

**Kandnr 706**

---

# **Skybaserte løysingar i eksterne og interne serverparkar**

**-Frå eit arkivfagleg perspektiv**

**Bacheloroppgåve 2016**  
**Bachelor i arkiv og dokumentbehandling**  
**Høgskulen i Oslo og Akershus, Institutt for arkiv-, bibliotek- og  
informasjonsfag**

## Samandrag:

Denne oppgåva tar føre seg bruken av nettsky i norske kommunar i dag. Interesse er stor rundt arkivlova (1999) sin §9 bokstav b, som stadfestar at:

Utan i samsvar med føresegner gjevne i medhald av § 12 i denne lova eller etter særskilt samtykke frå Riksarkivaren, kan ikkje arkivmateriale (...) førast ut or landet, dersom dette ikkje representerer ein naudsynt del av den forvaltningsmessige eller rettslege bruken av dokumenta.

Dette vil seie at med mindre materialet er til skanning eller til signering skal det ikkje være i utlandet. Oppgåva mi utdjupar dette. I tillegg tek den føre seg risikoar ved bruk av serverrom, både interne som ei kommune opprettar sjølve og eksterne som dei betalar ein leverandør for. Eg har hatt ei undersøking der eg har spurt utvalde kommanuar kva løysing dei har vald og kva tilgangar dei har gjeve i sitt arkivsystem.

Oppgåva tar føre seg Datatilsynet sin rapport (2012) som gjev tillating til å nytte skybaserte løysingar frå ein ekstern leverandør der serverane står i utlandet. Deretter tar oppgåva føre seg «Safe Harbour» som vart erkjent ugyldig av EU-domstolen, og kva løysingar som blir sett på i staden for «Safe Harbour» (Datatilsynet 06. Oktober 2015).

Til slutt vil eg ta føre meg risikoane ved bruk at serverrom, basert på «Forskrift om offentlege arkiv» kapittel IV (1999). Forskrifta er tiltenkt for arkivrom for fysisk arkiv, men kan og nyttast til serverrom. Heilt til slutt vil eg utdjupe løysingane som arkivskaper valde og min konklusjon.

Eksamen forside  
Fakultet for samfunnsfag  
Institutt ABI og JM

Kandidatnummer\*: 706

Emnekode/-namn\*: ARK3900/Bachelor-oppgåve

Utdanning: Arkiv og Dokumentbehandling

Dato innlevert: 13. Mai 2016

tal sider, inkl. forsida: 34 sider

Vedrørende fusk eller forsøk på fusk

X\* Eg har gjort meg kjent med forskrift om studie og eksamen ved HiOA:

<http://www.lovdata.no/cgi-wift/lldes?ltdoc=/for/ff-20120626-0718.html#7-5> §7-

5 *Fusk* og er klar over at dette blir sett alvorleg på og kan medføre strenge sanksjoner

X\* Denne oppgåva:

- er utført av personen som fyller ut dette skjemaet, eller av gruppas medlemmer dersom det er et gruppearbeid
- har ikkje vært brukt til ein annan eksamen/innlevering ved dette eller andre lærested innanlands eller utanlands
- brukar ikkje tidligare eller andre sitt arbeid utan å ha oppgitt kjelde
- har oppgitt alle kjelder og referanse i litteraturlista

\* sett en X her

## Innhold

|                                                       |    |
|-------------------------------------------------------|----|
| Samandrag: .....                                      | 2  |
| Eksamen forside .....                                 | 3  |
| Innleiing .....                                       | 5  |
| Bakgrunn .....                                        | 6  |
| Motivasjon .....                                      | 6  |
| Kva er skylagring? .....                              | 8  |
| Uttrykk nytta i denne oppgåva .....                   | 9  |
| Mine forventningar .....                              | 10 |
| Bruk av metode .....                                  | 11 |
| Status i dag .....                                    | 12 |
| Microsofts Cloud OS og Office 365 .....               | 12 |
| Jottacloud .....                                      | 14 |
| Google Apps og Datatilsynet sin rapport .....         | 15 |
| Riksarkivets eArkiv .....                             | 17 |
| Undersøkinga .....                                    | 18 |
| Risikoar .....                                        | 20 |
| Øydelagde serverar .....                              | 21 |
| Innbrot i serverrom .....                             | 22 |
| Hackar-angrep .....                                   | 22 |
| Migrering .....                                       | 23 |
| Sletting og kassasjon .....                           | 24 |
| Utgåtte kontraktar .....                              | 24 |
| Overgang til ein annan leverandør .....               | 24 |
| Sikkerheitskopiar .....                               | 25 |
| Innsyn .....                                          | 25 |
| Kva har løysingar har arkivskaparar vald sjølv? ..... | 26 |
| Eksterne serverparkar .....                           | 26 |
| Lokale serverparkar .....                             | 26 |
| Konklusjon og oppsummering .....                      | 27 |
| Litteraturliste .....                                 | 31 |

