivå i kommunen, med varierende IKT/IT-kompetanse og lengde på ansettelsesforhold.

Innledningsvis var det tenkt at studien ville gjennomføres som en case-studie av informanter kun fra denne kommunen. Etter samtaler med og ønsker fra informanter, veileder og øvrige kontaktpersoner, ble det bestemt å inkludere informanter fra én til kommune, en rådgivende organisasjon og en markedsaktør for å gi øvrige referanser til funnene fra hovedkommunen.

Informant J og K er ansatt i en mindre kommune med rundt 10.000 innbyggere. Kommunen har betraktelig mindre driftsavdeling enn hovedkommunen i denne oppgaven, og har i mindre grad industri og næringsliv i kommunen. Kontakten ble opprettet via mail med informant J.

Informant I arbeider i et privat firma, som tilbyr IT- og produktutviklingstjenester, som er spesialisert innen sky, data og programvare. Jeg tok kontakt med informanten direkte på LinkedIn, fordi hun i lys av sin rolle i selskapet hadde skrevet artikler i diverse nettaviser om datasuverenitet og selskapets tilbud av skytjenester for å sikre datasuverenitet. Informant I er inkludert for å gi innsikt i en markedsaktørs perspektiv på bruk av skytjenester i det offentlige, samt å gi et inntrykk av hvordan deres kommunale kunder tilnærmer seg problemstillinger rundt datasuverenitet. Fordi selskapet informant I tilhører aktivt bruker begrepene datasuverenitet og digital suverenitet i sitt arbeid, ble det inkludert spørsmål om forståelse av disse begrepene i intervjuguide for denne informanten.

Informant L og M tilhører et rådgivende selskap for kommuner. Selskapet er et medlemsbasert interkommunalt selskap for norske kommuner, som er etablert som en nasjonal ressurs for norske kommuner og fylkeskommuner. Formålet med selskapet er å bidra med rådgivning og relevant informasjon til medlemskommunene om informasjonssikkerhet. Selskapet er inkludert for å inkludere rådgivende organ for norske kommuner, og få innblikk i deres mer generelle erfaringer med skytjenester i norske kommuner, fra et sikkerhetsperspektiv.

Etter samtale med veileder ble det besluttet å anonymisere tilhørighet og navn på alle informanter, også de som hadde spesifisert at dette ikke var nødvendig. Dette fordi det ikke er den spesifikke kommunen, bedriften eller organisasjonen som er interessant, men kommunen som en kontekst og del av et større system.

5.5.1.2 Forberedelser: intervjuguide og informasjonsskriv

For å sikre at intervjuguiden og medfølgende spørsmål var på rett nivå for ønskede informanter, ble det gjennomført en samtale med min kontaktperson i kommunen. Jeg forklarte hva jeg ønsker å se på i mer dybde enn tidligere presentert per mail, og hvem jeg tenkte meg kunne være aktuelle å intervjue. Vi konkluderte med at det antakeligvis ville være nyttig med et litt mer generelt og forenklet fokus enn originalt tenkt, for at informanter på forskjellige nivå i kommunen skulle kunne bidra.

Det ble så utviklet en intervjuguide som kunne brukes til intervju med forskjellige kommunale informanter, så lenge de hadde innsikt i en eller flere skytjenester, eller arbeid med disse i kommunen.

Fordi denne første intervjuguiden, se vedlegg 1, ble utformet for å undersøke roller, organisering og tjenester i kommunen direkte, var det behov for å utvikle egne intervjuguider for informanter som ikke var kommunale.

Spørsmålene i den originale intervjuguiden ble derfor omstrukturert til en andre guide der markedsaktørene kunne svare for samme opplevelser på vegne av sine kunder og erfaringer, se vedlegg 2. I tillegg ble det utviklet en tredje intervjuguide for rådgivende organisasjoner, der de kunne svare på erfaringer fra sine medlemmer, se vedlegg 3.

Alle informantene fikk utsendt intervjuguiden på forhånd av intervjuene, slik at de kunne forberede seg og eventuelt søke opp mer informasjon før intervjuene ble gjennomført. Sammen med intervjuguiden ble informasjonsskriv med samtykkebekreftelse fra NSD sendt ut til signering, se vedlegg 4. Informasjonsskrivet inneholdt i tillegg til samtykkeerklæring, informasjon om prosjektet og hvorfor de var ønsket som informant.

Fordi datasuverenitet er et nokså ukjent begrep enda i Norge, ble det besluttet å utelate begrepet i sin helhet fra intervjuene med de kommunale informantene. Dette fordi problemstillingen kunne besvares med å spørre informantene om underkarakteristikker, som er mer gjenkjennelige. I informasjonsskrivet ble det derfor forklart at selv om oppgaven ser på

datasuverenitet i forbindelse med skytjenester, så ville det ikke være nødvendig for informantene å ha kjennskap til datasuverenitet som fenomen og begrep,

5.5.1.3 Gjennomføring og intervjusituasjon

Intervjuene ble gjennomført i perioden 22. mars til 27. april 2022. Totalt ble det gjennomført 12 intervjuer, der siste intervju inkluderte 2 informanter. Totalt inkluderer derfor prosjektet 13 informanter.

Underveis i intervjuene ble det stilt oppfølgende spørsmål der dette var relevant for prosjektet. Etter de første intervjuene ble det også inkludert øvrige spørsmål som var oppklarende for studiens fokus, eksempelvis angående eksterne ressurser tilgjengelig for kommunen.

Intervjuene ble gjennomført både med fysisk tilstedeværelse og via Teams, se tabell 4. For de intervjuene som ble gjennomført fysisk ble dette gjort på informantenes arbeidsplass.

5.6 Transkribering, datareduksjon og NVivo 12

Datareduksjon er nødvendig ettersom ikke alt i intervjuene og de innsamlede dokumentene vil være nyttig for å besvare oppgavens forskningsspørsmål og problemstilling.

Alle intervju ble transkribert før datareduksjonen. Under transkriberingen ble muntlige fyllord som «eeeh», «mhm», «ja», «ok» som kom underveis i intervjuet, utelatt dersom de ikke tilførte verdi til intervjukonteksten. Transkriberingen ble gjennomført ved hjelp av dataprogrammet Express Scribe. Express Scribe er en transkriberingssoftware for ikke-kommersiell bruk, som ikke krever lisens. Dataene lagres lokalt på utvalgt pc. Programmet er nyttig fordi det muliggjør spesialtilpassing av hurtigtaster for spoling, sette talefart raskere eller treigere, stopp og start. Videre er det mulig å bruke disse hurtigtastene selv om man har andre programmer åpne, slik som Microsoft Word.

Selve transkriberingen ble skrevet inn i individuelle Word-filer for hver informant. Filene ble merket med informantens tildelte bokstav, dato for intervju, lengde for intervju totalt og antall ord når ferdig transkribert.

Innledningsvis i datareduksjonen ble dataen kategorisert etter forskningsspørsmålene.

Det ble besluttet å benytte programmet NVivo 12 for å sortere i og redusere dataen videre. NVivo 12 er en software som brukes til lagring, håndtering og analysering av kvalitativ data (Kristi Jackson & Bazeley, 2019, s. 3).

I tabell 5 er kodene brukt til datareduksjon oppsummert.

Tabell 6. Koder brukt til datareduksjon i NVivo 12

Knyttet til forskningsspørsmål	Overordnet kode i NVivo 12	Underordnet kode i NVivo 12	Hensikt
1	Organisering av skytjenester	(ingen)	Generell innsikt i organisering av arbeid med skytjenester
1	Organisering av skytjenester	Strategier - lokale - nasjonale	Undersøke om det eksisterer relevante strategier nasjonalt eller lokalt
1	Organisering av skytjenester	Opplæring og erfaring	Opplæring og eventuell erfaring hos kommunalt ansatte
1	Organisering av skytjenester	Interne ressurser	Hvilke interne ressurser kommunen har på skytjenester
1	Organisering av skytjenester	Eksterne ressurser	Hvilke eksterne ressurser kommunen har på skytjenester
1	Organisering av skytjenester	Arbeidsprosess ved ny skytjeneste	Innsikt i arbeidsprosess og eventuelle rutiner ved ny skytjeneste og hvilke faktorer som vektlegges i dette arbeidet
2	Karakteristikker ved datasuverenitet	Verdier - Makt - Kontroll Hvor er dataen? Tilgangsstyring? Eierskap	Undersøke hvilke(n) aktør informantene opplever å ha makt over skytjenester og datasuverenitet. Undersøke om informantene opplever kontroll over hvor dataen befinner seg, tilgangsstyring og hvem som eier dataen.
2	Karakteristikker ved datasuverenitet	Data - Dataklassifisering Persondata vs andre data - Datatype - Kollektiv vs individuell dimensjon	Hvilke data kommunene behandler i sky og hvordan disse klassifiseres og differensieres basert på datatype
2	Karakteristikker ved datasuverenitet	Kontekst - Lovgivning Jurisdiksjon	Datasuverenitet sett i kontekst av lovgivning, og jurisdiksjon, og IT-arkitektur som påvirkes av aktørsammenspill

		- IT-arkitektur Private vs offentlige aktører Avhengigheter	
2	Karakteristikker ved datasuverenitet	Håndtering - Ledelsesstrategi - Virkemidler Interne Eksterne	Hvilken ledelsesstrategi og hvilke virkemidler kommunen bruker for å oppnå datasuverenitet
2	Karakteristikker ved datasuverenitet	Utfordringer	Hvilke utfordringer kommunene opplever i forbindelse med å ha kontroll over og rettigheter til egne data

I tabellen vises det kobling mellom forskningsspørsmål, overordnet kode og underordnet kode i NVivo 12. Kodene tilknyttet forskningsspørsmål 1 er utarbeidet med formål om å få innsikt i organiseringen av skytjenester i kommunene, og er basert på spørsmålene fra intervjuguiden. Kodene tilknyttet forskningsspørsmål 2 er basert på karakteristikkene for datasuverenitet, med tilhørende underkarakteristikker, som ble utarbeidet i oppgavens teoridel.

Bruk av NVivo 12 gjorde det mulig å sammenlikne svar på enkelte spørsmål fra informantene, samt fra tekstdokumenter, på en systematisk måte. De transkriberte dataene fra intervju, samt innsamlede dokumenter, ble redusert i NVivo 12 ved hjelp av koding basert på fastsatte tema. På denne måten vil alle svar eller funn relatert til ett tema, vise under samme søk. Programmet effektiviserte dermed datareduksjonen ved å fremstille relevant informasjon samtidig, som gjorde det lettere å holde oversikt, se trender og sammenlikne informasjon.

5.7 Kvalitetskriterier

I de følgende delkapitlene vil oppgavens kvalitetsmessige styrker og svakheter gjennomgås. Det vil redegjøres for reliabilitet, validitet og overførbarhet, samt en gjennomgang om hvordan studien er lagt opp for å sikre etisk forsvarlighet. Til slutt vil studiens metodiske styrker og svakheter belyses.

5.7.1 Reliabilitet

Reliabilitet handler om studiens pålitelighet, og er knyttet til selve fremgangsmåten bak datainnsamlingen (Leseth & Tellmann, 2014, s. 25). Reliabilitet deles inn i intern og ekstern reliabilitet. Intern reliabilitet dreier seg om i hvilken grad andre forskere kan anvende samme metode for å analysere data, som den opprinnelige forskeren (Krumsvik, 2015, s. 158). For å sikre intern validitet i denne studien er det gitt innsyn i forskningsstrategien, fremgangsmåte for innsamling, bruk av tekniske virkemidler til opptak av intervju for å sikre nøyaktig transkribering, reduksjon og kategorisering av data ved bruk av NVivo 12, og metodiske valg som er gjort i løpet av studien. Dette gir leseren innsikt i hvordan min forskningsprosess har foregått.

Ekstern reliabilitet viser til om andre forskere kunne ha gjenskapt resultatene, dersom de anvendte samme metode (Krumsvik, 2015, s. 158). I kvalitativ forskning vil det derimot ikke være mulig å gjenta en studie, og få nøyaktig de samme resultatene. Dette skyldes at fremgangsmåten til forskeren vil påvirke selve forskningsprosessen. Denne utfordringen kan møtes ved at forskeren gjør rede for selve forskningsprosessen, og hvordan datamaterialet er utviklet (Leseth & Tellmann, 2014, s. 22-23), slik som gjøres i denne oppgavens metodedel. For å styrke den eksterne reliabiliteten er det derfor fokusert på å gi innsikt i det teoretiske rammeverket og hvordan dette ble utarbeidet som et grunnlag for oppgavens videre analyse. Videre er det gitt innsikt i utvalget av informantene og intervjusituasjonen. Muligheten til å gjenskape resultatene vil påvirkes av de utvalgte informantenes erfaringer og forståelser, deres opplevelse av intervjuprosessen, og mine tolkninger av deres svar. Det er derfor også søkt å inkludere variasjon i informantenes arbeidsområder, samt å inkludere markedsaktør og rådgivende organisasjon med breiere erfaring.

5.7.2 Validitet

Validitet i kvalitativ forskning omhandler om en har undersøkt det som en ønsket å undersøke (Krumsvik, 2015, s. 151). Validiteten er rettet mot tolkningen av dataen (Leseth & Tellmann, 2014, s. 25), og validiteten er derfor avhengig av at informasjonen vi henter inn er troverdig, den er mulig å bekrefte, og at den har overføringsverdi (Krumsvik, 2015, s. 152).

Validitet kan deles inn i indre og ytre validitet. Indre validitet omhandler om den innsamlede dataen svarer til intensjonen med undersøkelsen (Leseth & Tellmann, 2014, s. 24), altså om funnene samsvarer med virkeligheten, og dermed om de er gyldige for det utvalget eller fenomenet som studien har undersøkt (Krumsvik, 2015, s. 152). Oppgavens problemstilling og intervjuguide ble utviklet til det valgte fokuset, og tilpasset til et passende nivå, etter

samtaler med både aktører som jobber med skytjenester og informasjonssikkerhet (ikke inkludert som informanter), og ved samtale med kontaktperson i hovedkommunen som undersøkes. Dette sikret at informasjonen samlet inn fanget opp det som var ønsket med undersøkelsen, fordi informantene hadde mulighet til å svare på spørsmålene selv om de ikke kjente til datasuverenitet fra før. Likevel vil dataen samlet fra de kommunale informantene bli preget av den enkelte informants opplevelse av forhold i egen kommune, og det vil i noen tilfeller være vanskelig å skille mellom informantens opplevelse og faktiske forhold.

Ytre validitet omhandler om man kan generalisere resultatene til andre situasjoner og utvalg som likner den studien er gjennomført i (Krumsvik, 2015, s. 152). Case-studier beskrives ofte som å ha begrenset verdi om hensikten med studien er å generalisere. Det er derimot ikke statistisk generaliserbarhet, men en teoretisk representativitet (Andersen, 2005, s. 14) denne studien har som mål. Det er mer naturlig å ha empirisk generalisering som mål i en fremtidig studie som ser på de samme forholdene i flere kommuner, når et teoretisk rammeverk allerede eksisterer. I denne studien er målet å få et dypere blikk inn i datasuverenitet i én kontekst, på bakgrunn i det teoretiske rammeverket som er utviklet i løpet av studien. Dette kan potensielt danne grunnlag for en videre studie med breiere omfang.

5.7.3 Etiske refleksjoner

Forskning er kontekstuell, og vil bli påvirket av valgene som forskeren gjør i løpet av hele forskningsprosessen (Leseth & Tellmann, 2014, s. 189). Det er derfor viktig med åpenhet i ethvert forskningsprosjekt, for å kunne vurdere funnenes gyldighet. Dette er spesielt viktig i kvalitativ forskning som ikke benytter seg av standardiserte teknikker for datainnsamling og analyse (Leseth & Tellmann, 2014, s. 189). Funnene i denne studien vil være påvirket av mitt teoretiske perspektiv, metoden jeg har valgt som fremgangsmåte, og konteksten prosjektet har vært plassert i, både tidsmessig og rom.

For å gi mulighet for kritisk refleksjon rundt min prosess og funn, vil jeg derfor presentere noen etiske refleksjoner som er gjort underveis i studien. Det er likevel viktig å påpeke at denne studien ikke vil lede til noen objektive sannheter, men vil være påvirket av både meg som forsker, samt informantene og situasjonen rundt dem.

For å sikre at datagrunnlaget basert på intervjuene ble så nøyaktig som mulig, ble intervjuene tatt opp og intervjuene transkribert nøyaktig. Det ble derfor nødvendig å sende inn søknad til NSD for å behandle personopplysninger. NSD definerer personopplysninger som «… enhver opplysning som kan knyttes til en person. Eksempler er fødselsnummer, navn eller e-

postadresse/IP-adresse. Stemme på lydopptak regnes også som en personopplysning» (NSD, u.å.). Den endelige godkjenningen fra NSD ble gitt 2 mars 2022, se vedlegg 5. Samtykkeskjema medfulgte i informasjonsskriv til informantene. Informasjonsskrivet inkluderte informasjon om prosjektet og deres rettigheter som informant, se vedlegg 4.

Informantenes navn ble knyttet til en bokstav, og denne oversikten ble lagret separat i eget system, borte fra transkribering og andre oversikter. I transkriberingen ble kun informantens bokstavkode inkludert i dokumentet. Lydopptak og transkribering medførte nøyaktig gjengivelse av informantenes svar på spørsmålene, samt at jeg kunne gå tilbake til punkter jeg var usikker på.

Informantene fikk under intervjuet tilbud om å få tilsendt sitatsjekk, eventuelt full transkribering. De som ønsket dette, fikk dette tilsendt per mail. Det ble avklart med informantene om de ønsket full anonymisering også av stillingstittel/rolle, og at dette også kunne endres i etterkant av intervjuene.

5.7.3.1 Forholdet mellom forsker og informant

Under intervjuene og kommunikasjon med informantene var jeg opptatt av å være bevisst på min rolle som forsker i denne studien. Ved å ta i bruk båndopptaker sikret det at min rolle som intervjuer fikk fullt fokus, slik at andre relevante spørsmål kunne følges opp og respons gis til informantene. Det tillot også at jeg kunne være mer til stede og avslappet under intervjuene, uten å stresse over å måtte skrive ned alt informantene sa. Dette medfulgte også at datagrunnlaget ble mest mulig nøyaktig ved transkribering. En uventet fordel med å ta opptak var at jeg fikk innsikt i egen opptreden og gjennomføring av intervjuene under transkribering, slik at jeg kunne forbedre dette til neste intervju. Eksempelvis oppdaget jeg etter de første intervjuene at jeg kom med unødvendig mange bekreftende kommentarer, for eksempel «mhm», og «ja» underveis. Dette forsøkte jeg å begrense i de kommende intervjuene, for å gi informanten mer plass uten avbrytelser.

Studien var preget av at flesteparten av informantene ikke er eksperter innenfor IKT/IT generelt, eller skytjenester spesielt. De kommunale informantene i denne studien har forskjellige roller i ulike fagavdelinger i kommunen, og har dermed varierende, og som oftest lav, erfaring med eller kompetanse innen skytjenester. Dette kunne ha ført til at informantene følte seg utilpass eller uegnet til å delta i studien. For å unngå dette ble intervjuguiden sendt til min kontaktperson i forkant av intervjuene, for å sikre at det tekniske nivået var passende for

de kommunale informantene, på en måte som tillot dem å delta og dele egne erfaringer sett fra eget kompetansenivå.

Fordi det overordnede temaet om datasuverenitet for oppgaven ville oppleves ukjent for de fleste av informantene, ble det poengtert i informasjonsskrivet (vedlegg 4) at det ikke var nødvendig å ha inngående kjennskap til datasuverenitet for å kunne bidra i studien, og at det kun krevdes erfaring med skytjenester i kommunen.

Flere av informantene uttrykket før starten av intervjuet at de var usikre på om de ville kunne bidra med interessant informasjon på grunn av manglende kompetanse, etter å ha lest gjennom informasjonsskrivet og intervjuguiden i forkant av intervjuet. Ved uttrykkelse av dette ble det brukt tid på å presisere at alle bidrag var nyttige, samt at dersom de ikke hadde et svar på et spørsmål, så gikk dette fint. Likevel viste det seg at alle som hadde denne bekymringen, hadde viktige og gode bidrag til studien.

Jeg anser også anonymisering av informantene samt tilbud om sitatsjekk som viktige tiltak for å sikre at informantene var komfortable med å dele informasjon, ettersom temaet datasuverenitet potensielt kunne ført til at de utleverte informasjon om at arbeid med sikkerhet rundt data ikke blir fulgt opp godt nok. Ved å sikre anonymitet og eventuelt at jeg tok bort sitater de selv ønsket, ønsket jeg å oppnå at de ikke var preget av flauhet eller skam overfor manglende rutiner eller mangelfull praksis. Dette opplever jeg under intervjuene at gikk svært bra, da informantene delte både positive og negative erfaringer både om egen kunnskap og praksis, og opplevelse av kommunen som system.

Det opplevdes som fordelaktig at de fleste av de kommunale informanten var i et kjent miljø under intervjuene, og at dette bidro til en avslappet stemning. Fire av intervjuene ble gjennomført på Teams på grunn av avstander til informanten, og ett ble gjennomført på Teams på informantens ønske. Tre av disse informanten var derimot ikke-kommunale informanter, som kan anses som eksperter på feltet. Det opplevdes som uproblematisk å gjennomføre intervjuene virtuelt, trolig fordi de fleste har blitt mer erfarne med dette i løpet av pandemien.

Alle intervjuene ble satt til tidspunkter som informantene selv definerte eller oppgitte som ledig, for å gjøre det mest mulig lettvint for informantene å delta. Intervjuene ble tatt opp digitalt for å sikre nøyaktig transkribering.

6. Empiri

I empirien presenteres funn fra de 13 informantene og 8 dokumentene som beskrevet i metodekapittelet. Disse funnene vil i diskusjonen bidra til å svare på problemstillingen.

Kapittelet er strukturert rundt hovedtemaer som naturlig kom frem av dataen under koding i NVivo12. I tillegg til å danne et datagrunnlag for diskusjonen, vil også empirien svare på oppgavens første forskningsspørsmål:

«Hvordan er arbeidet med skytjenester organisert i kommunen, og hvilke faktorer vektlegges i dette arbeidet?»

Forskningsspørsmålet er et deskriptivt spørsmål som var nødvendig å besvare før oppgavens diskusjonskapittel vil kunne bli besvart.

6.1 Hvilke data lagres i kommunens skytjenester, og hvilke vurderinger gjøres i forkant av anskaffelsene?

Kommunen har en stor mengde systemer i sky, og disse omfatter alt fra datalagring på Chromebook (pc-type) i grunnskolen, brukeroversikter for hjemmebaserte tjenester, systemer for vann og avløp, til administrative økonomi- og e-mailsystem. Systemene lagrer data om alt fra sensitive personopplysninger til virksomhetskritisk informasjon og kritisk infrastruktur. Systemene blir levert fra både enorme globale markedsaktører som Google og Microsoft som tilbyr store skybaserte systemer, og mindre lokale aktører som leverer én spesifikk tjeneste. Det er dermed stor variasjon innad i kommunen i hvilke data som samles inn og lagres i skytjenester, og hvem denne dataen får betydning for.

I motsetning til dette har kommune 2 svært få tjenester i sky per dags dato, og en mindre IKT-avdeling.

6.1.1 Vurderinger brukt før overføring til, eller opprettelse av, data i skytjenester

Selv om det er stor variasjon i hvilken type informasjon kommunen lagrer i sine skytjenester, er det i varierende grad at dataklassifisering brukes for å få oversikt over hvilken type data det er som skal bli overført til, eller opprettet i, skytjenester, og hvordan typen data påvirker valg av tjeneste.

Flere av informantene er enten usikre på om det gjennomføres dataklassifiseringer, eller viser til at det i liten grad blir benyttet vurderinger slik som følsomhetsvurderinger,

dataklassifisering eller kategorier basert på konfidensialitet og kritikalitet, for å klassifisere data før en skytjeneste tas i bruk.

Gjennomføring av DPIA (Data Protection Impact Assessment) og risikoanalyser blir derimot nevnt av noen informanter som konkrete vurderinger som har blitt brukt i forbindelse med anskaffelse av nye skytjenester eller utvidelse av eksisterende løsninger, selv om dette er vurderinger som ikke i seg selv er dataklassifiseringer. Øvrig nevnes gjennomgang av forhold i databehandleravtale som en vurdering som skal gjennomføres. Både informant B (Personvernombud) og informant J (Personvernombud/IKT) viser derimot til at det ikke alltid er slik at de som personvernombud blir inkludert i anskaffelsen av nye systemer, og dermed opprettelse av eller gjennomgang av forhold i databehandleravtale, slik som det egentlig er ønskelig.

Informant L (Daglig leder, rådgivende org.) og informant M (Sikkerhetsanalytiker, rådgivende org.) viser til at de i liten grad har sett bruk av dataklassifisering i norske kommuner.

6.1.2 Forskjeller i kommunens arbeid med persondata VS øvrig data i skytjenester

Ved spørsmål om det arbeides likt eller annerledes dersom dataen som skal i skytjenester er personopplysninger eller ei, er et gjengående svar hos informantene at det er mer oppmerksomhet rundt personopplysninger enn øvrige data.

Kommunens ansvar for persondata knyttes både til å beskytte dataen, men også at innbyggerne skal ha rett til innsyn i egne data, uansett hvor mange system de er del av. Det trekkes derimot frem at jo flere skytjenester, spesielt fra forskjellige leverandører, som benyttes, jo mer tungvint vil det å få oversikt over data bli.

Informant M (Sikkerhetsanalytiker, rådgivende org.) kommer med innspill om koblingen mellom persondata og informasjonssikkerhet som støttes av informant L (Daglig leder, rådgivende org.), «[…] jeg har en følelse av kommunene faktisk er flinkere på personvern, enn de er på informasjonssikkerhet.». Innspillet begrunnes i fokus på personvern etter personvernforordningen kom, og samsvarer med informantenes inntrykk av at det er stort fokus på personvern ved bruk av skytjenester.

Derimot peker informant A (IKT-rådgiver) på at vilkårene i databehandleravtalen for systemet hen er involvert i, skal gjelde alle data som settes i skytjenesten, og dermed at «data er data». Det vil si at de samme sikkerhetstiltakene skal gjelde for alle data som databehandler er

ansvarlig for. Dette inntrykket forsterkes av de øvrige informantene da databehandleravtale, som videre vil ses på under punkt 6.2.2, presiseres som det viktigste virkemiddelet for å sikre kontroll over data generelt.

Informant F (Seksjonsleder, kommunalteknikk) er trekker på den andre siden frem betydningen av å ha data om kritisk infrastruktur i skytjenester, og hens opplevelse med at det er få retningslinjer på nasjonalt nivå om hvordan kommunene skal organisere arbeid med den kritiske infrastrukturen og tilhørende data som potensielt lagres i skytjenester, som følger hans felt:

> I forhold til IT-sikkerhet så har jo elkraft, har jo sånn 150 siders manual med en god del krav. Hos oss [vann og avløp] så står det to linjer at vannverkseier skal vurdere hvilke tiltak som skal settes i gang. Og da er det opp til hver enkelt kommune, å finne ut hva de skal gjøre, hvordan skal de gjøre det, hva er hensiktsmessig, hva er ikke det. Og da er det sånn «ja hvem gjør den vurderingen her da?». Er det IT, eller er det noen på VA eller hvor er grensesnittet, og hvor legger man energien? (Informant F, seksjonsleder, kommunalteknikk).

Informant I (IT-selskap) trekker på sin side frem at typen data det er snakk om, burde påvirke valg av skytjeneste i kommunen:

> […] hvilken type data som kan behandles eller lagres, eksempelvis persondata, sensitive data eller virksomhetskritiske data, da er vi inne på valget mellom hvilken type løsning. Om det er privat, hybrid eller offentlig skyløsning. I særlig kritiske data, som vi snakker om her nå, sensitive, så bør kommunene være helt sikre på at de har privat skytjeneste, eller on-premise, altså lokalt lagret løsningen med data lagret på lokal jord, inkludert alt av de metadataene som jeg også har snakket om. Det vil si andre, tredjepartssystemer og så videre, for å sikre at det ikke er noe lekkasje av den type data som ikke skal ut av de interne systemene. (Informant I, IT-selskap).

Her vises det altså til at dataklassifisering i stor grad bør påvirke de tekniske beslutningene rundt type skytjeneste.

6.1.3 Oppsummering

Empirien som har blitt presentert i denne delen viser til den store variasjonen i hvilken type data kommunen behandler og setter i skytjenester. Det trekkes frem økt fokus på kontroll av persondata som følge av innføring av GDPR, men presiseres samtidig at det oppleves som at det er manglende regelverk nasjonalt sett for kritisk infrastruktur. På den andre siden trekkes det frem at tiltak for å beskytte data, slik som databehandleravtale, benyttes for alle typer data, og ikke kun persondata.

Selv om kommunen behandler store mengder data som krever forskjellige sikkerhetstiltak, er det ikke brukt dataklassifiseringer for å karakterisere dataene og tilpasse skytjenesten ut fra dette, og i liten grad brukt andre vurderinger før skytjenestene tas i bruk.

6.2 Forholdet mellom tjenesteleverandør og kommunen

Informantene har både positive og negative opplevelser med de private aktørene som tilbyr skytjenester. Fordelene knyttes til frigjøring av drift hos kommunen og ekspertise hos leverandøren, mens ulempene knyttes til bruk av standardkontrakter og at kommunen må være bevisste på at egne krav blir ivaretatt før kontrakten skrives under.

Det blir trukket frem at det oppleves som en trygghet å benytte en av de store leverandørene, eksempelvis Google og Microsoft, fordi de i større grad oppleves som profesjonelle og at sikkerheten ved tjenesten er god. På den andre siden påpekes det også at det oppleves som at disse store aktørene til en viss grad prøver å tvinge folk over på skytjenester ved at flere av deres løsninger flyttes over i sky uten alternative løsninger. Likevel blir det påpekt at det som regel alltid er flere reelle konkurrenter når en skal anskaffe skytjenester, og at en derfor ikke må gå med på suboptimale forhold i kontrakter.

Videre trekkes det frem at bruken av disse private leverandørene er fordelaktig, fordi en unngår å måtte bruke mye tid og midler på vedlikehold av potensielt veldig små systemer, og derfor frigir driftstid i kommunen.

En annen utfordring med anskaffelser av skylagring er at skylagring som tjeneste ofte blir solgt med standardvilkår, som gjør det vanskelig å tilpasse tilbudet og vilkår i kontrakten. Informant M (Sikkerhetsanalytiker, rådgivende org.) eksemplifiserer dette i praksis for kommunene ved anskaffelse av skytjenester:

> Det er jo sånn at hvis kommunen kommer med en databehandleravtale som de har laget som de har med sine leverandører generelt, til Microsoft, så sier Microsoft «nei

> den her har vi signert for deg», som er deres egne databehandleravtale da, for kommunen. (Informant M, sikkerhetsanalytiker, rådgivende org.).

Informant L (Daglig leder, rådgivende org.) poengterer videre at dette samspillet kan påvirkes av flere faktorer: «Jeg tror det er lettere å gjøre det overfor lokale leverandører, og norske softwareleverandøren, enn det er for de store internasjonale».

Det blir poengtert av informant F (Seksjonsleder, kommunalteknikk) at kommunen har en viktig rolle ved å sette absolutte krav i dialogen med skyleverandøren, og det er viktig å følge opp leverandøren på ønskede tilpasninger. Hen opplever at for mange i kommunen tar til takke med det leverandøren har tilgjengelig allerede av kontrakter. Flere informanter påpeker derimot at kommunen potensielt ikke vet hva de kan forlange av leverandøren, hvordan en setter opp sikkerhetsløsninger eller hva som er en god datamodell, og at de derfor er avhengig av veiledning fra markedet og tjenesteleverandør.

6.2.1 Kommunens innsikt i tekniske aspekter hos leverandøren

Kommunen har liten innsikt i IT-arkitekturen til sine egne skytjenester, hverken om tjenestene er offentlige, hybride eller private, eller tilknyttet hvordan databehandler lagrer, flytter og sikrer dataen.

Informant C (Digitaliseringsrådgiver) viser til ett eksempel, ved overgang til Office 365 der en hybrid løsning ble benyttet for å flytte kommunens data gradvis over i sky. Prosessen ble opplevd som vanskelig med hensyn til hvordan arbeidet skulle gjøres, og hvordan det som skulle over i sky skulle bli flyttet med minst mulig konsekvenser.

Informant I (IT-selskap) påpeker behovet for rådgivere og sparringspartnere dersom kompetansen er lav på it-arkitektur.

> Altså selve implementeringen er ikke igangsatt av så stor skala enda, men forståelsen overordnet av skytjenester er ganske høy vil jeg si, i offentlig sektor. Men det er likevel behov for at, tilbake til behov for rådgivere og sparringspartnere og veiledning i mer den praktiske utvelgelsen av hvilke skytjenester som passer for hvilke formål, er fortsatt til stede. Naturlignok, fordi det er et veldig stort felt. Og det er klart at det er ulik kompetanse i ulike kommuner da, når vi snakker om kommuner og andre i

> offentlig sektor, som jo av den grunn har ulik kompetanse på skytjenester. (Informant I, IT-selskap).

Sitatet passer overens med svarene til de kommunale informantene, der de har kjennskap til skytjenestene generelt og hvordan systemet er utformet fra et fagperspektiv, men det er ikke tenkt på, eller mangler kompetanse til, å vurdere mer tekniske aspekter slik som den faktiske oppbyggingen av skytjenestene.

Informant A (IKT-rådgiver) og informant J (Personvernombud/IKT) viser til at store leverandører som Google og Microsoft har gitt innsikt i hvordan dataen krypteres og innsikt i at data lagres på forskjellige lokasjoner for å sikre back-up og vanskeliggjøre kopiering av fullt datasett. Flere av informantene viser til at det er forskjeller på leverandører, både når det kommer til innsyn, men også tjenestene som tilbys og opplevd sikkerhet ved løsningene.

6.2.1.1 Geografisk plassering av datasentre

Det er store forskjeller i hvor stor innsikt kommunen har i hvor datasentrene tilknyttet skytjenestene befinner seg geografisk. Flere av informantene trekker frem at dette skal være spesifisert i databehandleravtalen de har med leverandøren, uten å kunne presisere mer enn at det bør stå der. Det er likevel svært ulik grad av innsikt, selv der databehandleravtalene skal være på plass.

Informant A (IKT-rådgiver) viser til at Google som leverandør oppgir kart som viser alle datasentrene som benyttes, men at det ikke spesifiseres hvilke datasenter nøyaktig som benyttes. Det er likevel presisert at de kun skal lagre kommunens data innenfor EU, og at dataen splittes på mer enn ett datasenter. Informant J (Personvernombud/IKT) viser til et eksempel der leverandør varslet på forhånd, før flytte av datasenter til et annet land. Begge disse formene for innsikt er initiert av leverandøren, og krever ikke noe ekstra presisert i hverken kontrakt eller oppfølging av kommunen.

Informant H (Prosjektleder, velferdsteknologi) viser til at plasseringen av datasentrene skal avklares i anskaffelsesprosessen, men er usikker på om det er beskrevet av alle leverandører i besvarelse av anskaffelsen. Informant K (Utviklingsleder) viser til at typen informasjon som skal lagres i løsningen, og hvor sensitivt det er, vil påvirke kravene til lagringssted spesifisert i databehandleravtalen. Prosessen før skytjenesten tas i bruk er dermed et viktig steg for å sikre den innsikten kommunen ønsker.

Informant B (Personvernombud) har derimot inntrykk av at kommunen har for stor tiltro til leverandørene når det kommer til plassering av datasentrene, og at kommunen generelt vet for lite om hvor disse befinner seg. Informant M (Sikkerhetsanalytiker, rådgivende org.) og informant L (Daglig leder, rådgivende org) påpeker også at kommunene i stor grad stoler på hva leverandøren sier, og mener at kommunene i større grad kun er opptatt av om dataene er lagret lovlig, og at de dermed ikke er interessert i å vite nøyaktig hvor dataen er lagret, så lenge lovverket blir fulgt.

Flere informanter forteller at de ikke vet om de har innsikt i hvor dataene lagres, eller at dette er usikkert hvem i kommunen tilknyttet et system som bør eller skal ha denne informasjonen.

6.2.1.2 Tilgangsstyring til data lagret i sky

Informantene er i større grad opptatt av tilgangsstyring internt i kommunen, enn hvilke tilganger leverandøren har til kommunens data i skyløsningene.

For intern tilgangsstyring nevnes vedlikeholdsrutiner for tilgangsstyring, og at kommunen ofte selv håndterer dette direkte i skytjenesten. Informant J (Personvernombud/IKT) viser til at de som et ledd i tilgangsstyring har hatt fokus på å sikre flere med tilgang til hvert system, for å redusere sårbarhet som tidligere har eksistert ved at kun én ansatt har tilgang via personlig pålogging. Flere informanter viser til at en kan be om innsyn i tilganger via rapporter fra leverandør dersom ønskelig. Derimot er det flere informanter som er usikre på om de i det hele tatt kan få innsikt i slik info fra leverandøren.

Informant A (IKT-rådgiver) forklarer derimot at de har godt innsyn i hvordan tilgangsstyring ordnes. Hos leverandøren er det spesifisert restriksjoner i tilgang både hos kommunens administrator, og for leverandøren som selskap.

Informant L (Daglig leder, rådgivende org.) og informant M (Sikkerhetsanalytiker, rådgivende org.) peker på at GDPR spesifiserer at leverandør skal kunne navngi alle som har tilgang, men at hvor mye tilgang leverandøren har antakelig er avhengig av løsningen som leveres. Eksempelvis vil SaaS (Software as a Service) kunne medføre at leverandør må ha tilgang til all data for å kunne identifisere feil og rette opp.

6.2.2 Virkemidler for å sikre at tjenesteleverandør ivaretar kommunens krav

Kommunen har både interne og eksterne virkemidler som kan være nyttige i å styrke datasuverenitet for de skytjenestene de benytter. Virkemidlene er derimot konsentrert rundt

kontraktbaserte krav, og involverer i mindre grad oppfølging av kravene i etterkant av inngåelse på grunn av manglende kompetanse eller ressurser.

Databehandleravtale trekkes frem som det viktigste virkemiddelet for å sikre kontroll over og rettigheter til egne data, overfor tjenesteleverandør. På spørsmål om databehandleravtaler oppleves som et godt virkemiddel for dette formål, presiserer informant B (Personvernombud) at det avhenger av hvordan det er arbeidet med avtalen:

> Jeg syns, hvis den er gjennomlest og den er god. Klart vi har de firmaene som skal sikre seg selv, mer enn å sikre oss. Men det å lese gjennom databehandleravtale, mener jeg, det må være godt nok per i dag. Vi har ikke kompetanse til så mye mer. (Informant B, personvernombud).

Muligheten til å benytte andre former for virkemidler problematiseres derfor opp mot kompetanse i kommunen til å sjekke leverandøren. Bruk av standardkontrakter, som tidligere nevnt, problematiseres også i den forbindelse at det kan begrense hvilke av kommunens krav som innfris i databehandleravtalen.

Informant L (Daglig leder, rådgivende org.) understreker at kommunene ofte sier seg fornøyd så lenge databehandleravtalen er på plass, og at en glemmer at kravene en setter overfor hovedleverandør må speiles nedover i leverandørkjeden til underleverandørene. Dette kan også få påvirkninger på datasuvereniteten ved at underleverandører oppholder seg i andre land enn hovedleverandøren.

Selv om databehandleravtaler omtales som et godt utgangspunkt, poengteres det også at flere forhold ikke nødvendigvis avklares i hver avtale. Det tekniske designet av skyløsningene relateres i hovedsak til mangel til innsikt i og kunnskap om løsningen. Informant F (Seksjonsleder kommunalteknikk) viser til at de eksempelvis ikke har kjennskap til om de kan ta uttrekk av data til rapporter, eller ved leverandørskifte.

Innkjøpsprosessen og selve anskaffelsen nevnes også som et mulig punkt for å sikre kontroll over og rettigheter til egne data. Anskaffelser trekkes frem som et naturlig punkt for å stille krav som kan sikre data. Informant B (Personvernombud) viser derimot til at utover i fagmiljøene i kommunen, så er det fremdeles mer vekt på leverandøravtalen, og denne kommer først i rekka før man tenker på databehandleravtale som en sekundær avtale.

Ved spørsmål om hvordan vilkårene i fastsatte avtaler, slik som databehandleravtaler, kan sikres etter inngåelse vises det til vanlig avtaleforvaltning, og at man må etterspørre informasjon fra leverandøren. Informant H (Prosjektleder velferdsteknologi) poengterer at å etterspørre informasjon og kontrollere, kan være vanskelig for kommunen:

> Det blir jo vanlig avtaleforvaltning. Det handler mye om hvor aktive vi er med og etterspør om [avtalene] blir oppfylt. Men det er litt tilbake til det som jeg sier, når du har en skybasert løsning så må du og… Jeg har ikke kompetanse til å sjekke ligger datasenteret i Irland eller ligger det i Nederland? Eller er de i USA? Så da måtte jeg jo hatt profesjonell hjelp, til å følge opp, sånn rent praktisk da. (Informant H, prosjektleder velferdsteknologi).

Videre poengteres tillitsforholdet til leverandørene på grunn av mangel på kompetanse og innsikt hos kommunen til å kontrollere løsningene:

> Det er der jeg mener, at jeg tror ikke hverken [kommunen] eller andre kommuner har tid eller kompetanse til å sitte og følge opp og faktisk etterprøve det som er i sky. Det er der jeg, igjen tilbake til det, så jeg sier, du må stole på leverandøren. (Informant H, prosjektleder velferdsteknologi).

Både informant I (IT-selskap) og informant L (Daglig leder, rådgivende org.) poengterer at når man har inngått en avtale med en leverandør, så må en sikre innsyn ved å etterspørre informasjon, eksempelvis i form av rapporter og styringsmodell. Informant L (Daglig leder, rådgivende org.) presiserer videre at kommunen må sette krav til informasjon, slik at leverandøren ikke «[…] kan gjemme seg bak «nei dette er felles for alle, så vi kan ikke dele dette her, for da deler vi andre firmaer sin [løsning]». Derimot fremheves det av flere at det er varierende om det er nok kompetanse og ressurser innad i kommunen til å ta seg tid til å forstå informasjon som leverandørene gir ut, for eksempel rapporter.

Tilsyn og revisjoner blir også trukket frem som et mulig virkemiddel, men i motsetning til databehandleravtaler som presiseres at er på plass av de fleste informantene, blir tilsyn og revisjoner nevnt som et potensielt virkemiddel som ikke benyttes i stor grad på grunn av manglende kompetanse og/eller ressurser. Informant B (Personvernombud) viser til at

kompetansen kan eksistere i kommunen, men at det er usikkert hvor ofte slik informasjon etterspørres:

> Jeg tror nok at vi skulle klart å finne riktig kompetanse, fordi de er veldig flinke [IT-avdelingen]. Men det vi kan gjøre er at vi kan spørre etter en gang i året, og det står det faktisk i rutinene våre at vi skal gjøre, ta en internkontroll og spørre har dere skiftet underleverandører, er det skjedd noe. Så det kan vi gjøre. Hvor stor grad det blir gjort, nei… det er ressurser. (Informant B, personvernombud).