## Innleiing

I desse dagar er det mykje snakk om nettsky. I hovudsak er det private som nyttar seg av desse muligheitene til å lagre bilete og dokument på andre sine serverar. Nettsky er ein effektiv måte å spare plass på sine eigne harddiskar og datamaskiner. Som privatperson kan ein gjøre med eigne private dokumenter og bilete som ein vil. Dersom du startar ei verksemd som ikkje er knytt til det offentlege står du også fritt til å gjere som du vil med dine dokument og bilete, unntaket er om dokumenta og bileta gjeld nokon andre eller dersom du tek oppdrag for det offentlege. Som offentlig verksemd og myndigheit gjeld andre reglar. I denne oppgåva skal eg for det meste ha fokus på bruk av skybaserte løysingar som ein del av det offentlege, mine tankar rundt dette og intervju med aktuelle kommunar som nyttar seg av skybaserte løysingar på forskjellige måtar. I tillegg vil eg studere kva Riksarkivet og utøvande myndigheit, Arkivverket, har uttalt vedrørende skybaserte løysingar frå utanlandske leverandørar. Samt kva som kan være framtida innan eksterne serverparkar.

Problemstillingar som eg vil finne svar på i denne oppgåva er for det første kva innverknad skylagring har på kommunale arkiv, og for det andre korleis kommunar kan sikre trygg bevaring av arkivmateriale som er lagra i interne og eksterne serverparkar.

I byrjinga av denne oppgåva skal eg først utdjupe mi interesse for å velje skyløysingar som tema for mi bacheloroppgåve. Deretter vil eg gå nærare inn på kva skyløysingar egentlig betyr og kva det er, før eg går vidare på uttrykk nytta i denne oppgåva, og kva forventningar eg har. Etter det vil eg gå igjennom min bruk av metode og status i arkiv-Noreg i dag. Der vil eg fortelje litt om dei forskjellige muligheitene som finst i dag, før eg går nærare inn på undersøkinga som eg har laga. Etter undersøkinga vil eg fortelje litt om risikoane ved bruk av serverrom, både for dei som nyttar skybaserte løysingar frå eksterne leverandørar, og dei som nyttar lokale løysingar. Deretter vil eg gå igjennom resultata mine frå undersøkinga å sjå kva løysingar arkivskaparar har vald som si løysing. Til slutt kjem konklusjon og oppsummering, med litteraturliste aller sist.

## Bakgrunn

Bakgrunnen for denne oppgåva er mi interesse for skybasert datalagring for langtidsbevaring. Med langtidsbevaring meiner ein det som skal lagrast i all overskodedeleg framtid. Interessa har vore særstør rundt arkivlova §9 bokstav b, som i utgangspunktet ikkje gjev tillateleg til skybasert datalagring. Dette er fordi dei fleste som tilbyr skybasert datalagring i dag held serverane som materialet ligg på utanfor Noregs grenser, noko som eg vil utdjupe meir i løpet av oppgåva.

Denne oppgåva er ute etter status i arkiv-Noreg i dag. Kva forhold har kommunar til skybasert datalagring? Interessa stør rundt kva løysingar som er til utredning, under utvikling eller allereie finst hjå kommunane. Eg som framtidig arkivar er spesielt interessert i kva risiko skylagring medfører, om risikoane er gjennomtenkte hjå arkivskaparar som nyttar seg av slike løysingar.

Aktuelle kommunar er Moss, Narvik og Alta, som har tinga avtale med forskjellige utanlandske leverandørar og tatt steget opp i skyene. Eg vil undersøke kva dei risikera ved å la utanforståande ta hand som deira arkivmateriale, og om dei har tenkt igjennom kva som står på spel og konsekvensane av deira handlingar. I tillegg vil eg forhøyre meg med andre kommunar som ikkje nyttar skybaserte løysingar hjå eksterne leverandørar, men har satt opp sitt eige datasenter eller har funne andre løysingar.

## Motivasjon

I større samanheng var det §9 bokstav b i arkivlova som satt mi interesse i sving. Arkivlova (1999) seier at

Utan i samsvar med føresegner gjevne i medhald av § 12 i denne lova eller etter særskilt samtykke frå Riksarkivaren, kan ikkje arkivmateriale (...) førast ut or landet, dersom dette ikkje representerer ein naudsynt del av den forvaltningsmessige eller rettslege bruken av dokumenta.

Då arkivlova vart skriven i 1992 (Publisert 1999) var det ingenting som heitte nettsky eller skybaserte løysingar. Då var alt på eigne harddiskar, diskettar eller CD-plater. Internett var ikkje like utbreitt som i dag og mykje dyrare og ikkje like raskt å bruke. Slik var det ikkje eit alternativ å laste opp dokumenta på ein ekstern server i eit anna land. Difor tek arkivlova ikkje høgde for skybasert datalagring. På den måten kan ein seie at lova har gått ut på dato, og ein no er tvungen til å sjå på lova på ein annan måte.