De samme tankene gjelder for bruk av tilsyn som virkemiddel av informant B (Personvernombud): «Men vi har ikke gått på noe tilsyn. Det har vi ikke mulighet til. Vi har 300 system. Så vi er litt avhengige av at det finnes alternativ». Ressursene står dermed i veien for å benytte kontrakter og avtaler som et videre punkt for kontroll.

Kommunen har også flere eksterne virkemidler som de benytter i prosesser rundt skytjenester. Eksterne konsulenter brukes i noen tilfeller både til tilsyn og revisjoner, bestilt av enten leverandør eller kommunen, men også som en støtte i anbudsprosessen for å sikre kommunens vilkår. Rapportene som produseres av revisjonene blir også trukket frem, men her problematiseres det at kommunen ikke nødvendigvis har den nødvendige kompetansen til å sette seg grundig inn i rapportene.

Det vises også til Datatilsynet og deres mal for databehandleravtale som en spesifikt nyttig verktøy.

6.2.3 Back-up løsninger for kommunens skytjenester

Avhengighetsforholdet mellom tjenesteleverandør og kommunen påvirker om kommunen kan klare seg uten leverandøren ved bortfall eller nedetid. I den grad back-up løsninger er planlagt, omhandler disse manuelle løsninger i form av papir eller tro på at en skal klare å håndtere nedetid når situasjonen oppstår. Nedetid presiseres likevel som alvorlig for drift.

Lang responstid trekkes frem som en utfordring av informantene, dersom skytjenesten har nedetid. Dette oppleves som mer utfordrende med bruk av tjenesteleverandør, enn i de tilfellene der kommunen tidligere eller nåværende drifter tjenester selv og lagrer lokalt.

Ved bortfall av en skytjeneste der kommunen mister tilgang til innholdet, er det i varierende grad sikret back-up løsninger. I den grad det finnes back-up løsninger, er dette hovedsakelig i

form av interne rutiner eller praksis hos kommunen, med overgang til kritisk informasjon som er tilgjengelig i papirformat, samt manuelt arbeid. Det er også usikkerhet om det tas back-up lokalt av data som er lagret i sky, i tilfelle permanent tap av dataen.

Det er enighet blant informantene om at bortfall av tjenestene som nå er i sky, ville vært alvorlig for kommunen, og at det i stor grad ville påvirket drift. Dette gjelder både administrative tjenester som bruk av Microsoft 365 for mail og fillagring, og tjenester utover i kommunen til innbyggere eller øvrige funksjoner. Informant A (IKT-rådgiver) poengterer at når det først er nedetid, er det lite de i kommunen kan gjøre enn å vente, og å gå over til ikke-digitale løsninger. Informant G (Rådgiver velferdsteknologi) viser også utfordringen med at ved å gjøre seg avhengig av leverandør for å rette opp i feil ved nedetid:

> Men vi opplevde jo faktisk dette tilfellet for ikke så lenge siden. Da var det begge internettlinjene til leverandøren som gikk ned. Så de var ikke på nett. Vi var på nett, men vi kom ikke frem til skyen der serverne var, for da å få signalene helt frem til oss. Da ble det baluba. Men da var det akkurat som om det ikke var noe som var planlagt, eller de visste ikke helt «hva gjør vi nå?». Fordi systemene ga ikke beskjed engang. Så da fant vi et lite sikkerhetshull, som har blitt utbedret. Men det var jo heldigvis kortvarig, men det rammet alle kundene til leverandøren. Så det var jo ikke bare oss, men det hjalp jo ikke. (Informant G, rådgiver velferdsteknologi).

Redundante løsninger som leveres fra samme leverandør problematiseres derfor.

Foruten rutiner ved nedetid, nevnes også arbeid med overordnet planverk i kommunen i tilfelle bortfall av skytjenester. Informant E (Driftssjef IKT) viser til en pågående oppdatering av beredskapsplan i kommunen, som vil omfatte digitale systemer.

Det nevnes også problematikk rundt å være avhengig av enkeltaktører. Informant F (Seksjonsleder, kommunalteknikk) mener det er personavhengig om man er opptatt av slik problematikk, og viser til én skyleverandør som nå er i bruk i kommunen:

> De begynner å danne seg et digitalt økosystem, og de begynner å ta kontroll over det. Det medfører at det kan bli veldig skummelt. For da kan man til slutt ikke sette prisen, og da har ingen reelle konkurrenter på forvaltningssiden. For nå er det flere og flere

> kommuner som tar det her i bruk. Nå er det 80 kommuner som har tatt det i bruk store deler av den porteføljen, og det er vel 200 som har ledningskartverket hos de, av rundt 300 i Norge. Det betyr jo på en måte at de har ganske stor markedsandel. (Informant F, seksjonsleder, kommunalteknikk)

Avhengigheten knyttes her både til mulighet til å velge bort den aktuelle tjenesten til fordel for andre, og kostnadene som følger leverandøren om det ikke er tilgjengelig andre leverandører.

Informant I (IT-selskap) påpeker at:

> […] valget av leverandør bør ikke nødvendigvis ligge på om de er større eller ikke, men at man heller sikrer at det er løsninger som er robuste, som ivaretar de behovene de har», som viser til at det ikke er leverandøren i seg selv, men hvordan bruk av en spesifikk leverandør påvirker ønsket løsning i form av interoperabilitet, mulighet til å skifte leverandør og mulighet til å benytte seg av siste gjeldende teknologi. (Informant I (IT-selskap).

6.2.4 Oppsummering

Forholdet mellom kommunen som kunde og leverandør av skytjenester er preget av at det er leverandørene som står for utviklingen av den tekniske infrastrukturen som trengs for å drive skytjenester. Bruk av tjenesteleverandører gjør at kommunen unngår å måtte bruke midler på vedlikehold, og frigir driftstid. Det oppleves som en trygghet for kommunen å bruke profesjonelle aktører med tanke på dataens sikkerhet.

Likevel karakteriseres dette forholdet av tidvis lite tilbøyelighet fra leverandørene, med bruk av standardkontrakter. Det er også lite innsikt i og tanker rundt tekniske aspekter ved løsningene, som datamodell og type skytjeneste. Det er også i varierende grad at kommunen vet om de har innsyn i hvor tjenestene befinner seg geografisk. Ved tilgangsstyring er det i hovedsak fokus på å kontrollere dette innad i kommunen, og lite fokus på om leverandøren har full tilgang til kommunens data.

Innkjøpsprosessen og databehandleravtaler pekes på som viktige områder og virkemidler for å sikre kommunens vilkår i møte med skyleverandører. Tilsyn og revisjoner benyttes i enkelte

tilfeller, men det poengteres at kommunen ikke har mulighet til å gjennomføre disse aktivitetene så ofte som de skulle ønsket, på grunn av mangel på kompetanse og ressurser. Det er dermed et tillitsforhold til leverandørene, der en tar for gitt at forholdene beskrevet i kontrakter ivaretas.

Forholdet til tjenesteleverandørene preges også av avhengighet. Det er lite fokus på back-up tjenester i kommunen, og der disse eksisterer er det manuell drift med papir som nevnes. Bortfall av tjenestene karakteriseres derimot som alvorlige, og det trekkes frem som utfordrende at responstid hos leverandørene kan være lang som følge av store kundebaser.

6.3 Lovgivning og jurisdiksjon betydning for kommunens skytjenester

I kommunen blir lovverket opplevd som komplisert, og til en viss grad for rigid for flere av områdene i kommunen som lovgivningen gjelder for. Spesielt GDPR beskrives som vanskelig å anvende på lavere nivå i kommunen, men oppleves også som nyttig i dialog med tjenesteleverandører.

Informant A (IKT-rådgiver) beskriver utfordringen i forbindelse med tidsbegrenset bruk av mindre skytjenester:

> Vi jobber i det offentlige, og vi forholder oss til lovverket som det er. Men vi ser at på enkelte områder så blir det litt rigid. Så det er ikke noe problem å overholde det i forhold til de store tjenestene som alle elevene bruker. Det er viktig. Men det som er utfordringen i forhold til GDPR, det er at du skal egentlig gjør den samme jobben for Google som bruker 4000 brukere hele året, som for en liten app som en klasse skal bruke i ei uke. Og det er utfordrende. (Informant A, IKT-rådgiver).

GDPR oppleves derfor som passende for større anskaffelser, men kompliserer mindre prosjekter, fordi de samme vurderingene må gjøres for disse også, tross begrenset bruk og tidsperspektiv.

På den andre siden blir lovverket beskrevet som et hjelpemiddel som kommunen kan lene seg på i samtale ved leverandører. Ved spørsmål om GDPR gjør det lettere å forholde seg til leverandører, svarer informant H (Prosjektleder velferdsteknologi): «[…] jeg syns det ja. Det er veldig klart hvilke krav du skal stille, på et vis. Det var nok mer krevende før, sånn sett, å formulere på god måte hvordan en ønsket, ja, sikkerhet ivaretatt.»

Det blir også vist til at det var nødvendig å gjøre innstramminger og endringer etter at GDPR ble satt i kraft, men at krav i lovgivning, som å sikre databehandleravtaler, fremdeles kommer lenger bak i rekken enn det personvernombudet ønsker. Informant B (Personvernombud) påpeker at det nå er gjort endringer vedrørende digitalisering, for å fange opp blant annet forhold som påvirkes av lovverket:

> En av mine kjepphester er jo at personvern ikke skal være etterpå når alt er gjort, men før eller sammen i starten. Det som Digitaliseringsrådet nå har gjort, med at vi tar den vurderingen, gjør jo at vi kommer inn tidligere. Sånn at den vurderingen kommer. Men hadde det ikke vært GDPR så hadde de ikke brydd seg. (Informant B, personvernombud).

Det er dermed satt inn tiltak, i form av et rådgivende og beslutningstakende organ, som blant annet skal sørge for at lovgivningen blir fulgt. Likevel er det inntrykk av at fokus på lovverk, og GDPR spesifikt, oppleves som noe man «må» gjøre fordi lovverket sier det. Dette inntrykket støttes av informant L (Daglig leder, rådgivende org.) som påpeker at kommunene er opptatt av å ikke måtte melde feil inn til Datatilsynet og få bot, og at dette er en driver for arbeid med personvern og sensitive opplysninger, men at øvrige data muligens ikke får like mye oppmerksomhet.

Informant I (IT-selskap) oppsummerer tilbakemeldinger de har fått via selskapets kunder om lovverk rundt datalagring:

> Regulativene gjør at det er komplekst, kan i hvert fall opplever som komplekst og kanskje litt nitidig å forholde seg til. Krevende å forholde seg til. Tilbakemeldingen er at det er utfordrende på grunn av endringer, og det kan oppleves komplekst. Det er ikke alltid så lett å forstå. Det er også ulike roller som har mer kompetanse enn andre, […] for det er klart at de som er ansatt som personvernombud, har jo veldig god kjennskap til regulativer, i form av sin jobb. Mens andre med sine, andre kvalifikasjoner og kompetansenivå, har kanskje ikke det på den siden, men mer teknisk forståelse og kompetanse. (Informant I, IT-selskap).

Opplevelsen av lovverket knyttes dermed til kompetansen innad i kommunen til å forstå lovverket, og at det er store variasjoner basert på rolle og bakgrunn. Informant I (IT-selskap) presiserer også videre at «På grunn av regulativer, vegrer offentlig sektor i Norden seg på å akselerere deres sky-reise». Kompleksiteten ved lovverket kan stå i veien for at kommuner benytter skytjenester der det passer.

6.3.1 Fokus på jurisdiksjon i andre land

Det er forståelse i kommunen for hvordan jurisdiksjon kan påvirke kommunens data lagret i sky, og fokuset er rettet mot både den geografiske plasseringen til datasentrene, og vertslandet til leverandøren og eventuelle underleverandører.

Det vises blant annet til prosesser i kommunen der man har valgt å ikke gå for en løsning og leverandør, fordi leverandøren kom fra USA. Ved usikkerhet på eksempelvis lagringsland vises det til at denne informasjonen etterspørres, og at en ikke vil gå for tjenesten dersom usikkerheten ikke er avklart. Informant L (Daglig leder, rådgivende org.) viser til at det oppleves som at personvernombud i kommunene er godt opplest på GDPR og detaljer ved Schrems II dommen, som går inn på problematikken blant annet rundt oversending av personopplysninger ut fra EU.

Likevel trekkes det frem at i noen tilfelle vil forhold om motstridende jurisdiksjon, slik som at en skytjenesteleverandør er hjemmehørende til USA, aksepteres. Dette eksemplifiseres ved bruk av Microsoft i kommunen, og det trekkes frem at slike leverandører følger ønskene på lagringssted, men at det er det faktum at selskapet er hjemmehørende til USA som skaper usikkerhet på grunn av potensiell risiko for utlevering av data til myndighetene.

Anbudsprosessen og kontrakter blir trukket frem som det viktigste punktet for kommunen å sikre innsikt i, og unngå, potensiell motstridende jurisdiksjon, eksempelvis hvor dataen er lagret. Derimot problematiseres det av informant H (Prosjektleder velferdsteknologi) om kommunen har nok tid og kompetanse til å følge opp kontraktene etter inngåelse:

> Til daglig så tenker jeg, når du går inn i anskaffelsen så stiller du de kravene, og [leverandøren] besvarer det ut. Hvis de underveis skulle komme til å flytte det datasenteret til India eller hvor de ville uten å informere oss, så tror jeg ikke at vi ville visst det. Det er der jeg mener, at jeg tror ikke hverken [navn på kommunen] eller andre kommuner har tid eller kompetanse til å sitte og følge opp og faktisk etterprøve

> det som er i kontrakten. Det er der du må stole på leverandøren. (Informant H, prosjektleder velferdsteknologi).

Forholdet til jurisdiksjon knyttes dermed opp til kommunens egen kompetanse og ressurser til å følge opp leverandørene på kontraktsforhold, og at det blir et tillitsforhold mellom kommunen som kunde og leverandøren, der en regner med at alle forhold er som de var ved inngåelse.

6.3.2 Oppsummering

Lovgivning som påvirker datalagring i skytjenester oppleves på én side som komplisert og rigid, men på den andre siden som nyttig å lene seg på i møte med leverandører. Det er i stor grad fokus på GDPR i kommunen når personopplysninger behandles. Samtidig påpekes det at det mangler kompetanse utover i kommunen til å forstå lovverket, og at roller med kompetanse, slik som personvernombud, ikke blir involvert tidlig nok i anskaffelse av skytjenester.

Informantene er klar over hvordan jurisdiksjon kan påvirke kommunens data, og det presiseres at man både kan etterspørre informasjon om dette, og at det har blitt sagt nei til tjenester dersom leverandør eller lagringsplass tilhører uønsket sted. Likevel aksepteres slike forhold i visse tilfeller ved store leverandører, og det påpekes som vanskelig å følge opp om det er endringer i lagringssted eller tilholdssted.

6.4 Håndtering av datasuverenitet – organisering, strategier og virkemidler som påvirker arbeid med skytjenester i kommunen

Arbeidet med skytjenester i kommunen påvirkes både av strategier på nasjonalt nivå, og arbeidet som gjøres på lokalt nivå i kommunen.

6.4.1 Nasjonal strategi for datasuverenitet

Det finnes per i dag ingen egen offisiell strategi for å sikre datasuverenitet i Norge. Derimot eksisterer det lovgivning, veiledninger og strategier både i Norge og EU/EØS som peker på karakteristikker ved datasuverenitet, og hvordan disse kan opprettholdes eller styrkes. Flere av disse er rettet spesifikt mot skytjenester.

Det er det norske og EU lovverket som i hovedsak setter rammene for hvordan og hvor data skal oppbevares, og dermed også oppfordrer til eller setter begrensninger for, bruk av skytjenester. Lovgivningen er i hovedsak konsentrert rundt personopplysninger. I en veileder

utviklet av Det europeiske personvernrådet presiseres det at vilkårene fastsatt i GDPR også må følge med dataen der den fraktes (European Data Protection Board, 2020). Dette medfører at overføring av persondata til et tredje land, ikke kan undergrave beskyttelsen denne dataen skal ha i EU. Bruk av skytjenester forutsetter dermed at man vurderer overgang til, og bruk av tjenesteleverandør ved overføring til andre land utenfor EU (European Data Protection Board, 2020).

Der det eksisterer veiledninger for norske virksomheter, omhandler disse generelt informasjonssikkerhet og/eller personvern. Likevel er det flere av disse som kommer inn på råd og informasjon som er spesielt interessant for datasuverenitet i kommunene. Blant annet har NSM utviklet «Grunnprinsipper for IKT-sikkerhet» som er aktuelt for skylagring gjennom fokus på generell informasjonssikkerhet (Nasjonal sikkerhetsmyndighet, 2020a), og «Anbefaling om landvurdering ved tjenesteutsetting» som legger frem vurderingskriterier av vertslandet for tjenesteleverandøren, slik som skyleverandører (Nasjonal sikkerhetsmyndighet, 2019).

I Nasjonal strategi for digital sikkerhet vises det til at myndighetenes rolle i utviklingen av det digitale rom er begrenset, fordi en stor andel av den kritiske digitale infrastrukturen i Norge eies og driftes av virksomheter som er private (Departementene, 2019, s. 9). Dette medfører at beslutninger om utvikling og sikkerhet i det digitale i større grad blir omfattet av kommersielle aktører. Digital sikkerhet er derfor avhengig av et godt offentlig-privat samarbeid (Departementene, 2019, s. 9). Ett av virkemidlene som staten har er å benytte sin rolle som lovgiver, tilrettelegger og tilsynsmyndighet. Strategien påpeker også at det er et mål at den offentlige sektoren har god styring og kontroll på sin digitale sikkerhet. Derfor rådes det at alle virksomheter lager en oversikt over «virksomhetens sentrale mål, hvilke verdier og verdikjeder som inngår, hvor viktige data lagres og hvem som har tilgang til disse dataene» (Departementene, 2019, s. 14).

I NSMs sikkerhetsfaglige anbefalinger ved tjenesteutsetting presenteres fem punkter for å ivareta IKT-sikkerheten ved tjenesteutsetting (Nasjonal sikkerhetsmyndighet, 2020c). Virksomheter må være bevisst på behovet for 1) oversikt og kontroll på hele livsløpet for tjenesteutsettingen, 2) ha god bestillerkompetanse, 3) gjøre gode risikovurderinger for å kunne ta riktig beslutning, 4) stille riktige og gode krav til IKT-tjenesten og til leverandør, og 5) ta riktig beslutning på riktig nivå (Nasjonal sikkerhetsmyndighet, 2020c). Disse punktene stiller krav til hvordan kommunene gjennomfører arbeidsprosessen ved anskaffelse av skytjenester. Blant annet bør de sikre at de har sikkerhetskompetanse, gjennomføre risikovurderinger både

av leverandør og tjenesten, ha innsyn i sikkerhetsarkitekturen og vurdere risiko ved bortfall av tjenesten (Nasjonal sikkerhetsmyndighet, 2020c).

Den norske regjeringens strategi for skytjenester viser til to ulike potensielle måter å ivareta at det offentlige har kontroll over egne data som lagres i sky (Kommunal- og moderniseringsdepartementet, 2016, s. 27). Den første måten er gjennom å etablere egne datasentre for offentlig sektor, mens det andre er å sikre kontrollen gjennom kontrakter ved leverandører. En utredning gjort på forespørsel av regjeringen viser at det ikke er avdekket behov for offentlige datasentre. Kontrakter vil på sin side kreve at det offentliges behov blir ivaretatt, samtidig som at det finnes mekanismer som kan sjekke disse kontraktene etter inngåelse (Kommunal- og moderniseringsdepartementet, 2016, s. 27).

Når en kommune skal gjøre endringer eller omlegginger i et IKT-system eller IKT-drift, viser strategien for skytjenester at skytjenester skal vurderes på linje med andre løsninger. Dersom skytjenesten er den mest hensiktsmessige og kostnadseffektive løsningen, skal en ta i bruk denne (Kommunal- og moderniseringsdepartementet, 2016). Den norske tilnærmingen til bruk av skytjenester er dermed lite restriktiv.

Det settes derimot krav til at den må følge virksomhetens krav til informasjonssikkerhet, og at virksomheter må etablere en sourcingstrategi som innebærer å analysere om den løsningen som er valgt tilfredsstiller kravene som gjelder for den informasjonstypen som skal være i systemet, og dermed om den valgte strategien har akseptabel risiko (Kommunal- og moderniseringsdepartementet, 2016).

Den nasjonale strategien viser til ansvaret kommunen har som behandlingsansvarlig.

> Ressurssterke tilbydarar av skytenester kan i mange tilfelle gi betre tryggleik enn det mange mindre verksemder kan greie sjølve. Dette vil sjølvsagt avhenge av tilbydaren. Det er brukaren av skytenesta som må vurdere om dei opplysningane han tenker å legge i skya er sårbare dersom dei kjem utanfor norsk jurisdiksjon, og vege konsekvensane og risikoen opp mot fordelane med skytenesta. (Kommunal- og moderniseringsdepartementet, 2016, s. 16).

Selv om data settes i sky, er det fremdeles kommunen som skal gjøre vurderinger for å sikre at dataen er sikret godt nok. Dette går også igjen i Datatilsynets sjekkliste med punkter som virksomheter må vurdere får de tar i bruk skytjenester for å behandle personopplysninger. Disse punktene innebærer at virksomheten må gjøre risikovurderinger, inngå

databehandleravtaler, revidere tjenesten jevnlig, sørge for at data overført til andre land gjennomføres på lovlig måte, kommunikasjon må være kryptert, sikre at personopplysninger fra andre kunder er skilt fra egne opplysninger og kunne dokumentere løsningen som blir brukt (Kommunal- og moderniseringsdepartementet, 2016). Lovgivningen forvaltes dermed via kontrakter og oppfølging av disse. Det er opp til den behandlingsansvarlige, her kommunen, til å sikre at lovverket er forstått, at vilkårene i kontraktene er dekkende for krav og behov, og at disse holdes i etterkant av inngåelse.

I veileder i bruk av skytjenester til behandling av helse- og personopplysninger, utviklet av Direktoratet for e-helse, gjennomgås det krav til bruk av skytjenester fra start til eventuell slutt av prosessen. Veilederen stiller krav til både arbeidsprosessen og plassering av ansvar, og poengterer blant annet at det eksisterer en rekke sikkerhets- og beredskapsutfordringer ved outsourcing av drifts- og systemutviklingsoppgaver (Direktoratet for e-helse, 2020).

Der tidligere rapporter, strategier og uttalelser er svært åpne for bruk av skytjenester for datalagring, ble det derimot i en rapport fra januar 2022 åpnet opp om NSMs bekymring for økende nasjonal avhengighet til utenlandske skytjenesteleverandører (Nasjonal sikkerhetsmyndighet, 2022). I rapporten vises det til et behov for å ha datasentre i Norge, slik at disse i større grad kunne blitt tatt i bruk til samfunnskritiske funksjoner og for informasjon som en ønsker å skjerme på grunn av nasjonale sikkerhetsinteresser. Til tross for at rapporten har fokus på nasjonal sikkerhet, kommer den innpå flere punkter av relevans for norske kommuner. Eksempelvis vil en endring kunne fått betydning for den kritiske infrastrukturen og samfunnskritiske funksjoner som kommunene drifter. Rapporten poengterer at denne diskusjonen ikke omhandler privateid versus offentlig eid, men om trygghet til at både virksomheter og brukere har tilgang til sine data og system under alle omstendigheter, og å unngå bortfall av for eksempel skytjenester (Nasjonal sikkerhetsmyndighet, 2022).

Selv om det ikke eksisterer en egen norsk strategi for datasuverenitet, er det dermed flere områder som berører relevant tematikk tilknyttet skytjenester og digitalisering, og som får betydning for norske kommuner. Derimot er det stor overvekt i fokus på hvordan skytjenester som datalagring må ta hensyn til personopplysninger, spesielt dersom disse skal fraktes ut av Norge eller EU.

6.4.2 Lokal strategi i kommunen for datasuverenitet og skytjenester

Fordi datasuverenitet er et ukjent begrep i kommunen, er det ikke direkte spurt om strategier som omhandler dette. Istedenfor er det spurt om strategier for skytjenester eller kontroll over og rettigheter til egne data i kommunen.

Det er i varierende grad at informantene kjenner til lokale strategier eller planer som omhandler organisering av arbeid med skytjenester spesifikt, eller kontroll over og/eller rettigheter til egne data.

Informant E (Driftssjef IKT) viser til at en ny beredskapsplan er under utvikling, der kartlegging av alle systemer, inkludert skytjenester, og tilhørende kritikalitet, skal gjennomføres. Hen viser også til at det eksisterer en strategi for informasjonssikkerhet, men kjenner ikke til en egen for skytjenester spesifikt.

Kommunen har rutine for at alle anskaffelser skal gjennom Digitaliseringsrådet, som blir nevnt av flere av informantene via praktisk erfaring med prosessen. Denne praksisen poengteres også av informant J (Personvernombud/IKT) og K (Utviklingsleder), som viser til etablering av en sikkerhetsgruppe i egen kommune. Informant K viser også til den pågående prosessen med utvikling av ny digitaliseringsstrategi i denne kommunen, og involvering av utviklingsgruppen og sikkerhetsgruppen i arbeidsprosesser med systemer slik som skytjenester.

Informant J (Personvernombud/IKT) viser til en rutine som spesifiserer at prosjekter som skal kjøpe inn system skal involvere personvernombud, men påpeker at det er i varierende grad at hen blir involvert.

6.4.3 Organisering og arbeidsprosess ved anskaffelse av skytjenester i kommunen

Informantene beskriver mangel på fastsatt organisering av arbeid med skytjenester i kommunen. De viser til varierende forståelser fra person til person og avdeling til avdeling.

Informant G påpeker at det enda oppleves som at kommunen er i en overgangsfase, med å finne ut hvordan organiseringen skal være. Det pekes også til mangel på oversikt over anskaffelser i kommunen. Informant C (IKT-rådgiver) viser til at mer oversikt ville ført at en kan vurdere om eksisterende løsninger kan anvendes, men at den nåværende organiseringen er fragmentert og preget av siloarbeid og tunnelsyn. Informant F viser også til at det er mangler i «anskaffelsesbiten».

Videre vises det også til stor variasjon i hvordan kommunen går frem ved anskaffelse av skytjenester.

Informant B (personvernombud) opplever at fremgangsmåten er preget av ønske om nytt system eller tjeneste, og ikke om løsningen ligger i sky eller ei.

Kun informant F viser til en faktisk prosedyre, men forklarer også at måten det arbeides på er et resultat av at hen har hatt flere ulike roller, og at prosessen i stor grad omhandler samspill med leverandør for å sikre en løsning som passer.

Flere av informantene viser til bruk av interne ressurser rundt fremgangsmåte ved nye skytjenester. Informant A og H viser til involvering av personvernombud, og informant H viser i tillegg til involvering av IT-avdelingen. Informant H viser også til etableringen av en databehandleravtale, som en del av fremgangsmåten mot ny skytjeneste.

Det eksisterer også usikkerhet i kommunen angående arbeidsprosess ved nye skytjenester. Informant C (Digitaliseringsrådgiver) oppsummerer variasjonen i kommunen i hvordan fremgangsmåten er ved nye skytjenester er:

> […] vet du hva, det vet jeg ikke helt. Fordi det varierer fra avdeling til avdeling, sånn som jeg har inntrykk av. Nå er det jo kommet på plass et Digitaliseringsråd, som skal forhåpentligvis forbedre dette her da. Så nå vet jeg ikke helt hvordan det fungerer nå, men målet der er at alt skal gå via det, sånn at man skal kunne få denne oversikten. Og at det er en gruppe her som er med og rådgir de som skal gå til innkjøp. Om hva er det viktig at vi tenker på, hva er det viktig at er på plass i et sånn system, blant annet det med at er det mulig med lagring i sky, hvordan skal vi administrere det, hvordan skal vi drifte. Hvordan koblinger er det mot andre systemer? Informant C, digitaliseringsrådgiver).

I arbeidsprosessen er det også store forskjeller i hvilke faktorer som poengteres som vektlagte faktorer ved anskaffelse av skytjenester.

Informantene som representerer fagområder i kommunen har fokus på GDPR og beskyttelse av personopplysninger, driftssikkerhet, at regelverk blir fulgt, og ikke minst at tjenesten skal møte et behov i kommunen. Kun én av disse informantene nevner kost som en viktig faktor.

Informantene som representerer IT, IKT og personvernombud har på sin side kun fokus på sikkerhet ved løsningen, eksempelvis hvor dataen er lagret, hvem som er underleverandør, hvilken type informasjon som settes i sky og hvordan den blir sikret. Informant E (Driftssjef IKT) trekker også spesifikt frem at det er viktig at kommunen eier dataen, og at det til en viss grad er viktig at dataen er lagret i Norge.

Informantene fra rådgivende organisasjon mener at det for kommunene oftest er kostnader er den viktigste faktoren i vurdering om en skytjeneste skal tas i bruk eller ei, og at kommunene gjennom å benytte skytjenester kan frigjøre kostnader knyttet til drift.

Informant I (IT-selskap) har derimot en mer variert forståelse av kommunenes vektlagte faktorer, og trekker frem sikkerhet, skalerbarhet, kostnadsbesparende, sikker og stabil drift med høy oppetid og smidige operasjonsmodeller som vektlagte faktorer.

6.4.4 Interne ressurser i kommunen

Det er i stor grad mangel på opplæring i skytjenester ute i fagavdelingene og hos de som er systemansvarlige eller systemeiere for skytjenester.

De kommunale informantene viser til lite erfaring og opplæring i skytjenester gitt gjennom arbeidsplassen, utenom den praktiske erfaringen de har fått gjennom arbeidet i nåværende eller tidligere stilling. Informant A har i regi av sin stilling og engasjement deltatt på kursing av skyleverandør Google. Informant J (Personvernombud/IKT) har på sin side deltatt på kurs i regi av skyleverandør Microsoft.

Informant B viser til at ansatte i IT-avdelingen antakeligvis har mest opplæring på skytjenester, som bekreftes av informant E som viser til at IT-ansatte som arbeider med drift, holder på med å ta kurs i nye skytjenester. Informant G har mastergrad innen informatikk-feltet, men har også i begrenset grad vært innom skytjenester utenfor jobbsammenheng.

Derimot eksisterer det til en viss grad intern kompetanse på skytjenester i kommunen, som i varierende grad blir benyttet. IT- og IKT-avdelinger blir nevnt i forbindelse med støtte til drift av skytjenestene. Informant E (Driftssjef IKT) viser til at IT-avdelingen i kommunen på nåværende tidspunkt kurses i skytjenester, og dermed utvider kompetansen på dette feltet.

Personvernombud blir av flere informanter nevnt i forbindelse med avtaler og kontrakter. Informant H (Prosjektleder velferdsteknologi) trekker også frem fordelene med at personvernet i kommunen er «frempå» og oppdatert, sammenliknet med hens inntrykk av andre kommuners personvernombud.

Flere informanter problematiserer mangel på direkte kompetanse om skytjenester. Både informant A (IKT-rådgiver) og informant F (Seksjonsleder kommunalteknikk, systemeier) trekker frem at de i stor grad har måttet lene seg på egen kompetanse i forbindelse med skytjenester. Kompetansen virker dermed i stor grad å være både personavhengig både med tanke på kompetanse og interesse for skytjenester. Det vises eksempelvis til tap av god kompetanse når enkeltpersoner slutter i en stilling. Dette støttes av informant L (Daglig leder, rådgivende organisasjon) «…det er veldig sjelden å oppdage at du har en spesialist på skytjenester. At det er en egen person som bare har spesialisert seg på skytjenester» og følger det opp med:

> […] og det er egentlig litt skremmende når vi samtidig vet at så å si alle kommuner har en eller annen form for plan eller tanke eller prosess på å flytte over i sky. Så det henger ikke helt sammen da. Kompetansen og hva slags hensikter og prosesser som kommunene er i. (Informant L, daglig leder rådgivende org.).

Informant B (Personvernombud) og informant J (Personvernombud/IKT) trekker frem at interne ressurser i større grad kunne blitt benyttet i anskaffelsesprosesser. Eksempelvis involveres ikke alltid personvernombud ved innkjøp av nye systemer eller utvidelser, fordi en ikke registrerer at dette er prosjekt som krever databehandleravtaler. Dette samsvarer med informant M (Sikkerhetsanalytiker, rådgivende org.) sin beskrivelse av at kommunene i varierende grad benytter den interne kompetansen i IKT/IT-avdelinger under anskaffelser av skytjenester:

> […] og så er det jo variasjon i forhold til hvordan, altså hvem i kommunen som håndterer arbeidet. Det starter jo som gjerne i et tjenesteområde, enten helse eller skole eller teknisk. Og så blir behovet enten dekket av det tjenesteområdet selv, uten involvering av IKT-avdelingen. Eller så blir IKT-avdelingen involvert, og så har du hele spekteret mellom. Delvis involvert, ganske involvert, og så fullt involvert da på en måte. Så det varierer fra kommune til kommune hvor mye IKT-avdelingen blir involvert. Og dermed også graden av sikkerhet i vurderingene. Jo mer IKT-avdelingen er involvert, jo mer sikkerhet blir det diskutert i anskaffelsen. Men det foregår anskaffelser som går helt utenfor IKT-avdelingen, og da vet vi egentlig ikke så veldig

> mye om hvor mye sikkerhet som blir diskutert i det hele tatt. (Informant M, sikkerhetsanalytiker, rådgivende org.).

Intern kompetanse blir også trukket opp mot desentralisering av ansvar for skytjenester i kommunen. Flere av informantene poengterer kompleksiteten som medfølger desentralisering av ansvar for skytjenester. Informant B (Personvernombud) presiserer at «Jeg syns det er delegert litt for langt ut i organisasjonen, fordi du kan ikke forvente at kompetansenivået skal være så høyt. Det er andre ting som er fokuset enn skytjeneste eller ikke». Informant F (Seksjonsleder kommunalteknikk, systemeier) oppsummerer desentralisering av ansvaret slik:

> Det er sånn at vi hos oss, vi er jo vann, avløp, renovasjon og veifolk i utgangspunktet. Men så skal vi forstå, forvaltningslov, offentligslov. Vi skal forstå hva det betyr å gjøre innkjøp, vi skal kunne masse norske standarder. Vi skal ha kurs opp og ned i mente på det. Og så skal vi i tillegg være flinke til å forvalte alle de systemene vi har. Så det med IT-kompetanse, før var det nok at folk kunne vann og avløp, og kunne drifte det. Nå er det «ja vi ser etter en driftsoperatør som kan vann og avløp, men i tillegg kan bruke data». (Informant F, seksjonsleder kommunalteknikk).

Informant F (Seksjonsleder kommunalteknikk, systemeier) følger også opp tankene om desentralisering med å poengtere at denne formen for organisering krever at IT-avdelingen er mer «rådgivere enn utførere», slik at de kan rådføre fagmiljøene til å få ting til å henge sammen. Informant G (Rådgiver velferdsteknologi) viser også til samspillet mellom fagavdelingene og IT-avdelingen, og at IT-avdelingen ikke nødvendigvis trenger å styre tjenestene i sin helhet, men heller kontrollere sikkerheten. Hen viser samtidig til at ved å sette ut drift til skytjenesteleverandør, får en frigitt tid hos IT-avdelingen.

Likevel blir det trukket frem at denne formen for organisering er fordelaktig, fordi fagfolkene vet «hvor skoen trykker», og forstår hvordan for eksempel et system lagt til sky bør utformes

Som et slags motbør til personavhengig kompetanse har kommunen opprettet et Digitaliseringsråd. Dette er også tilfellet i kommune B, som har en utviklingsgruppe og en sikkerhetsgruppe som fyller mye av de samme funksjonene. Disse gruppene skal gjennomgå nye anskaffelser eller utvidelser, for å sikre at visse krav i kommunen blir holdt. Gruppene besitter dermed kompetanse uten at denne blir like personavhengig, og vil vurdere flere ulike

aspekter som er relevant for datasuverenitet, eksempelvis informasjonssikkerhet og om databehandleravtale er på plass. Selv om Digitaliseringsrådet blir nevnt som en ressurs, poengteres det også at innføring av en ekstra struktur som sånne grupper utgjør, vil kunne føre til mer byråkrati i kommunen.

Informant M (Sikkerhetsanalytiker, rådgivende org.) trekker paralleller mellom å sette ut drift og mengden intern kompetanse i kommunen:

> Jeg tror egentlig kommuner som har mye drift selv, er flinkere til å stille krav til de tjenesteleverandørene de har eksternt, enn de kommunene som er dårligere bemannet og har alt sammen noe annet sted. Fordi de rett og slett har solgt ut kompetansen sin. (Informant M, Sikkerhetsanalytiker rådgivende org).

Informant L (Daglig leder, rådgivende org.) poengterer videre at kommuner som setter ut drift til for eksempel skyleverandør, også tror de kan sette ut ansvar for sikkerhet i tjenestene:

> […] man setter ut driften, enten til et, ett eller annet selskap i Norge, eller et eller annet i skyen. Og tror da at man kan sette ut dette her, og dermed også sette ut ansvar for sikkerheten for data og konfidensialiteten da. Men det sitter fremdeles hos kommunedirektøren. (Informant L, daglig leder rådgivende org.).

6.4.5 Eksterne ressurser kommunen kan benytte seg av

Kommunen kjenner til flere lokale, regionale og nasjonale eksterne ressurser som kan være tilgjengelige og hjelpsomme ved spørsmål om skytjenester og kontroll av data.

Digi Rogaland blir nevnt av informanter i begge kommunene som en ressurs som kan benyttes. Det nevnes at det innad i Digi Rogaland eksisterer et kompetansemiljø på informasjonssikkerhet, men at det ikke er noe spesifikt rettet mot skytjenester.

Kommunen er også del av forskjellige nettverk som kan fungere som en ekstern ressurs de benytter seg av ved spørsmål om skytjenester. Interkommunale prosjekt, nabokommuner og samarbeidskommuner blir nevnt som eksempler.

Nasjonale ressurser slik som nasjonalt program for velferdsteknologi og Datatilsynets veiledningstjeneste nevnes som aktivt brukte ressurser.

Kommunen bruker også eksterne firmaer som ressurs overfor skyleverandører. Informant A (IKT-rådgiver) og informant K (Utviklingsleder) nevner bruk av eksterne firmaer for å gjennomføre revisjoner eller tilsyn. Informant A poengterer at bruk av en ekstern ressurs, slik som et revisjonsfirma, kan være nyttig både med tanke på at de selv ikke kunne fått tilgang til alt, men også at det mangler kompetanse i kommunen for å gjennomføre slike revisjoner:

> […] Og det føler jeg ivaretar, for vi har ingen mulighet til å reise til datasentrene, og vi ville ikke fått kommet i nærheten av døra engang. Altså det er helt umulig å komme og gjøre revisjon, og vi ville ikke hatt kompetansen til det. Og Google kan ikke slippe inn alle kundene. Det er helt utelukket. Så jeg syns det er en god måte det blir gjort på. (Informant A, IKT-rådgiver).

Derimot presiseres det at i dette tilfellet er det leverandøren selv som bestiller disse revisjonene, for så å tilgjengeliggjøre rapportene for kommunen som kunde. I tilfellet informant K (Utviklingsleder) nevnte ble tilsynet bestilt av kommunen selv.

Informant I (IT-selskap) presiserer at leverandøren, slik som dem selv, kan benyttes som en ressurs og sparringspartner for kommunene.

6.4.6 Oppsummering

På nasjonalt nivå finnes det ingen strategi direkte for datasuverenitet. Datasuverenitet og skytjenester i kommunene blir likevel påvirket av øvrige dokumenter og strategier som omhandler skytjenester, anskaffelser og informasjonssikkerhet. Det oppfordres av myndighetene til å benytte skytjenester så lenge dette gjøres forsvarlig, og at GDPR følger ved overføring av personopplysninger til andre land.

Det er også mangel på lokal strategi i kommunen, og planverk som eksisterer eller holder på å bli utarbeidet handler generelt om informasjonssikkerhet, beredskap eller personvern. Digitaliseringsrådet er innført som et tiltak for å samle beslutninger rundt digitale løsninger som skytjenester. Både organiseringen av og arbeidsprosessen mot nye skytjenester oppleves derimot som fragmentert. Den desentraliserte modellen fører til at fagavdelingene i kommunen på én side får mer passende leveranser, men på den andre siden stiller det store krav til kunnskap om sikkerhet, skytjenestene og lovgivning. De i kommunen som har denne kompetansen blir ikke involvert så ofte, eller så fort, som de kunne.

Det eksisterer derimot flere interne ressurser i kommunen, i hovedsak i IT-avdelingen og hos personvern. Likevel viser informantene til at det mangler direkte kompetanse på skytjenester. Av eksterne ressurser benytter kommunen både lokale, regionale og nasjonale ressurser i sitt arbeid med skytjenester. Leverandøren blir også trukket frem som en viktig ressurs.

7. Diskusjon

For å forstå ivaretakelsen av datasuverenitet i kommunens arbeid med skytjenester må funnene i empirien ses i lys av det teoretiske rammeverket utformet i kapittel 4.

Diskusjonen er strukturert etter karakteristikkene og underkarakteristikkene identifisert i oppgavens teorikapittel. Jeg vil se på hvilke karakteristikker som kan identifiseres, hvordan disse ivaretas og hvilke utfordringer kommunen møter i dette arbeidet.

I tabell 7 er funnene fra empirien satt i system med sammenhengende analysekategori fra det teoretiske rammeverket, og dilemma for drøfting.

Tabell 7. Empiriske funn knyttet til teoretisk rammeverk og diskusjon

Analysekategori fra teoretisk rammeverk	Empiriske funn	Identifiserte dilemmaer i kommunens arbeid med skytjenester
Verdier **- Kontroll** **- Makt**	• Usikkerhet rundt geografisk plassering av data • Fokus på tilgangsstyring internt, men ikke eksternt hos leverandør • Leverandør setter i stor grad premissene for tjenestene som utvikles	• Vanskelig å garantere kontroll over data på grunn av mangel på innsikt i geografisk plassering og tilgangsstyring eksternt • Manglende kompetanse til å stille krav og vurdere leverandør • Avhengighet av leverandør på grunn av mangel på back-up
Datatype **- dataklassifisering**	• Store mengder forskjellig data i sky • Dataklassifisering tas ikke systematisk i bruk til å definere typen data • Typen data påvirker i liten grad valg av løsning • Større fokus på sikkerhet rundt persondata	• Løsninger ikke tilpasset data på grunn av mangel på dataklassifisering
Kontekst **- IT-arkitektur** **- Lovgivning**	• Liten innsikt i tekniske aspekter ved skytjenesten • Lovgivningen oppleves som kompleks og vanskelig å tilpasse alle prosjekter	• Manglende integrering av datasuverenitet i IT-arkitekturen • Lovverk er styrende for arbeidet, men utfordrende å etterfølge i praksis

	• Lovgivningen brukes samtidig som redskap i møte med leverandør	• Lovverket tar i hovedsak for seg personvern
Håndtering **- Ledelsesstrategi** **- Virkemidler**	• Mangel på nasjonal og lokal strategi for datasuverenitet • Desentralisering av arbeidet fører til fragmentert siloarbeid med stor variasjon • Ressurser og virkemidler internt og eksternt er konsentrert rundt anskaffelse	• Mangel på overordnet strategi fører til fragmentert håndtering • Håndtering preges av mangel på teknisk kompetanse og å lene seg på lovverket
Utfordringer	• Komplisert lovverk • Mangel på teknisk kompetanse ute i kommunen • Lite ressurser til avtaleforvaltning	• Utfordringer med manglende kompetanse og/eller ressurser til å følge opp eksisterende avtaler

I de følgende delkapitlene vil jeg dermed benytte de fem analysekategoriene fra det teoretiske rammeverket utviklet i kapittel 4 (verdier, datatype, kontekst, håndtering og utfordringer) for å identifisere datasuverenitet i kommunens arbeid med skytjenester. I tabellens høyre felt presiseres dilemmaene som jeg vil diskutere i lys av den identifiserte empirien.

7.1 Har kommunen kontroll og makt over data i skytjenester?

Som gjennomgått i oppgavens teoridel, er datasuverenitet som konsept i hovedsak konsentrert rundt de to verdiene «kontroll», som omhandler hvor dataen befinner seg og hvem som har tilgang til den, og «makt» som omhandler hvem som har autoriteten over utvikling av skytjenester som felt og forholdet mellom leverandør og kommunen som kunde (Hummel et al., 2021).

7.1.1 Ivaretakelse av verdien «kontroll»

Empirien viser at ivaretakelse av verdien «kontroll» kun delvis kan identifiseres i kommunen, på grunn av store forskjeller i viten om, hvor lagringsplassen til dataen geografisk er plassert. Mangel på bevissthet rundt hvor dataen er lagret i kommunen, vil kunne være negativt for datasuverenitet i kommunen, fordi en da ikke vet hvilken lovgivning som gjelder for dataen. Å ikke vite hvor dataen er plassert kan på den ene siden føre til at kommunen begår lovbrudd dersom en ikke fyller kravene i lovgivning for lagring av data, for eksempel men hensyn til personvern eller arkivkrav (Arkivloven, 1999; Personopplysningsloven, 2018), og på den andre siden kan dataen risikere å bli underlagt uønsket jurisdiksjon eller plassert i land der en står overfor risiko for å miste data på grunn av ustabiliteter (Hummel et al., 2021, s. 6). Ved å være konsekvent ved inngåelse av databehandleravtaler på den geografiske plasseringen av dataen, ville kommunen kunne ivaretatt datasuvereniteten som gjelder kontroll bedre, fordi en

ville vært bevisst på betydningen av lagringssted, og dermed også kunne fulgt dette opp med kontraktsfestede krav.

Det er også identifisert i empirien at det er liten innsikt i hvem hos tjenesteleverandøren som har tilgang til kommunens data, og hvilke aspekter av dataen de har innsyn i. Tilgangsstyring for å begrense leverandørens innsyn i datamaterialet, og dermed leverandørens mulighet til å utlevere disse, er i liten grad i fokus hos kommunen, som kan tyde på at kommunen har tillit til at leverandøren ikke misbruker dataen. Tilgangsstyring hos leverandør er svært viktig for å hindre unødvendig innsyn i data, både om kommunens data omhandler innbyggere, eller eksempelvis virksomhetskritisk informasjon. Uten tilgangsstyring, kan hvem som helst med enten fysisk eller operatørtilgang til servere få tilgang til den lagrede dataen (De Filippi & McCarthy, 2012, s. 11). En oversikt over hvem hos leverandøren som har innsyn i kommunens data, samt aktivitetslogging, spesifiseres derfor av NSM som krav til leverandøren som bør utvikles av virksomheten før anskaffelsen (Nasjonal sikkerhetsmyndighet, 2020c).

Dersom kommunen ikke har innsikt i eller rutiner for å styre tilgangsstyring hos leverandøren risikerer de dermed at flere aktører har tilgang til data som kommunen i utgangspunktet ønsker å holde lukket. Den nåværende passive tilnærmingen er derimot basert på at en antar at leverandøren kun har tilgang til det de må, som viser til at det er tillit til at leverandøren følger retningslinjer som ikke er etablert. Dersom leverandøren ikke har etablerte rutiner for tilgangsstyring vil det derimot føre til at kontroll over data ikke er ivaretatt.

Derimot er det rutiner for og innsikt i hvem som har tilgang til data og system innad i kommunen, både med tilgangsstyring og bruk av aktivitetslogg. Å begrense datatilgangen også innad i kommunen vil også være positivt for datasuvereniteten, da spesielt for den individuelle dimensjonen av datasuverenitet og personvern for innbyggerne i kommunen, fordi en begrenser og har oversikt over hvem som har tilgang til persondataen, og eventuelt om den blir misbrukt. På denne måten kan en unngå eksempelvis urettmessig oppslag gjort av ansatte (Khan & Jebens, 2018).

7.1.2 Ivaretakelse av verdien «makt»

Empirien viser at verdien «makt» i stor grad preges av at det er private aktører som står for utbygging av infrastruktur og utvikling av skytjenester. På den ene siden oppleves det av kommunen som en trygghet å bruke leverandører med ekspertise på disse tjenestene, og at det

er positivt at kommunen dermed unngår å bruke midler på vedlikehold, som igjen frigir driftstid.

Ved å benytte seg av private aktører som tjenesteleverandør av skytjenester kan en argumentere for at kommunen gir opp en viss mengde kontroll over egne data, til fordel for den tekniske kompetansen som trengs for å sikre dataen og frigjøring av ressurser internt. Private aktører som tilbyr tjenesteutsetting, kan være mer profesjonelle og tilby mer stabile og tilgjengelige tjenester enn kommunen selv, og de har ofte bedre kompetanse og ressurser på IKT-sikkerhet. Det kan dermed være store fordeler for kommunen å benytte private aktører til skytjenester, dersom kommunen mangler ekspertkompetanse eller verktøy, som tjenestetilbyderen besitter (Kommunal- og moderniseringsdepartementet, 2016, s. 9-12).

Forutsetningen ved denne bruken er at det må eksistere nok kompetanse hos kommunen til å vurdere om tjenesteleverandøren nettopp er profesjonell, og for å følge opp kravene som er satt i kontrakter og avtaler for å bekrefte dette. Som empirien viser blir oppfølging av krav i kontrakter gjort i svært begrenset grad, både på grunn av mangel på ressurser, og fordi kommunen ikke har kompetanse til å gjennomføre slike aktiviteter, som revisjoner og tilsyn. Om makt over egen data er ivaretatt, er det dermed potensielt på grunn av at tjenesteleverandøren følger slike krav i lys av å være en seriøs aktør. Likevel er det viktig for kommunen å ta hensyn til at det er de, i lys av å være behandlingsansvarlig, som skal sikre at tiltak er på plass som sikrer dataen tilstrekkelig (Personopplysningsloven, 2018).

Selv om informantene opplever at det er mulig å velge mellom flere aktører, er det påpekt at de kan bli bedre på å sette absolutte krav til leverandør. Forholdet mellom leverandør og kommunen risikerer dermed å bli preget av at det er mangel på kompetanse om hva man kan stille krav til, spesielt om tekniske aspekter, slik at leverandøren er den som definerer leveransens kravspesifikasjoner i kontrakten ut fra hva de tenker er passende. Eksisterende kompetanse muliggjør at en utvikler mer relevant kompetanse som trengs for å ha makt over egen data (König, 2017, s. 9). Derimot så er ikke mangel på intern kompetanse ensbetydende med at tjenesteleverandør leverer dårligere løsninger og utvikler markedet kun til vinning for seg selv. Likevel vil et asymmetrisk kompetanse forhold mellom kommunen som kunde, og tjenesteleverandøren som utvikler og premissettende part, forskyve maktbalansen og kunne føre til mer avhengighet av at leverandøren ivaretar tiltak som skal sikre kontroll over data. Det er derfor mulig at lav grad av makt hos kommunen også medfører usikkerhet om eller lav kontroll, fordi det blir opp til leverandøren å sikre disse behovene i lys av å vær en seriøs aktør.

I tillegg, som påpekt av informant F (Seksjonsleder, kommunalteknikk) er det ikke bare gigantleverandører som Google og Amazon som styrer skymarkedet. Det er også eksempler på mindre aktører som spiser opp markedsandeler, og slik minsker kommunens mulighet for reelle valg mellom leverandører. Det kan dermed være vanskelig å unngå enkelte aktører, fordi hele markedet er basert på en sentralisering av verdikjeden av skytjenester og leverandører. NSM inkluderer denne tanken om avhengighet av utenlandske aktører spesifikt, i sin rapport om dataautonomi, og viser til skepsis til avhengighet til skyleverandører som befinner seg i utlandet, da spesielt om disse benyttes til å lagre samfunnskritiske tjenester og funksjoner (Nasjonal sikkerhetsmyndighet, 2022, s. 3). I den grad bruk av utenlandske aktører problematiseres av kommunen, er det derimot i forbindelse med å følge kravene til GDPR, og dermed om lagringen befinner seg innenfor EU eller ei. Avhengighet av enkeltaktører i seg selv er ikke nødvendigvis en utfordring for datasuverenitet, så lenge tjenesteleverandør ivaretar de kravene kommunen som kunde måtte sette for å ivareta datasuverenitet. Derimot kan stor avhengighet av enkeltleverandører være utfordrende dersom dette øker nedetid for viktige tjenester, responstid på grunn av mange kunder, fare for sikkerhetsbrudd eller mindre mulighet for kommunen å få gjennom sine ønskede krav i fravær av alternative leverandører.

Fordi bortfall av tjenester karakteriseres som svært problematisk av informantene, er det svært negativt for ivaretakelse av datasuverenitet at skytjenestene i liten grad er dekket av formelle back-up løsninger. Zheng og kollegaer har gjennomført en kvantitativ studie av nedetid hos flere av de store skyleverandørene, som også leverer infrastruktur til andre skytjenesteleverandører. Dataen viser til at hver leverandør vanligvis opplever nedetid hvert eneste år, og selv om 14% av denne nedetiden var på under 1 time, var også over 40% av nedetiden mellom 6-24 timer (Li et al., 2013, s. 4-6). For en kommune ville såpass lang nedetid ha rukket å påvirke viktige områder av kommunens drift. Selv om det er svært positivt at kommunen har fokus på nedetid ved valg av leverandør, kan det aldri garanteres at en tjeneste aldri har bortfall. Å stole på at nedetiden forblir kort, eller at man klarer å omorganisere seg medfører derimot stor usikkerhet. Antakeligvis vil de klare å tilpasse seg, og nedetiden være kort, men dette kan de ikke vite helt sikkert, som potensielt kan være negativt for datasuvereniteten. Derimot vil faste rutiner som nevnt at noen informanter være svært positivt for datasuverenitet, da en minsker avhengighet av skytjenestene dersom noe skulle skjedd.

7.2 Vurderinger av datatype og hvem dataen har betydning for

I empirien er det presentert at kommunen i liten grad benytter dataklassifiseringer før data skal flyttes over i, eller opprettes i skytjenester. Dataklassifisering er derimot nødvendig for å bestemme i hvilken grad data må sikres og hvilken verdi den har for kommunen som virksomhet (Shaikh & Sasikumar, 2015, s. 494), og vil dermed få betydning for datasuverenitet ettersom det danner grunnlaget for å velge korrekt type tjeneste. Ulike resultater av dataklassifisering vil gi ulike behov for sikkerhetstiltak (Føyen & Maanum, 2015, s. 42). Dette ble også presisert av informant I (IT-selskap), som viser til at dataklassifiseringen bør få betydning for hvilken type skytjeneste kommunen benytter, og at spesielt sensitive data bør eksempelvis holdes i private skyløsninger.

Det mangler derfor en kobling mellom hvilken type data kommunen lagrer, og hvilken teknisk løsning som velges, for at datasuverenitet skal ivaretas. Dette kan føre til suboptimale løsninger i lys av datasuverenitet. Ved mangel på gjennomføring av disse analysene risikerer dermed kommunen at data lagres i samme tjeneste som andre virksomheter, i offentlige skyer. Istedenfor at denne dataen blir begrenset til en lukket tjeneste som er avgrenset til kommunen som virksomhet (Kommunal- og moderniseringsdepartementet, 2016, s. 9). Selv om dette er lovlig, vil det kunne føre til dårlig ivaretakelse av kommunens data med tanke på datasuverenitet, fordi det er begrenset hvilke sikkerhetstiltak en får innført.

Det kan derimot se ut som om kommunen har mer fokus på sikkerhet og beskyttelse av data, når dataen kan oppfattes som personopplysning, og er koblet til den individuelle dimensjonen og innbyggerne i kommunen. DPIA nevnes som en vurdering av konsekvenser for personopplysninger ved bruk av skytjenester. Å gjennomføre DPIA er en plikt etter personvernloven, og artikkel 35 definerer når denne analysen skal gjennomføres, hva den skal inneholde og hvilken aktør som skal gjennomføre den (Datatilsynet, u.å). DPIA er dermed ikke er dataklassifisering i seg selv, men skal benyttes dersom dataen det omhandler defineres som personopplysninger. Det viser til at selv om kommunen ikke gjennomfører dataklassifiseringer rutinemessig, så er det fremdeles et forhold til hvilken type data som skal plasseres i sky dersom disse er koblet til den individuelle dimensjonen. Dette kan muligens forklares ved at det ligger flere lovkrav til denne typen opplysninger. Både fokus på personvern ved bruk av databehandleravtale og etterlevelse av GDPR, samt rettighet til innsyn for innbyggerne, trekkes frem. Kompleksiteten i skytjenester og generell datalagring kan derimot påvirke datasuverenitet negativt, fordi det ikke er oversikt eller en automatisert prosess for å hente ut persondata med betydning for den individuelle dimensjonen.

Innsynsretten skal derimot sikre at individer kan spørre virksomheter, som behandler opplysninger om individet, om hvordan disse behandles og hvilke opplysninger som er lagret (Datatilsynet, 2018b), og det er problematisk dersom kommunen ikke har rutiner for dette.

På kollektivt nivå viser informantene til dataens betydning for drift i kommunen, eksempelvis tap av e-mailsystemer, fillagring og kritisk infrastruktur som ligger i sky, slik som vann og avløp. Betydningen av data som påvirker kollektiv dimensjon knyttes på en side til administrative data som ikke anses som kritiske for drift utover i kommunen, og på den andre siden til manglende retningslinjer fra myndighetene, når det relateres til kritisk infrastruktur. Sammenliknet med data som kobles til den individuelle dimensjonen nevnes det ikke bruk av vurderinger på hvordan data med betydning for kollektiv dimensjon, for eksempel virksomhetskritisk informasjon som økonomisk informasjon, kan påvirkes av å bli satt i skytjenester. Dette kan medføre at når funksjoner slik som fillagring blir satt i sky, så er det ikke i like stor grad gjennomført vurderinger for å klassifisere dataen og medfølgende risikoer. Selv om generelle risikovurderinger blir nevnt av informantene som et redskap før bruk av skytjenester, vil det være viktig å benytte dataklassifiseringer også for denne typen data, fordi den har en verdi for kommunen som en helhet, og kommunen bør dermed tilpasse både tekniske aspekter og sikkerhetstiltak til typen data.

Mulighetene for å ivareta datasuverenitet ville derimot blitt satt mer i system dersom dataklassifiseringer ble anvendt på en konsekvent måte før anskaffelse, slik at vurderingen kunne påvirke utformingen av skytjenesten for alle typer data. Ved å inkludere ulike former for dataklassifiseringer ved prosesser rundt skytjenester i kommunen, vil de i større grad kunne sikre at de rette sikkerhetstiltakene og typen skytjeneste blir satt opp rundt spesifikke datatyper. Det sterke fokuset på den individuelle dimensjonen, til tross for manglende dataklassifisering, kan antakeligvis begrunnes i hvor stor betydning og påvirkning GDPR har fått for kommunens arbeid med data, og samsvarer med informant L (Daglig leder, rådgivende org.) sitt innspill om at kommunene antakeligvis er bedre på personvern enn informasjonssikkerhet.

7.3 Hvordan påvirker IT-arkitektur og lovgivning som kontekst kommunens arbeid med skytjenester?

De to kontekstene IT-arkitektur og lovgivning danner grunnlag for identifisering av to ulike aspekter av datasuverenitet i kommunens arbeid med skytjenester.

7.3.1 Mangel på innsikt i IT-arkitektur i kommunen

Fra empirien er det tydelig at kommunen har liten innsikt i IT-arkitekturen bak skytjenestene de benytter. Dette gjelder både leveransemodell (offentlig/hybrid/privat), eller oppbygging av selve løsningen eller back-up løsning, inkludert sikkerhetstiltak som kryptering.

Som diskutert under kapittel 7.2 kan valg av leveransemodell få betydning for datasuvereniteten fordi de tekniske aspektene av skytjenesten bør tilpasses til typen data som skal lagres. Kommunens mangel på innsikt i skytjenestenes tekniske oppbygging kan dermed påvirke datasuverenitet ved at det er mer tilfeldig om løsningene er optimale for formålet og dataen som skal lagres, spesielt med tanke på sikkerhetsnivå og tiltak.

Private skytjenester anses som regel som positive for beskyttelse av data, fordi skytjenesten tilgjengeliggjøres kun for de virksomhetene som tjenesten gjelder for, som åpner for mer spesifikke kundetilpasninger enn andre leveransemodeller (Datatilsynet, 2018c). Det er derimot ikke slik at privat sky alltid er det beste for å sikre sine egne data. Likevel, siden de som anskaffer skytjenestene ikke har et forhold til leveransemodell, er det potensielt kun tilfeldigheter, eller leverandørens anbefalinger for utforming, som påvirker om tjenesten er utformet på en måte som komplementerer dataene som skal lagres.

Det er også svært liten innsikt i øvrige aspekter ved datamodellen, slik som sikkerhetsstrukturene som skal beskytte kommunens data. NSM viser til at alle seriøse skyleverandører skal ha en «omfattende vurdering av sikkerheten som er gjennomgått av en eller flere tredjeparts revisjonsvirksomheter» (Nasjonal sikkerhetsmyndighet, 2020b). Denne typen opplysninger kan kunden få tilgang til for å vurdere om skytjenesteleverandøren har det ønskelige sikkerhetsnivået (Nasjonal sikkerhetsmyndighet, 2020b). Bruk av denne typen opplysninger for å vurdere skytjenester forutsetter at kommunen har kompetanse til å forstå slik informasjon. Som empirien viser inkluderes hverken personvernombud eller IKT/IT-avdeling ofte tidlig nok i innkjøpsprosessen, som er de aktørene i kommunen som potensielt har kompetanse på slike områder. Det kan være et potensiale for kommunen å bruke opplysninger fra leverandør mer aktivt for å sikre at tjenestene ivaretar datasuverenitet og øvrige krav.

Den desentraliserte organiseringen fører også til at fokuset i kommunen ikke er på IT-arkitekturen til løsningen, men på funksjonene den skal utfylle som fagsystem ute i avdelingene. Derimot viser NSM til at verdivurderinger av data, som diskutert under kapittel 7.2, og risikovurderinger av tjenesteutsettelse bør gjøres først, før konkrete utforminger av

løsninger vurderes. De har derimot erfaring med at virksomheter først presenterer potensielle løsninger som vurderes å kjøpes, før slike analyser gjennomføres, og beskriver dette som en uheldig rekkefølge (Nasjonal sikkerhetsmyndighet, 2020b). Ved å ha fokus på leveransen først risikerer dermed kommunen at datasuverenitet ikke er integrert i IT-arkitekturen til løsningen, fordi teknisk utforming enten er utenfor kompetanseområdet til de som gjør anskaffelsen, eller IKT/IT-avdelingen blir inkludert for sent i prosessen.

Det er også viktig å poengtere at selv om kommunen benytter seg av tjenesteutsetting i form av skytjenester, så er det fremdeles kommunen som har overordnet sikkerhetsansvar, uansett hvor mye av dette arbeidet skyleverandøren tar på seg i delt ansvar (Nasjonal sikkerhetsmyndighet, 2020b). Eksempelvis må kommunen sikre seg at dataen beskyttes i transitt til skytjenesten, i bruk og der den er lagret (Nasjonal sikkerhetsmyndighet, 2020b). Kommunen har svært liten innsikt i hvordan databehandler lagrer, flytter og behandler deres data, som medfører at en ikke vet om alle disse punktene er ivaretatt. Igjen er det stor tillit til at leverandøren har kontroll på og ordner de tekniske aspektene som ikke omhandler selve program-/systemutformingen, selv om kommunen har ansvar for å sikre at leverandør gjør dette. Kommunen mangler et overordnet fokus på utforming av tekniske aspekter ved skytjenestene, og dette kan få betydning for dataens sikkerhet. Dette kan ikke skyldes på enkeltansatte nede i fagavdelingene som har som ansvar for å finne og gå til innkjøp av skytjenester, fordi disse ikke har teknisk bakgrunn eller opplæring for å ha grunnlag fir å hensynta slike aspekter. Det er derimot ledelsen i kommunen som har ansvar for at slike forhold blir tatt hensyn til, og en kan dermed peke på manglende strategi på ledelsesnivå som avgjørende for hvorfor kommunen ikke integrerer datasuverenitet i alle aspekter av IT-arkitekturen i skytjenester.

7.3.2 Lovgivningen som rammeverk for kommunens arbeid med skytjenester

Lovgivningens påvirkning på datasuverenitet henviser til betydningen av nasjonalstater i arbeid med datasuverenitet, fordi det er den norske stat, og EU, som utformer lovgivningen kommunen følger om datalagring. Det er dermed viktig å ha et systemperspektiv på datasuverenitet, fordi forhold og aktører utenfor kommunen, slik som lovgivning, danner et rammeverk for hvordan kommunen kan og bør arbeide med skytjenester og datalagring. og fremhever viktigheten av å ha et systemperspektiv på datasuverenitet fordi det setter kommunens arbeid i lys av å vær del av et større system.

Fra empirien kommer det frem at kommunen har et bevisst forhold til lovgivning som kan påvirke datalagring. Kommunen opplever på den ene siden lovverket som komplisert, og i

visse tilfeller rigid og upassende for prosjekter og aktiviteter av mindre størrelse som gjennomføres i kommunen. Dersom lovverket er for komplisert, eller ikke tilpasset til virkeligheten i norske virksomheter, kan lovverket oppleves som et hinder for datasuverenitet. Et for komplisert, eller restriktivt, lovverk vil gjøre det vanskelig for kommunen å følge alle krav, selv om intensjonen med lovverket i utgangspunktet er god. Et lovverk som ikke er tilpasset det praktiske behovet fører til at man enten overser lovverket, eller at nye innovative løsninger ikke tas i bruk. En studie fra 2012 fant at kommunal regeletterlevelse blir påvirket av en etterlevelsesillusjon (Tranvik, 2012). Etterlevelsesillusjonen manifesterer seg i at kommunale dokumenter som beskriver regeletterlevelse er svært like og fremstår lojale til etterlevelsen som kreves i lovgivningen. Derimot er etterlevelsen i praksis svært forskjellig fra dette. Dette skyldes ikke at kommunen forsøker å «lure» andre rundt seg til å tro at de følger reglene – de ønsker å gjøre som regelverket krever, men hindres i dette av interne barrierer (Tranvik, 2012, s. 132).

Dette er interessant for denne studien, da det i hovedsak er undersøkt hvordan informantene opplever aspekter av datasuverenitet i praksis. Eksempelvis kan vi da se på tilfellet med kontroll over geografisk plassering av data versus fokus på jurisdiksjon. På et generelt spørsmål om hvordan informantene forholder seg til usikker jurisdiksjon der leverandør eller lagringssted befinner seg, svarer informantene at dette vil gjøre at de etterspør informasjon eller velger bort leverandøren. Derimot er det flere, på konkret spørsmål om hvor dataen tilhørende systemet/systemene de er ansvarlig for er lagret, som sier at det er de ikke klar over, eller at det *bør* stå i databehandleravtalen. Dersom en IKT-tjeneste som skylagring skal leveres fra utlandet, anbefaler NSM å vurdere både tjenestetilbyderen og vertslandet der tjenesten tilbys fra og leverandøren oppholder seg (Nasjonal sikkerhetsmyndighet, 2020c, s. 15). Det virker som om kommunen som regel forholder seg til det lovverket krever med tanke på jurisdiksjon når dette gjelder personvern og lagring i EU. Derimot vises det at øvrige leverandører som skal levere tjenester som ikke gjelder persondata, for eksempel Microsoft som er basert i USA, blir godtatt selv kommunen foretrekker å unngå USA for lagring av data. Ved å ikke ha et konsekvent forhold til hvilke landområder en velger å unngå, selv om dette ikke er krevd i lovverket for annet enn persondata, risikerer dermed kommunen å lagre øvrig data i områder der jurisdiksjon kan få negativ påvirkning på datasuverenitet.

For kommunen er det spesielt GDPR som blir vist til at setter rammer og påvirker hvordan kommunen arbeider med skytjenester. Dette vises i kommunens forhold til bruk av databehandleravtaler som viktig virkemiddel, og som nevnt tidligere under kapittel 7.2, fokus

på personvern og personopplysninger. Selv om lovverket oppleves som komplisert, oppfattes det dermed også som et virkemiddel og noe å lene seg på, i dialog med leverandører. Et konkret lovverk med tilhørende virkemidler slik som databehandleravtaler, kan dermed sees som positivt for datasuverenitet, fordi det faktisk blir benyttet og gir kommunen holdepunkter for sitt eget arbeid. Likevel oppleves også lovverket rundt spesielt personopplysninger som så restriktivt at det ikke passer kommunens mangfoldige drift, som omfatter både store og svært små prosjekter. Dersom dette fører til at aktører i kommunen velger å benytte seg av tjenester til tross for dette, er det potensielt svært negativt for datasuverenitet fordi ordentlige vurderinger ikke blir gjennomført. Dette kan i stor grad løses ved at overordnede aktører forhåndsgodkjenner en mengde tjenester på vegne av kommunene, som har begrenset med ressurser og tid til å gjennomføre slike analyser.

Der personopplysningsloven setter rammeverk for personopplysninger, og sikkerhetsloven setter rammeverk for informasjonssikkerhet tilknyttet nasjonale sikkerhetsinteresser, mangler det derimot liknende verktøy som kan ramme all ønskelig data. Dette kan være en av grunnene til at virkemidler som databehandleravtaler, omtales av kommunen som verktøy for å beskytte all data, selv om formålet med databehandleravtaler formelt er å sikre at personopplysninger blir behandlet i tråd med regelverket (Datatilsynet, u.å.-a). Det kan også forklare hvorfor det kommer frem av empirien at kommunen har mer fokus på persondata, eller som presisert av informant L (Daglig leder, rådgivende org), at de antakeligvis er bedre på personvern enn informasjonssikkerhet.

7.4 Hvilken ledelsesstrategi benytter kommunen i arbeid med skytjenester?

I kommunen finnes aspekter av alle de fire ledelsesstrategiene presentert i teorikapittelet. I mangel på offisielle strategier eller planverk i kommunen som gjelder datasuverenitet, er ikke disse vedtatte strategier, men de blir synlige gjennom kommunens håndtering av karakteristikkene av datasuverenitet i skytjenestene de benytter.

7.4.1 Lovverk som ledelsesstrategi

Kommunen benytter lovverket som et utgangspunkt for å sikre kontroll over og rettigheter til egne data. Foruten den faglige utformingen av den ønskede løsningen eller tjenesten, trekkes spesielt GDPR og persondata frem som utgangspunkt for hvilke krav kommunen setter overfor databehandler.

En fallgruve med denne ledelsesstrategien er at slike betraktninger i kommunen i hovedsak blir gjort ved inngåelse av kontrakter og avtaler, slik som databehandleravtaler. Databehandleravtaler er i kommunen påpekt som et viktig virkemiddel for å sikre at både lovverket, og kommunens egne krav, blir holdt av leverandør. Å benytte lovverk som ledelsesstrategi blir derimot begrenset dersom dialogen med leverandør ikke opprettholdes jevnlig fra både kommunens og leverandørens side, etter inngåelse. Datatilsynet beskriver at bruk av kontrollerende elementer er viktig, fordi de bidrar til å fange opp avvik fra systemet via periodiske gjennomganger. Kontrollerende elementer inngår i hvordan en virksomhet kan etablere internkontroll for å sikre informasjonssikkerhet, spesielt rettet mot personopplysninger (Datatilsynet, 2018a). Undersøkelser viser at det er svakheter i norske kommuners arbeid med å «etablere og vedlikeholde systematisk internkontroll på informasjonssikkerhetsområdet» (Digitaliseringsdirektoratet, 2020, s. 2). Selv om innkjøpsprosessen oppfattes som et viktig område for å sikre krav relatert til datasuverenitet, og kommunen aktivt benytter dette som et virkemiddel for å følge lovgivning, vil det ikke sikre datasuverenitet i det lange løpet dersom forhold ikke følges opp av enten kommunen eller leverandør.

Det er også begrensninger i innholdet i lovgivningen i seg selv, som kan påvirke bruken av denne ledelsesstrategien. Kommunens håndtering av datasuverenitet er i stor grad avhengig av den nasjonale tilnærmingen både via lovverk, strategier og veiledninger. Fordi GDPR og personopplysningsloven setter krav til blant annet eierskap av data, forholdet mellom databehandler og behandlingsansvarlig og geografisk plassering, fyller det i stor grad kravene som vil være ønskelig for å ivareta datasuverenitet ved bruk av skytjenester, som ikke ivaretas i annen lovgivning for data som ikke defineres som persondata.

I stedet for å stille spørsmål om hva som skal til for at norske kommuner og virksomheter på eget initiativ skal gjøre for å sikre datasuverenitet, kan man reise spørsmål om lovverket bør utvides for å inkludere datasuverenitet over all data, ikke kun persondata, arkivverdig informasjon eller data som faller under sikkerhetsloven. En slik tilnærming vil flytte diskusjonen ut fra kommunen, og lenger opp i systemet til myndighetsnivå. Mekanismene og rådgivningen eksisterer allerede, men de er i stor grad koblet til personopplysninger. Kommunen på sin side anser virkemidler som databehandleravtaler som nyttig for å sikre kontroll over øvrige typer data allerede. Vi ser også at lovgivningen har ført til at det allerede eksisterer kompetanse innad i kommunene, i form av personvernombud og roller for informasjonssikkerhet, men som empirien her har pekt på brukes ikke deres kompetanse og

ekspertise godt nok utover i kommunen. Hvis fokus rundt tiltak for persondata i enda større grad ville blitt benyttet for alle typer data, som det i tilfellet rundt databehandleravtaler allerede i en viss grad blir brukt, kunne datasuverenitet i enda større grad blitt ivaretatt i kommunene, uten å innføre nye metoder.

Der Norge per i dag kun har en strategi rundt datalagring som i hovedsak anbefaler skylagring, og først og fremst begrenses av GDPR-reglement for persondata, er det andre land som har mer offensive strategier med et bevisst forhold til datasuverenitet. Tyskland har etablert en egen statlig «sky» for å skape uavhengighet av eksterne leverandører i det offentlige. Arbeidet ble påbegynt i 2013 og plattformen ble etablert i 2017. Tysklands strategi påpeker at private leverandører av skytjenester kun skal benyttes om staten ikke kan tilby en tilstrekkelig tjeneste (Stach, 2020), noe som står i sterk kontrast til den norske strategien der det anbefales å benytte skytjenester så langt dette er den mest kostnadseffektive løsningen, gir best resultat, og ikke strider mot andre viktige hensyn (Kommunal- og moderniseringsdepartementet, 2016, s. 4). BRICS-landene (Brasil, Russland, India, Kina og Sør-Afrika) tatt en mer aktiv tilnærming til datasuverenitet, blant annet gjennom å signere en avtale i 2012 som innebærer å styrke suverenitetsrettigheter og ta aktiv styring over internett (Polatin-Reuben & Wright, 2014, s. 2). Daværende president i Brasil har vært en forkjemper for at utenlandske skyleverandører måtte lagre brasilianske data på servere i Brasil, mens Russland ved Putins styre har økt reguleringer relatert til datasuverenitet siden 2012 (Polatin-Reuben & Wright, 2014, s. 3-4). Kina har på sin side tatt i bruk et nasjonalt intranett med stor bruk av sensur som har muliggjort et eget «internettøkosystem» (Polatin-Reuben & Wright, 2014, s. 4).

Likevel er det ikke slik at et offentlige initiativ nødvendigvis er den beste måten å sikre datasuverenitet på. Et statlig ledet initiativ med tilhørende krav for offentlige virksomheter om å benytte offentlig skylagring, vil både kunne styrke og svekke datasuverenitet. På den ene siden gjør man det offentlige mindre avhengige av markedsaktører med offentlige tjenester, mens på den andre siden vil bruk av private aktører kunne styrke sikkerheten ved skytjenester og datasentre fordi de har ressurser og kompetanse til å drive innovasjon og teknologi fremover, og håndtere skytjenester på en sikker måte, som det ikke nødvendigvis finnes kompetanse eller ressurser til i det offentlige.

Spesielt relevant er dette på kommunenivå, som eventuelt ville vært avhengig av at slike initiativ ble startet på nasjonalt nivå om det i det hele tatt skulle vært aktuelt, fordi de ikke har nok ressurser eller kompetanse til å drive frem slike store prosjekter. NSM påpeker i sin siste

rapport om datasentre og dataautonomi at det ikke er diskusjonen om privat eid fremfor offentlig eid som er sentral, men at en skal kunne ha trygghet til at virksomheter og brukere får tilgang til sine data under alle omstendigheter (Nasjonal sikkerhetsmyndighet, 2022). Som vist i oppgavens empiri, trekkes det frem at bortfall av skytjenestene ville fått stor betydning for kommunens evne til å levere tjenester utover i kommunen. I sin rapport viser NSM til at nettopp bortfall av datasentre spesifikt vil skape utfordringer for mange virksomheter, og potensielt få store konsekvenser for evnen samfunnet har til å levere digitale tjenester. De argumenterer dermed for at det norske arbeidet med digitalisering bør fokusere på verdien av å sikre og skape robuste datasentre som befinner seg i Norge (Nasjonal sikkerhetsmyndighet, 2022).

Med den lovgivningen og anbefaling som foreligger i dag er det derfor ikke nødvendigvis negativt at kommunen benytter private selskaper som leverandør for skytjenester, og dette kan i flere tilfeller gi bedre sikkerhet og kontroll enn dersom kommunen eller øvrige offentlige aktører skulle etablert andre alternativ.

7.4.2 Teknisk tilnærming som ledelsesstrategi

En teknisk tilnærming til datasuverenitet i kommunen, innebærer som gjennomgått i oppgavens teorikapittel, fokus på å integrere datasuverenitet i IT-arkitekturen, gjennom å se på hvilke rutiner som må etableres, for eksempel kryptering og tilsyn.

Denne strategien er i en viss grad til stede, men tilsynelatende svært vilkårlig og personavhengig utover i fagavdelingene i kommunen. Det mangler faste etablerte rutiner, praksis og protokoller, eller kunnskap om de eventuelle rutinene som eksisterer. Undersøkelser viser at små og mellomstore kommuner i mindre grad enn store kommuner har skriftlige informasjonssikkerhetspolicyer eller fagansvarlige for informasjonssikkerhet. Det medfører at de i mindre grad har evaluert, forbedret eller fornyet sitt styringssystem som omhandler informasjonssikkerhet (Digitaliseringsdirektoratet, 2020, s. 7). Desentralisering og mangel på etablerte rutiner eller kunnskap har i kommunen ført til en fragmentert tilnærming til karakteristikkene av datasuverenitet, når det kommer til skytjenester. Dette medfører at ivaretakelse av datasuverenitet via denne ledelsesstrategien blir mer tilfeldig og i stor grad personavhengig.

Det er derfor i varierende grad bruk av en teknisk tilnærming i form av kontrollmekanismer som revisjoner, tilsyn og innsikt i IT-arkitekturen eksempelvis kryptering og monitorering. Informantene begrunner den begrensede bruken i mangel på teknisk kompetanse om

skytjenester, og ressurser og tid tilgjengelig for å gjennomføre slikt arbeid. Kommunen er dermed avhengig av et tillitsforhold til leverandør, om at de følger de spesifikasjonene og kravene som er satt i innkjøpsprosessen eller som generelt forventes av en tjenesteleverandør. Variasjon i fremgangsmåte er dermed positivt for kommunen i de tilfellene der det finnes personlig kompetanse eller avdelingsrutiner, men negativt der dette ikke eksisterer og flere aspekter blir overlatt til tilfeldigheter eller leverandør.

Det er imidlertid etablert ett sentraliserende tiltak, i form av kompetansegrupper slik som Digitaliseringsrådet, som skal formalisere og strømlinjeforme prosessen ved anskaffelse av nye digitale løsninger. Ved å ha fokus på faktorer ved datasuverenitet, eksempelvis slik kommunen nå gjør med Digitaliseringsrådet via å identifisere tilholdsland i gjennomgangen før anskaffelse, allerede i innkjøpsprosessen, kan kommunen bygge datasuverenitet inn i IT-arkitekturen til alle nye løsninger. Derimot vil dette ikke påvirke de systemene og løsningene som kommunen allerede har i sky, og som gjennomgått under kapittel 7.4.1, er det utfordrende for kommunen å benytte slike kontrollmekanismer som Datatilsynet oppfordrer til å gjennomføre, for å kontrollere at vilkår som er etablert blir holdt.

7.4.3 Fokus på epistemiske utfordringer som ledelsesstrategi

Å tilnærme seg datasuverenitet gjennom å redusere epistemiske utfordringer, er til stede i kommunen, hovedsakelig via fokus på at leverandøren skal informere om behandling av persondata og personvern. Informantene henviser til etterlevelse av GDPR, informasjon om Schrems II og databehandlingsavtaler som virkemidler ved bruk av skytjenester, for å sikre at personvernet ivaretas. Stort fravær av dataklassifisering vitner derimot om at denne ledelsesstrategien potensielt kunne blitt utnyttet bedre, ved å gjennomføre ordentlige dataklassifiseringer for hvert system, som igjen kunne bidratt til å utforme IT-arkitekturen på en måte som beskytter kommunens data enda bedre.

For å minske epistemisk usikkerhet må kommunen også ha bevissthet om hva deres egne data brukes til og hvor de behandles. Eksempelvis vil dette bety at all data, inkludert metadata, må kontrolleres og kategoriseres. Dette kan også få betydning for om underleverandører eller utviklere får tilgang til reelle eller fiktive datasett. Informasjon som i utgangspunktet ikke defineres som skjermingsverdig, kan skifte status til skjermingsverdig dersom den blir lagret i en skytjeneste eller datasenter som også lagrer informasjon om andre samfunnsfunksjoner (Kommunal- og moderniseringsdepartementet, 2016, s. 11). Kommunen har fokus på bruk av databehandleravtaler, der slike forhold kan og bør presiseres. Det er derimot i varierende grad at informantene har oversikt om slike forhold faktisk blir satt krav til i databehandleravtalen,

og i enda mindre grad om de følges opp jevnlig etter inngåelse av avtalene. Uvissheten kan dermed bety at datasuvereniteten enten ikke blir ivaretatt på dette området, eller at det er mer tilfeldig og opp til leverandøren om det er ivaretatt.

7.4.4 Promotere grunnleggende komponenter ved data som ledelsesstrategi

Fordi en grunnleggende komponent av datasuverenitet er dataens natur, vil datasuverenitet kunne påvirkes fordi dataen er enkle å kopiere, til lav kostnad, uten at kvaliteten tapes (Hummel et al., 2021). Dette kan utgjøre en trussel for dataene kommunen lagrer og behandler i skytjenester, dersom uvedkommende får tilgang til dataene. Tiltak slik som kryptering av data og splitting av data til flere enn ett senter, kan dermed være virkemidler for denne strategien. Det er svært begrenset hvor god innsikt kommunen har i slik praksis hos leverandørene, og det er ikke registrert at kommunen selv setter krav til dette. Sikring av kryptonøkler som brukes til å låse opp kryptert data anses som en absolutt forutsetning for å ivareta konfidensialitet og integritet ved data. Dette kan håndteres av enten skytjenesteleverandøren, en tredjepart eller kommunen selv, og er avhengig av kompetansenivå og tilgjengelige ressurser. Å kryptere data vil både beskytte den mot utro tjenere hos skyleverandøren, mot trusselaktører generelt, men også mot at tjenesteleverandøren blir beordret til å utlevere data av egne myndigheter. Dette krever derimot at krypteringen ikke kun skjer i selve datasenteret til leverandøren (Nasjonal sikkerhetsmyndighet, 2020b). Fordi kommunen ikke har fokus på dette selv, er de avhengig av at tjenesteleverandøren eller en tredjepart tar seg av krypteringen. Dersom det ikke stilles krav til dette er det derimot ikke sikkert i hvilken grad slike tiltak gjennomføres, og dermed om datasuvereniteten er ivaretatt.

Den andre grunnleggende komponenten er at dataene er kontekstavhengige, og henger sammen med lovgivningen, skikker og normer i landet dataen kommer fra. Innbyggere i norske kommuner forventer at kommunene skal forvalte data på en forsvarlig måte, og kommunene etterstreber å følge både det norske lovverket og EU/EØS-regulativ. Denne strategien vil bety at også andre land, eksempelvis de landene der datasentrene befinner seg, potensielt vil ha sin egen forståelse av strategien for å oppnå datasuverenitet. For denne strategien må kommunen derfor fokusere på motstridende eller usikker jurisdiksjon i land som kan påvirke egen data i sky.

Som gjennomgått er det bevissthet rundt jurisdiksjon i kommunen, og hvordan dette kan få negative innvirkninger på kommunens data lagret i sky. Derimot er denne ledelsesstrategien ikke helt konsekvent i kommunen. I enkelte tilfeller er det avslått leverandør og tjeneste på

grunn av tilknytning til USA, mens det i andre tilfeller har blitt akseptert løsninger fra samme sted fordi disse var nødvendige. Det er også, som gjennomgått, interessant at det påpekes fokus på jurisdiksjon, til tross for at flere av informantene er usikre på hvor dataene tilknyttet systemene de er ansvarlige for, er lagret. I de tilfellene der dette sammenfaller vil en dermed risikere at datasuvereniteten ikke er ivaretatt, og at dersom den er det, er det grunnet tilfeldigheter eller leverandørens initiativ.

7.5 Hvilke utfordringer møter kommunen i arbeid med skytjenester?

Som presentert i teorien er utfordringene tilknyttet datasuverenitet, i likhet med ledelsesstrategiene, kategorisert etter fire underkarakteristikker rundt grunnleggende komponenter av datasuverenitet, teknisk design, lovgivning og epistemisk usikkerhet.

7.5.1 Utfordringer knyttet til lovgivning

Utfordringene tilknyttet lovgivning er i hovedsak relatert til at lovgivningen oppleves som kompleks og i stadig endring. Empirien viser til at ansvarlige for skytjenester er fagpersoner uten juridisk bakgrunn, og at den desentraliserte tilnærmingen til håndtering av skytjenester fører til at de også må ha kunnskap om lovgivning og skytjenester. Det eksisterer god kompetanse på lovgivning i kommunen, hos personvernombudet. Derimot blir rollene med den største kompetansen, slik som personvernombud, ikke inkludert i den viktigste prosessen under anskaffelse. Dette kan vitne om mangel på struktur i kommunen som system, fordi de eksisterende ressursene blir benyttet i mindre grad enn de kunne blitt. En risikerer dermed at for eksempel databehandleravtalene, som anses av kommunen som et viktig virkemiddel for å følge lovverket og oppnå ønskede krav, ikke ivaretar aspekter ved data eller oppfølging som ønsket.

Som diskutert i forrige kapittel er det også utfordrende at lovverket i stor grad er konsentrert rundt persondata. Dette fører også til at kommunens fokus er sentrert rundt denne typen data, og at andre typer data potensielt ikke får like stor oppmerksomhet eller sikkerhetsfokus. Det utfolder seg også ved at det ikke gjennomføres dataklassifiseringer før skytjenester tas i bruk, unntatt oppfattes som persondata vil det gjennomføres vurderinger av risiko.

7.5.2 Utfordringer ved det tekniske designet av skytjenester

Utfordringene tilknyttet det tekniske designet av skyløsningene relateres i hovedsak til mangel på innsikt i, og kunnskap om, hvordan skytjenesten er utformet og hvordan dette igjen påvirker datasuverenitet ved valg av rett løsning for type data. Dette er i empirien identifisert som en stor utfordring, da kommunen i liten grad har innsikt i den tekniske utformingen av

løsningen, hverken leveransemodell eller datamodell inkludert sikkerhetstiltak som kryptering, tilgangsstyring eller redundans.

Som gjennomgått påvirkes denne utfordringen av at det sjelden gjennomføres dataklassifiseringer i forkant av innkjøp, eller at det er bevissthet rundt IT-arkitekturen i valgt løsning. Dersom kommunen ikke forstår egne data og grunnleggende egenskaper med disse, for eksempel om de er sensitive i form av personopplysninger eller virksomhetskritisk, vil det kunne føre til at skytjenestene som benyttes ikke følger de utformingene eller sikkerhetstiltakene som anbefales. Det kan likevel pekes på at en ansvarlig leverandør antakeligvis ønsker å oppfylle disse kravene. Eksempelvis er det antakeligvis igangsatt sikkerhetstiltak som kryptering, begrenset innsyn i data, og etterlevelse av GDPR uten at kommunen vet dette. Likevel er det en utfordring for kommunen å ikke ha innsikt i slike aspekter, fordi de bygger datasuvereniteten på tillit til leverandøren, uten å selv ta ansvar. Leverandøren kan benyttes som en ressurs, men det bør kombineres med dialog slik at kommunen er sikker på at de har den kontrollen de ønsker, og skal ha, over egne data. Dette ansvaret kan ikke settes ut fullstendig til tjenesteleverandøren, om datasuverenitet skal være ivaretatt.

Utfordringen ved det tekniske designet stammer antakeligvis også fra manglende teknisk kompetanse utover i kommunen. Fokuset blir dermed på at løsningen passer formålet, og mindre på de tekniske aspektene. Fordi myndighet delegeres lengre ned i organisasjonen kan en også risikere at lederne som befinner seg ute i kommunen har for lav bevissthet om at de er ansvarlige for IKT-sikkerheten og dermed ikke ivaretar denne rollen (Digitaliseringsdirektoratet, 2020, s. 7). Det er derfor potensiale for å inkludere IT-avdelingen mer for å sikre at også løsningens tekniske utforming benyttes som en sjanse til å integrere datasuverenitet i IT-arkitekturen. Selv om det har blitt påpekt at IT-avdelingen undergår kursing i nye skytjenester, er det et krevende arbeid å holde denne kunnskapen og kompetansen dagsaktuell, ettersom skyløsningene og deres leverandører har ukentlige oppdateringer og store endringer i både lisens og produkt, og ett kurs blir derfor ikke tilstrekkelig for å ha oppdatert kunnskap. Sikkerhetsarbeid er derimot også ofte kun én av mange oppgaver tilskrevet kommunens IT/IKT-miljø, som ofte er svært små (Digitaliseringsdirektoratet, 2020, s. 11), og det er dermed utfordrende om denne avdelingen skal måtte involveres i alle system og oppfølging av disse, om ressursene ikke strekker til.

7.5.3 Epistemisk usikkerhet som utfordring

Det er også store utfordringene og usikkerhetene hos kommunen tilknyttet epistemisk usikkerhet, spesielt usikkerhet som gjelder hva deres egne data brukes til og hvor de behandles.

Som sett på under kapittel 7.3.2, er jurisdiksjon en utfordring for kommunen, fordi det ikke er konsekvent hvordan man forholder seg til dette spørsmålet. Som presentert oppgir informantene at de har fokus på jurisdiksjon, som står i kontrast til at flere av informantene ikke er klar over hvor dataen i systemene de er tilknyttet er lagret. Selv om man er bevisst på at jurisdiksjon kan være utfordrende, poengteres det også at man i en visse grad velger å gå for tjenesten like vel, eksempelvis ved store USA-baserte selskaper. Dermed ser det ut til at selv om kommunen er bevisst på at dette kan være utfordrende med tanke på å ha kontroll på data, så er det andre ting som oppleves som viktigere. Eksempelvis at en tjeneste blir levert, eller formildende på det faktum at en benytter aktører fra uønskede land og områder, ved at en opplever det sikkert nok å ha databehandleravtale på plass også med disse aktørene.

Denne epistemiske utfordringen kan lett elimineres, ved å kreve innsyn i plassering for både tjenesteleverandør, lagringssted og underleverandører i databehandleravtalen. Derimot er det vanskeligere å ta stilling til eksempelvis om man skal godta bruk av amerikanske selskaper eller ei, og dette bør antakeligvis henge sammen med hvilken type data skytjenesten skal lagre for kommunen. Derfor er mangel på dataklassifisering også en stor utfordring for kommunen, fordi dataklassifisering og dermed å bygge skytjenesten rundt typen data identifisert, ville gitt mer fokus på nødvendige sikkerhetstiltak og oppbygging av selve skytjenesten.

7.5.4 Utfordringer med grunnleggende komponenter ved data

Utfordringene tilknyttet de grunnleggende komponentene av datasuverenitet omhandler dataens natur og at dataen er konktekstavhengig.

Om uvedkommende får tak i dataene er de enkle å kopiere eller endre til relativt lave kostnader. Utfordringen knyttes av informantene til digitalisering og bruk av teknologi generelt, og gjelder dermed ikke kun for skytjenester. Det er dermed det faktum at dataene er digitale, og for eksempel kan tilgjengeliggjøres av hackere eller falle bort på grunn av teknisk svikt, som anses som en utfordring av kommunen.

Det er derimot negativt at kommunen har begrenset med innsyn i, og setter tilsynelatende lite krav til, praksis som kan beskytte dataen for å bli kopiert og endret. Selv om bare én av informantene viser til praksis hos leverandør med kryptering, splitting på flere datasentre og

tilgangsstyring hos leverandør, kan en likevel anta at dette er i bruk hos flere leverandører som i lys av å være en seriøs aktør, ønsker å beskytte sine kunders data. Selv om en kommune benytter tjenesteutsetting, er det fremdeles kommunen som er behandlingsansvarlig, og som må kontrollere at vilkår i lovverket blir fulgt av leverandør. Kommunen bør derfor ta flere steg for å sikre seg at dette stemmer, for å ivareta datasuverenitet.

Fordi dataen er kontekstavhengige (Hummel et al., 2021, s. 7), er det også svært utfordrende å ikke ha innsikt i hvilken jurisdiksjon dataene, eventuelt tjenesteleverandør, ligger under. Som diskutert over, kan denne utfordringen løses ved å kreve innsyn i hvor dataen, eventuelt leverandør og underleverandør, er plassert. Likevel, fordi dataens natur tillater at denne flyttes rundt etter der det er kapasitet for lagring og behandling i lagringsnettverket, er det nødvendig for kommunen å etterspørre denne informasjonen jevnlig, og ikke kun under selve kontraktsignering slik det er praksis for nå, i forbindelse med inngåelse av databehandleravtale. Fordi kommunen ikke har ressursene til å følge opp alle avtalene de har for skytjenester, risikerer de dermed at datasuvereniteten ikke blir ivaretatt dersom leverandør tar valg som kan påvirke hvilken jurisdiksjon dataen ligger under, for eksempel ved å flytte data uten å informere kommunen.

8. Konklusjon

Fokuset i oppgaven er hvordan karakteristikker for datasuverenitet ivaretas i en norsk kommunes arbeid med skylagring, samt hva de sentrale utfordringene i dette arbeidet innebærer. Gjennom informantenes innspill om kommunens arbeid med skytjenester har det kommet frem verdifulle innsikter om hvordan datasuverenitet ivaretas i dette arbeidet.

Kommunen er godt på vei til å ha fokus på og ivareta de aspektene av datasuverenitet som er knyttet til konkrete krav i lovverket, spesielt vedrørende individuell dimensjon. De er opptatt av å følge GDPR og benytter seg av databehandleravtale, selv om det er presisert at innkjøpet ofte kommer i første rekke før personvernombud involveres i prosessene. Det eksisterer også kompetanse på relevante områder for datasuverenitet i kommunen, hos IT-avdeling, personvernombud og enkeltindivider med enten erfaring med eller interesse for skytjenester. Det er opprettet en intern styringsgruppe i form av Digitaliseringsrådet, som tar for seg relevante aspekter av datasuverenitet i innkjøpsprosessen.

Fra diskusjonen kommer det derimot frem at de identifiserte karakteristikkene av datasuverenitet som ivaretas, i stor grad er avhengig av tilfeldig eller ikke-rutinebasert praksis som varierer fra avdeling til avdeling og person til person. Den interne kompetansen som

eksisterer i kommunen blir ikke benyttet på systematisk måte via rutiner, og på grunn av den desentraliserte organiseringen blir beslutninger om skytjenester tatt av ansatte uten kompetanse på hverken skytjenester eller sikkerhet. Dette fører til at kommunen er avhengig av at tjenesteleverandørene gjennomfører mye av arbeidet som trengs for å ivareta datasuverenitet.

De største utfordringene for ivaretakelse av datasuverenitet ligger i mangel på gjennomføring av dataklassifisering, for lite kompetanse om hvordan skytjenesters IT-arkitektur bør tilpasses data og ønsket sikkerhetsnivå, mangel på relevante rutiner for anskaffelser, kjennskap til disse rutinene, liten bruk av intern kompetanse, og ikke minst for få ressurser til avtaleforvaltning. Det er også mindre fokus på data med betydning for kollektiv dimensjon.

Fordi kommunens bruk av skytjenester ivaretas av private aktører, kan en derimot anta at flere av disse manglende fokusområdene fra kommunens side, ivaretas av leverandøren. Datasuvereniteten er derfor potensielt mer ivaretatt enn kommunens arbeid tilsvarer at den skulle vært, fordi leverandørene er profesjonelle og kompetente. Derimot blir dette kun en antakelse, og det eksisterer dermed stor usikkerhet rundt områder som kan bidra til å ivareta datasuverenitet bedre i kommunen.

Selv om beslutninger rundt skytjenester, og dermed faktorer som omhandler datasuverenitet, i stor grad blir tatt ute i avdelingene i kommunen, kan en ikke skylde på enkeltansatte for at datasuverenitet ikke er ivaretatt. Det er kommunen som system som må sørge for at de har nok kompetanse og rutiner for å beskytte egne data på ønskelig måte. Digitaliseringsrådet er dermed ett steg på vei i riktig retning, men avtalene må også følges rutinemessig opp etter inngåelse. Det er likevel viktig at aspekter ved datasuverenitet ikke sentraliseres i for stor grad, fordi en da ender opp med løsninger som ivaretar datasuverenitet, men ikke behovet de er ønsket for i fagmiljøene. Lovverket og medfølgende veiledninger for myndighetene, er også til en viss grad mangelfulle fordi de i liten grad tar hensyn til vern av all data som er ønskelig.

Jeg vil derimot argumentere for at løsningen på å ivareta datasuverenitet i norske kommuner ikke ligger i å ansette en datasuverenitetsekspert eller opprette en egen prosedyre for å kun fokusere på dette. Kommunen kan komme en lang vei og forbedre ivaretakelse av datasuverenitet på de viktigste utfordrende områdene ved å strømlinjeforme arbeidet som allerede gjøres ute i avdelingene. Ved å sikre at IT-avdelingen jevnlig kurses i skytjenester og tekniske løsninger, ha fokus på informasjonssikkerhet for all data, inkludere

personvernombudet tidlig i innkjøpsprosessen, klassifisere egen data og ha dialog med leverandør om utforming av tjenesten ut fra datatype, samt å sette av mer ressurser til avtaleforvaltning for å følge opp krav inngått i databehandleravtalen, vil kommunen komme ett steg opp og ut fra det nåværende lovverket ha god nok datasuverenitet. På denne måten kunne kommunen fått en mer effektiv utnyttelse av de ressursene de allerede har, uten at den enkelte person ute i fagavdelingene måtte blitt eksperter i både eget fagfelt, skytjenester og lovgivning. Mest utfordrende vil antakeligvis bevilgning av mer midler til oppfølging av kommunens store mengder systemer bli, da kommuner har svært begrenset med midler.

Jeg tror likevel at etter hvert som datasuverenitet, og liknende begreper som dataautonomi, blir mer velkjente og fokusert på, så vil også lovgivningen og rådgivning fra myndighetene føre til at vi ser en endring på samme måte som vi så etter GDPR ble innført, der kommunene måtte endre sin drift for å ivareta personvern i større grad.

8.1 Forslag til videre forskning

Denne studien er utformet som en case-studie for å se nærmere på fenomenet datasuverenitet i én kommune, og samtidig ha tid til å utforme et rammeverk for datasuverenitet som før denne studien ikke fantes. Det ville vært interessant å se dette rammeverket bli benyttet på en kvantitativ studie som inkluderte et større utvalg kommuner, for å undersøke om funnene fra denne studien går igjen i andre kommuner.

Etter hvert som datasuverenitet får mer oppmerksomhet og begrepet i seg selv blir mer kjent, ville det også vært spennende å gjennomføre en kvalitativ studie med myndighetsaktører og offentlige aktører rundt strategi for datasuverenitet og behovet for et nytt sikkerhetsbegrep.

I lys av at mange av utfordringene i denne studien kan knyttes til manglende kompetanse og ressurser, ville det også vært interessant om det ble gjennomført en kvalitativ studie som gjelder hvordan sikkerhetskultur påvirker ivaretakelse av datasuverenitet.

Referanser

Andersen, S. S. (2005). *Case-studier og generalisering - forskningsstrategi og design*. Fagbokforlaget.

Antonsen, S. & Haavik, T. K. (2012). Case Studies in Safety Research - Methodological Foundations, Challenges and Future Directions. I Kenneth Pettersen Gould & Carl Macrae (Red.), *Inside Hazardous Technological Systems* (s. 69-100). CRC Press.

Arkivloven. (1999). *Lov om arkiv* (LOV-1999-12-04-126). Kultur- og likestillingsdepartementet. https://lovdata.no/dokument/NL/lov/1992-12-04-126?q=arkivloven

Arkivverket. (2019, 13. januar 2021). *Skylagring og skanning i utlandet*. Hentet 23. februar 2022 fra https://www.arkivverket.no/for-arkiveiere/skylagring-og-skanning-i-utlandet#!#block-body-4

Boillat, T. & Legner, C. (2013). From on-premise software to cloud services: the impact of cloud computing on enterprise software vendors' business models. *Journal of theoretical and applied electronic commerce research, 8*(3), 39-58. https://www.mdpi.com/0718-1876/8/3/21

Bokføringsloven. (2004). *Lov om bokføring* (LOV-2004-11-19-73). Finansdepartementet. https://lovdata.no/dokument/NL/lov/2004-11-19-73

Couture, S. & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *new media & society, 21*(10), 2305-2322.

Datatilsynet. (2018a). *Etablere internkontroll*. Hentet 1. juni 2022 fra https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/

Datatilsynet. (2018b). *Rett til innsyn*. Hentet 3. juni 2022 fra https://www.datatilsynet.no/rettigheter-og-plikter/den-registrertes-rettigheter/rett-til-innsyn/

Datatilsynet. (2018c). *Skytjenester*. Hentet 1. juni 2022 fra https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/skytjenester/

Datatilsynet. (2020). *Utfyllende veiledning om Schrems II*. Hentet 23. februar 2022 fra https://www.datatilsynet.no/regelverk-og-verktoy/internasjonalt/retningslinjer-og-uttalelser-fra-personvernradet/utfyllende-veiledning-om-schrems-ii/

Datatilsynet. (u.å, 17. juli 2019). *Vurdering av personvernkonsekvenser (DPIA)*. Hentet 31. mai 2022 fra https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/

Datatilsynet. (u.å.-a, 20. desember 2019). *Hvordan lage en databehandleravtale*. Hentet 18. februar 2022 fra https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/hvordan-lage-en-databehandleravtale/

Datatilsynet. (u.å.-b). *Virksomhetenes plikter*. Hentet 18. februar 2022 fra https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/

De Filippi, P. & McCarthy, S. (2012). Cloud computing: Centralization and data sovereignty. *European Journal of Law and Technology, 3*(2).

Denzin, N. K. (2012). Triangulation 2.0. *Journal of mixed methods research, 6*(2), 80-88. https://journals.sagepub.com/doi/full/10.1177/1558689812437186

Departementene. (2019). Nasjonal strategi for digital sikkerhet. https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf

Digdir. (u.å.). *Hva er Schrems II-dommen*. Hentet 23. februar 2022 fra https://www.digdir.no/handlingsplanen/hva-er-schrems-ii-dommen/2581

Digitaliseringsdirektoratet. (2020). *Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner*. https://www.digdir.no/media/1102/download

Direktoratet for e-helse. (2020). *Veileder i bruk av skytjenester til behandling av helse- og personopplysninger*. https://www.ehelse.no/normen/veiledere/veileder-i-bruk-av-skytjenester-til-behandling-av-helse-og-personopplysninger

DSB. (2016). *Samfunnets kritiske funksjoner* https://www.dsb.no/rapporter-og-evalueringer/samfunnets-kritiske-funksjoner/

Elms, D. (2021). *Digital sovereignty: protectionism or autonomy?* Hinrich Foundation. https://www.hinrichfoundation.com/research/wp/digital/digital-sovereignty-protectionism-or-autonomy/

European Commission. (2021). *Standard Contractual Clauses (SCC)*. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

European Data Protection Board. (2020). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_en

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, *33*(3), 369-378.

Føyen, A. & Maanum, E. J. S. O. (2015). *Utredning av juridiske forhold ved bruk av nettsky i kommunal sektor - en mulighetsstudie* (KS FoU-posjekt 144008). Advokatfirmaet Føyen Torkildsen AS. https://www.ks.no/contentassets/f1eadbe0d27e4416a2fd2266005a91b9/sammendrag.pdf

GDPR.EU. (u.å). *Complete guide to GDPR compliance*. https://gdpr.eu/

Hollis, D. B. (2012). Stewardship versus Sovereignty? International Law and the Apportionment of Cyberspace. *International Law and the Apportionment of Cyberspace (March 19, 2012). Canada Centre for Global Security Studies, Cyberdialogue*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2038523

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M. & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, *45*(4), 3171-3189. https://link.springer.com/article/10.1007/s13369-019-04319-2

Hummel, P., Braun, M., Tretter, M. & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, *8*(1). https://journals.sagepub.com/doi/full/10.1177/2053951720982012

International Telecommunication Union. (2008). *Series X: Data networks, open system communications and security: Telecommunication security; Overview of cybersecurity*. https://www.itu.int/rec/T-REC-X.1205-200804-I

Kaloudis, M. (2021). Digital sovereignty–European Union's action plan needs a common understanding to succeed. *History Compass*, *19*(12), e12698. https://compass.onlinelibrary.wiley.com/doi/full/10.1111/hic3.12698

Khan, R. R. & Jebens, A. (2018). *Pågang av saker om «snoking» i arbeids-givers data-systemer*. Hentet 30. mai 2022 fra https://juristen.no/ditt-arbeidsliv/2018/10/p%C3%A5gang-av-saker-om-%C2%ABsnoking%C2%BB-i-arbeids%C2%ADgivers-data%C2%ADsystemer

Kommunal- og moderniseringsdepartementet. (2016). *Najonal strategi for bruk av skytenester*. https://www.regjeringen.no/contentassets/4e30afec51734d458596e723c0bdea0e/nasjonal_strategi_for_bruk_av_skytenester.pdf

Kristi Jackson & Bazeley, P. (2019). *Qualitative data analysis with NVivo*. SAGE Publications Ltd.
Krumsvik, R. (2015). Forskningsdesign og kvalitativ metode-ei innføring (2. utg.). *Oslo: Fagbokforlaget*.
KS. (u.å). *Informasjonssikkerhet og personvern*. https://www.ks.no/fagomrader/digitalisering/kompetanse-og-verktoy/informasjonssikkerhet-og-personvern/
Kvale, S. (2012). *Doing interviews*. Sage.
Kvale, S., Brinkmann, S., Anderssen, T. M. & Rygge, J. (2015). Det kvalitative forskningsintervju (2. utg.). *Oslo: Gyldendal akademisk*, 50-60.
König, P. D. (2017). The place of conditionality and individual responsibility in a "data-driven economy". *Big Data & Society*, *4*(2), 205395171774241. https://doi.org/10.1177/2053951717742419
Leseth, A. B. & Tellmann, S. M. (2014). *Hvordan lese kvalitativ forskning?* Cappelen Damm.
Li, Z., Liang, M., O'brien, L. & Zhang, H. (2013). The cloud's cloudy moment: A systematic survey of public cloud service outage. *International Journal of Cloud Computing and Services Science,*, *2*(5). https://arxiv.org/abs/1312.6485
Meld. St. 22 (2020–2021). *Data som ressurs— Datadrevet økonomi og innovasjon*. Kommunal- og distriktsdepartementet.
Mell, P. & Grance, T. (2011). *The NIST definition of cloud computing*. National Institute of Standards and Technology. http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf
Merriam-Webster. (u.å). *Jurisdiction*. Hentet 29. mai 2022 fra https://www.merriam-webster.com/dictionary/jurisdiction
Nasjonal sikkerhetsmyndighet. (2019). *Landvurdering ved tjenesteutsetting av IKT-tjenester*. Hentet 16.04.2022 fra https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/landvurdering-ved-tjenesteutsetting-av-ikt-tjenester
Nasjonal sikkerhetsmyndighet. (2020a). *NSMs Grunnprinsipper for IKT-sikkerhet*. https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/beskytte-og-opprettholde/ivareta-sikkerhet-i-anskaffelses-og-utviklingsprosesser/
Nasjonal sikkerhetsmyndighet. (2020b). *Ofte stilte spørsmål om sky og tjenesteutsetting*. Hentet 1. juni 2021 fra https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/ofte-stilte-sporsmal-om-sky-og-tjenesteutsetting/sporsmal-om-sky-og-tjenesteutsetting/
Nasjonal sikkerhetsmyndighet. (2020c). *Sikkerhetsfaglige anbefalinger ved bruk av tjenesteutsetting og skytjenester*. https://nsm.no/regelverk-og-hjelp/rapporter/sikkerhetsfaglige-anbefalinger-ved-tjenesteutsetting/om-temarapporten/
Nasjonal sikkerhetsmyndighet. (2022). *Temarapport om norske datasenter og digital autonomi*. https://nsm.no/regelverk-og-hjelp/rapporter/temarapport-om-norske-datasentre-og-digital-autonomi/sammendrag/
Njå, O., Sommer, M., Rake, E. L. & Braut, G. S. (2020). *Samfunnssikkerhet : analyse, styring og evaluering*. Universitetsforlaget.
NSD. (u.å.). *Fylle ut meldeskjema for personopplysninger*. Hentet 7. mars 2022 fra https://www.nsd.no/personverntjenester/fylle-ut-meldeskjema-for-personopplysninger/
Nugraha, Y. & Sastrosubroto, A. S. (2015). Towards data sovereignty in cyberspace. 2015 3rd international conference on information and communication technology (ICoICT),
NUPI. (u.å). *https://www.nupi.no/Publikasjoner/Innsikt-og-kommentar/Hvor-hender-det/HHD-fakta/Hva-er-en-jurisdiksjon.-hhd13-1*. Hentet 29. mai 2022 fra

Pedersen, E. (2019). *Dette må du huske på når du lagrer regnskapet i skyen*. Sticos. Hentet 23. februar 2022 fra https://www.sticos.no/fagstoff/categoryid/47/categoryname/regnskap/dette-maa-du-huske-naar-du-lagrer-regnskapet-i-skyen

Personopplysningsloven. (2018). *Lov om behandling av personopplysninger* (LOV-2000-04-14-31). Justis- og politidepartementet. https://lovdata.no/dokument/LTI/lov/2000-04-14-31

Peterson, Z. N., Gondree, M. & Beverly, R. (2011). A position paper on data sovereignty: The importance of geolocating data in the cloud. 3rd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 11),

Philpott, D. (2003, 22. juni 2022). *Sovereignty*. Stanford Encyclopedia of Philosophy,. Hentet 10. februar 2022 fra https://plato.stanford.edu/entries/sovereignty/

Polatin-Reuben, D. & Wright, J. (2014). An Internet with {BRICS} Characteristics: Data Sovereignty and the Balkanisation of the Internet. 4th {USENIX} Workshop on Free and Open Communications on the Internet ({FOCI} 14),

Posch, R. (2017). Digital sovereignty and IT-security for a prosperous society. I *Informatics in the Future* (s. 77-86). Springer, Cham. https://library.oapen.org/bitstream/handle/20.500.12657/28055/1001939.pdf?sequence=1#page=86

Seip, Å. A. (2020). *Sourcingstrategier for IKT i offentlig sektor: Om skytjenester og digitale veivalg i fire statlige virksomheter og fire kommuner*. Fafo. https://www.fafo.no/zoo-publikasjoner/fafo-rapporter/item/sourcingstrategier-for-ikt-i-offentlig-sektor-2

Shaikh, R. & Sasikumar, M. (2015). Data Classification for achieving Security in cloud computing. *Procedia computer science*, *45*, 493-498. https://www.sciencedirect.com/science/article/pii/S1877050915003233

Sikkerhetsloven. (2019). *Lov om nasjonal sikkerhet* (LOV-2018-06-01-24). Justis- og beredskapsdepartementet. https://lovdata.no/dokument/NL/lov/2018-06-01-24/kap7#kap7

Skogli, E., Aamo, A. W., Stormo, L. K. & Cimadamore-Werthein, G. (2019). *Verdien i data - hvordan sikre fellesskapets interesser?* (63/2019). Menon economics. https://www.forskningsradet.no/siteassets/publikasjoner/2019/verdien-i-data-hvordan-sikre-fellesskapets-interesser.pdf

Stach, H. (2020). *Data storage as a federal responsibility – The Bundescloud*. eForvaltningskonferansen 2020. https://medlem.ntl.no/Content/203742/attr=A07FFCC1CA09102FE0530100007F6BD6/Presentation%20of%20the%20Bundescloud%20at%20eForvaltningskonferansen%202020.pdf

Statistisk sentralbyrå. (2019). *Digitalisering i kommunene. Overblikk over tilstanden i 2018*. https://www.ssb.no/teknologi-og-innovasjon/artikler-og-publikasjoner/digitalisering-i-kommunene

Stortinget. (u.d., 15.10.2019). *Sentralmakt og lokalstyre*. Hentet 29.11.2021 fra https://www.stortinget.no/no/Stortinget-og-demokratiet/Storting-og-regjering/Folkestyret/Sentralmakt-og-lokalstyre/

Tranvik, T. (2012). Kommunal regeletterlevelse – Illusjoner og realiteter på personvernområdet. *Tidsskrift for samfunnsforskning*, *53*(2), 131-156. https://doi.org/10.18261/ISSN1504-291X-2012-02-01

van Hoek, R., Aronsson, H., Kovács, G. & Spens, K. M. (2005). Abductive reasoning in logistics research. *International journal of physical distribution & logistics management*.

von Solms, R. & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102. https://www.sciencedirect.com/science/article/pii/S0167404813000801
Whitman, M. E. & Mattord, H. J. (2021). *Principles of information security*. Cengage Learning.
Yin, R. K. (2014). *Case Study Research: Design and Methods* (6th ed. utg.). Sage.

Vedlegg

Vedlegg 1. Intervjuguide kommunale informanter

Intervjuguide kommunale informanter – masteroppgave i samfunnssikkerhet

Bakgrunn og forståelse av kommunen som system

1. Hva er din stilling i kommunen, og hvordan kommer dine arbeidsoppgaver i berøring med lagring og behandling av data i skytjenester?
    a. Hvilken erfaring eller opplæring har du i bruk av og anskaffelse av skytjenester i arbeidssammenheng?
2. Hva er ditt inntrykk av organiseringen av anskaffelser av, og bruk av, skytjenester i kommunen?
    a. Dersom det vurderes å anskaffe en ny skytjeneste i ditt arbeidsområde, hvordan går du frem?
    b. Hvilke ressurser og/eller kompetansepersoner opplever du at du kan benytte deg av i kommunen ved inngåelse av nye avtaler om skytjenester?

Datatype og valg av skytjeneste

3. Hvilken type data behandles i systemene/løsningene/tjenestene du arbeider med?
4. Kan du fortelle om dere benytter vurderinger slik som følsomhetsvurderinger, dataklassifisering eller kategorier basert på konfidensialitet og kritikalitet for data før overføring av data til skytjenester?
5. Hvilke faktorer opplever du som viktige i vurderingen av om en skytjeneste skal benyttes eller ei?
6. Hvilken type skytjeneste *(offentlig/privat/hybrid),* benyttes i systemene/løsningene/tjenestene du er tilknyttet?
    a. Hvordan kommer dere frem til hvilken form for skytjeneste som skal benyttes i de enkelte tilfellene?

Innsikt i skytjenestene

7. Hvilken innsikt har dere i hvor datasentrene tilknyttet skytjenestene dere benytter, geografisk befinner seg?
8. Hvilken innsikt har dere i hvordan databehandler lagrer, behandler og flytter deres data?

9. Hvordan kan dere få oversikt over, og styre hvem som har tilgang til data lagret i skytjenestene dere benytter, både internt i kommunen og hos databehandler?

Håndtering av skytjenester

10. Hvordan arbeider dere for å sikre at dere har kontroll over og rettigheter til egen data som behandles og lagres i skytjenester?
    a. Benyttes det spesifikke virkemidler, ressurser eller tiltak for å sikre denne kontrollen?
    b. Kan du forklare om dere arbeider likt eller forskjellig med å sikre kontroll over data, dersom dataen som skal lagres defineres som personopplysninger eller ikke?
11. I hvilken grad kan dere påvirke tilbudet og innhold i kontrakter og avtaler med en tjenesteleverandør av skytjenester?
12. Hvordan kan dere sikre at vilkårene i avtaler og kontrakter for skytjenester blir fulgt av databehandler etter inngåelse?
    a. Hvordan vil et eventuelt brudd på kontraktsforhold følges opp, og har du erfaring med at det har vært behov for reaksjoner overfor databehandler frem til nå?

Utfordringer og krav

13. Hvordan vil bortfall av de nåværende skytjenestene påvirke tjenestene dere leverer?
    a. Hvilke back-up-løsninger har dere i tilfelle bortfall av nåværende tjenester som er basert i sky?
14. Kan du beskrive om dere opplever usikkerheter eller utfordringer tilknyttet kontroll over, og rettigheter til, egne data lagret i skytjenester?
15. Hvordan forholder dere dere til lovgivning som kan sette krav til data lagret i skytjenester?
16. Kan du fortelle hvordan dere forholder dere til mulig usikkerhet i jurisdiksjon vedrørende rettigheter til innsyn i data? Eksempelvis jurisdiksjon som kan medfølge ved bruk av datasentre eller databehandlere med tilholdssted utenfor EU/EØS.

Avsluttende

17. Er det noe annet du vil tilføye?

Vedlegg 2. Intervjuguide markedsaktør

Intervjuguide markedsaktør – masteroppgave i samfunnssikkerhet

Bakgrunn og systemforståelse

18. Hva er din stilling, og hvilken kobling har dine arbeidsoppgaver/din bedrift til bruk av skytjenester i offentlig sektor?
19. Hva er din forståelse av datasuverenitet/digital suverenitet?
    a. Hva er sovereign cloud, og hvordan skiller det seg fra andre skytjenester?
20. Hvilket forhold opplever du at det offentlige har til datasuverenitet som konsept?
21. Hvilke aspekter ved datasuverenitet opplever du at kommunene har fokus på?
    a. Hvilke aspekter ved datasuverenitet har de ikke fokus på?
22. Hvordan kan eller bør norske kommuner utforme sin tilnærming til skytjenester, for å sikre datasuverenitet?
    a. Hvordan opplever du at tilnærmingen til skytjenester i det offentlige er nå, sammenliknet med svaret i forrige spørsmål?

Datatype og valg av skytjeneste

23. Hvordan anbefaler dere at kunder arbeider med klassifisering av data før disse skal settes i sky?
    a. Hvordan bør kommuner tilpasse bruken av skytjenester etter hvilken type data som skal behandles eller lagres? (eks persondata, sensitive data, virksomhetskritisk data)
24. Hvilke faktorer opplever du at det offentlige/kommuner anser som viktige i vurderingen av om en skytjeneste skal benyttes eller ei?
25. Kan du fortelle om du ser en preferanse eller tanker rundt type skytjeneste (offentlig/privat/hybrid) i det offentlige/kommuner?

Innsikt i skytjenestene

26. Hva bør en kunde ha innsikt i hos tjenesteleverandør ved bruk av en skytjeneste, for å sikre suverenitet?
    a. Hvordan gir dere egne kunder innsikt i hvor datasentrene deres skytjenester er tilknyttet, befinner seg geografisk?

27. Hvilke krav opplever du at offentlige kunder/kommuner setter til geografisk plassering av datasentre, innsikt i hvordan data lagres og tilgangsstyring?

Håndtering av skytjenester

28. Hva opplever du at det offentlige/kommuner er opptatt av når det kommer til å kontrollere og beskytte egne data?
29. Hvem opplever du som ledende aktør(er) innenfor utvikling/påvirkning av datasuverenitet?
30. Hvilke virkemidler og/eller ressurser kan kunder bruke for å sikre at de har kontroll over og rettigheter til egne data som behandles og lagres i skytjenester?
31. Hvordan kan en kunde sikre at vilkårene i avtaler og kontrakter for skytjenester blir fulgt av databehandler etter inngåelse?

Utfordringer og krav

32. Kan du fortelle om du opplever at det er fokus fra kommunenes side på å sikre back up løsninger der de anvender skytjenester?
33. Hvilke usikkerheter eller utfordringer opplever du at det offentlige/kommuner har i forbindelse med kontroll over, og rettigheter til, egne data lagret i skytjenester?
34. Hvilket inntrykk har du av hvordan det offentlige/kommuner forholder seg til lovgivning som kan sette krav til data som lagres og behandles i skytjenester?
    a. I hvilken grad har de intern kompetanse på dette feltet, og i hvilken grad er de avhengig av kompetanse hos leverandør?
35. Hvordan kan kommuner forholde seg til mulig usikkerhet i jurisdiksjon vedrørende rettigheter til innsyn i data?
36. Hvilke tanker har du om kommuner bør være bevisste eller ei, eller ha fokus på avhengigheter av enkeltaktører eller stor bruk av markedsdominerende leverandører?

Avsluttende

37. Er det noe annet du vil tilføye?

Vedlegg 3. Intervjuguide rådgivende organisasjon

Intervjuguide rådgivende organisasjon – masteroppgave i samfunnssikkerhet

Bakgrunn og forståelse av kommunen som system

1. Hva er din/deres stilling(er), og hvordan kommer dine/deres arbeidsoppgaver i berøring med bruk av skytjenester i norske kommuner?
2. Hvordan bistår dere det offentlige i forbindelse med bruk av skytjenester?
    a. Har dere vært involvert i hendelseshåndtering tilknyttet skytjenester i kommuner?
3. Hva er deres inntrykk av organiseringen av anskaffelser av, og bruk av, skytjenester i norske kommuner?
    a. I hvilken grad opplever dere at kommunene har interne ressurser og/eller kompetansepersoner på skytjenester?
    b. Hvilke andre aktører opplever dere at kommunene kan benytte seg av vedrørende spørsmål om skytjenester eller informasjonssikkerhet?

Datatype og valg av skytjeneste

4. Kan dere fortelle om dere ser at det benyttes vurderinger slik som følsomhetsvurderinger, dataklassifisering eller kategorier basert på konfidensialitet og kritikalitet for data før man tar i bruk skytjenester i kommunene?
5. Hvilke faktorer opplever dere at det offentlige anser som viktige i vurderingen av om en skytjeneste skal benyttes eller ei?
6. Kan dere fortelle om dere opplever fokus rundt type skytjeneste i det offentlige? (offentlig/privat/hybrid)

Innsikt i skytjenestene

7. Hvordan kan det offentlige sikre seg garanti for hvor datasentrene tilknyttet skytjenestene de benytter, geografisk befinner seg?
8. Hvilken innsikt opplever dere at kommunene har i hvordan databehandler lagrer, behandler og flytter deres data?
9. Hvordan kan kommunene få oversikt over, og styre hvem som har tilgang til data lagret i skytjenestene de benytter, både internt i egen virksomhet og hos databehandler?

Håndtering av skytjenester

10. Hva opplever dere at kommuner er opptatt av når det kommer til å kontrollere og beskytte egne data?

11. Hvilke virkemidler og/eller ressurser kan kommunene bruke for å sikre at de har kontroll over og rettigheter til egne data som behandles og lagres i skytjenester?
12. I hvilken grad kan kunder som kommuner, påvirke tilbudet og innhold i kontrakter og avtaler med en tjenesteleverandør av skytjenester?
13. Hvordan kan en kommune sikre at vilkårene i avtaler og kontrakter for skytjenester blir fulgt av databehandler etter inngåelse?

Utfordringer og krav

14. Kan dere fortelle om dere opplever at det er fokus på å sikre back up løsninger der kommunene bruker skytjenester?
15. Hvilke usikkerheter eller utfordringer, opplever dere at kommunene møter/har i forbindelse med kontroll over, og rettigheter til, egne data lagret i skytjenester?
16. Hvilket inntrykk har dere av hvordan det offentlige forholder seg til lovgivning som kan sette krav til data som lagres og behandles i skytjenester?
17. Hvordan opplever dere at kommuner forholder seg til mulig usikkerhet i jurisdiksjon vedrørende rettigheter til innsyn i data? Eksempelvis ved bruk av databehandler med tilholdssted utenfor EU/EØS, eller som benytter datasentre eller underleverandører utenfor EU/EØS.

Avsluttende

18. Er det noe annet dere vil tilføye?

Vedlegg 4. Informasjonsskriv NSD

Vil du delta i forskningsprosjektet

Datasuverenitet i kommunen ved bruk av skytjenester

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å undersøke datasuverenitet i kommunen ved bruk av skytjenester. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Du trenger ikke å ha kjennskap til begrepet datasuverenitet for å kunne svare på intervjuspørsmålene, da begrepet i seg selv ikke vil bli benyttet.

Formål

Prosjektet er en mastergrad i samfunnssikkerhet ved Universitetet i Stavanger. Målet med prosjektet er å undersøke hvordan det arbeides med skytjenester i kommunen, og hvordan dette påvirker karakteristikker for datasuverenitet.

Hvem er ansvarlig for forskningsprosjektet?

Universitetet i Stavanger
Det teknisk- naturvitenskapelige fakultet
Institutt for sikkerhet, økonomi og planlegging

Hvorfor får du spørsmål om å delta?

Du får spørsmål om å delta fordi du har en rolle som berører bruk av skytjenester i kommunen.

Hva innebærer det for deg å delta?

Hvis du velger å delta i prosjektet, innebærer det at du stiller opp på ett intervju på ca. 60 minutt. Intervjuet vil inneholde spørsmål om datalagring i system/tjenester/løsninger du arbeider med og prosesser rundt skytjenester i kommunen. Jeg tar lydopptak og notater fra intervjuet. Intervjuguiden sendes ut i forkant av intervjuet.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

Kun veileder Kenneth Arne Pettersen Gould (Førsteamanuensis UiS) og jeg vil ha tilgang til opplysningene.

Navnet og kontaktopplysningene dine vil jeg erstatte med en kode som lagres på egen navneliste adskilt fra øvrige data. Datamaterialet lagres i tråd med UiS sine retningslinjer for forskningsprosjekter.

I selve oppgaven vil kun stillingstittel/rolle og arbeidskommune benyttes.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er 15. juni 2022. Opptak og personopplysninger slettes ved prosjektets slutt.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene,
- å få rettet personopplysninger om deg,
- å få slettet personopplysninger om deg, og
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Institutt for sikkerheit, økonomi og planlegging har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?

Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- Institutt for sikkerheit, økonomi og planlegging ved
  Sofie Sagedahl Høydal (Masterstudent Samfunnssikkerhet UiS) tlf 94817430, e-mail ss.hoydal@stud.uis.no
  Kenneth Arne Pettersen Gould (Veileder, førsteamanuensis) tlf 51831658, e-mail kenneth.a.pettersen@uis.no
- UiS sitt personvernombud: personvernombud@uis.no

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:

- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen

Sofie Sagedahl Høydal
Masterstudent Samfunnssikkerhet

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet **Datasuverenitet i kommunen ved bruk av skytjenester**, og har fått anledning til å stille spørsmål. Ved å signere samtykker jeg til:

- å delta i intervju
- at opplysninger om meg, nærmere bestemt stillingstittel/rolle og arbeidskommune, publiseres slik at jeg kan gjenkjennes

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

(Signert av prosjektdeltaker, dato)

Vedlegg 5. Meldeskjema for behandling av personopplysninger

Meldeskjema / Masteroppgave i samfunnssikkerhet - datasuverenitet i kommunene / Vurdering

Vurdering

Referansenummer

238395

Prosjekttittel

Masteroppgave i samfunnssikkerhet - datasuverenitet i kommunene

Behandlingsansvarlig institusjon

Universitetet i Stavanger / Det teknisk- naturvitenskapelige fakultet / Institutt for sikkerheit, økonomi og planlegging

Prosjektperiode

01.01.2022 - 15.06.2022

Meldeskjema

Dato	Type
02.03.2022	Standard

Kommentar

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg, og eventuelt i meldingsdialogen mellom innmelder og Personverntjenester. Behandlingen kan starte.

DEL PROSJEKTET MED PROSJEKTANSVARLIG

For studenter er det obligatorisk å dele prosjektet med prosjektansvarlig (veileder). Del ved å trykke på knappen «Del prosjekt» i menylinjen øverst i meldeskjemaet. Prosjektansvarlig bes akseptere invitasjonen innen en uke. Om invitasjonen utløper, må han/hun inviteres på nytt.

TYPE OPPLYSNINGER OG VARIGHET

Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til den datoen som er oppgitt i meldeskjemaet.

LOVLIG GRUNNLAG

Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake.

Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER

-Personverntjenester vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om

-lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen -

formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke behandles til nye, uforenlige formål
-dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
-lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), og dataportabilitet (art. 20).

Personverntjenester vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
Personverntjenester legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

Ved bruk av databehandler (spørreskjemaleverandør, skylagring eller videosamtale) må behandlingen oppfylle kravene til bruk av databehandler, jf. art 28 og 29. Bruk leverandører som din institusjon har avtale med.

For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og/eller rådføre dere med behandlingsansvarlig institusjon.

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til oss ved å

oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde: https://www.nsd.no/personverntjenester/fylle-ut-meldeskjema-for-personopplysninger/melde-endringer-i-meldeskjema Du må vente på svar fra oss før endringen gjennomføres.

OPPFØLGING AV PROSJEKTET

Personverntjenester vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet! 2/2