I dei seinare åra har bruk av skytjenester eksplodert både hjå private og offentlege bedrifter. Det er først no i 2016 at regjeringa ser det naudsynt å tilpasse lovverket dagens verkelegheit. Kommunal- og moderniseringsdepartementet (2016 s. 24) seier at

Regjeringa vil (...) Revidere arkivforskrifta og eventuelt delar av arkivlova for blant anna å tilpasse arkivregelverket betre til digitalisering. Som ein del av dette vil ein vurdere behov for endring slik at offentlege organ kan ta i bruk skytjenester med serverar utanfor Noreg for arkiv.

Arkivlova stadfestar at ein KAN føre arkivmateriale ut or landet dersom det er for signering eller godkjenning. «Dispensasjon har imidlertid blitt innvilget ved flere anledninger, hovedsakelig ved midlertidlig utførsel av papirarkiv for skanning i utlandet.» (Johannessen & Gaarder, 2015). Denne dispensasjonen stadfestar at arkivmateriale kan førast ut or landet dersom det er mellombels, altså at man har ein plan for å tilbakeføre det til Noreg for langtidsbevaring. Denne planen kan settas i verk enten ved at materialet har blitt signert som avtalt eller at skanninga er gjennomført og materialet vert ført attende til Noreg.

Dette vil då seie at frå eit arkivfagleg fokus bryt dei kommunane som har valt å flytte sitt arkiv ut i skya ved hjelp av utanlandske leverandørar arkivlova § 9 bokstav b. Dette er fordi dei utanlandske leverandørane vil følge dei lovene i det landet der serverane står, eller det landet der firmaet er registret. Dersom dei hadde hatt serverane i Noreg hadde det vært naturleg å følge norsk lov og norske reglar.

## Kva er skylagring?

Nettskya, Cloud'en, Skya, Skylagring er alle forskjellige namn på lagring av materiale på eksterne serverar. Skylagring går ut på at du lagrar materiale på eksterne serverar som du har tilgang til via internett. Felles for desse er at dei er eigd av nokon andre enn arkivskapar, altså vil det være mange som ein ikkje kjenner til som har tilgang til serverane, og dermed også datane som ligg på serverane.

Det er jo gode grunnar for det. Nokon må jo vedlikehalde brannmurane, slette det som skal kasserast og vidare. Spørsmålet er kor mykje kan arkivskapar stole på denne leverandøren som man har inngått ei avtale med. Kan ein stole på at dei ikkje gjev ut data til ein tredjepart, eller lar personar og andre firma få autorisasjon og tilgang til arkivskapar sine data? Det er klart at om serverane står i Noreg ligg dei under norsk lov. Dermed kjem brot på avtala opp for norsk rett. Det er som nemnd tidlegare ikkje tilfellet om serverane står i eit anna land.

Kvifor er det blitt so moderne med nettbasert skylagring no? Er det verkeleg naudsynt å bruke skybasert lagring, eller er det berre moderne å ha materialet i nettskya? Grunnen for at ein vil nytte seg av skybasert datalagring må jo være for å spare pengar, men har kommunane verkeleg spart so mykje på å gå over til nettskya? Dette skal eg komme tilbake til seinare i oppgåva.

Det positive med skylagring er at ein slepp å ha kontroll på eigne serverar og kan fordele dette ansvaret til andre. Det er klart at ei kommune med dårleg økonomi ikkje har muligheit til å utvikle eit velfungarande serverrom og ha tilsette som kan ta vare på og reparere ved behov.

Problema oppstår når serverane og leverandøren er begge i og frå utlandet. Då er arkivmaterialet per definisjon ute or landet, og då bryt det med arkivlova sin § 9 bokstav b.

## Uttrykk nytta i denne oppgåva

Eksterne serverparkar blir i denne oppgåva nytta som eit meir skildrande namn på «Cloud», «skya» og det vi vanlegvis kallar nettopp eksterne serverparkar. «Begrepet *cloud* eller *sky* stammer fra den måten leverandørene tegner bildet av hvordan det hele fungerer, på.» (Dørum 2014, s. 124). Før var alt fysisk plassert hjå arkivskapar eller i eit fjernarkiv. I dag nyttar dei fleste elektronisk arkivering, og då mykje på internett.

Interne eller lokale serverparkar er serverparkar som det offentlege har oppretta sjølve med tanke på si eiga arkivering og nytting. Desse serverparkane er det kommunane sjølve som driftar og held ved like, og har då begrensa tilgang for uvelkomne.

Skybaserte løysingar nyttar eg i denne oppgåva som både eksterne og interne serverparkar.

Sjekksummar er ein generert algoritme som undersøkar den matematiske funksjonen til data som ligg i dokumentet eller fila. Noark (Riksarkivet 2013, s. 271) beskriv det som «Verdi (hash value) som fremkommer ved å behandle en datastrøm i henhold til en gitt algoritme» Ein sjekksum kan genererast både til (vanlegvis i arkivverda) dokument, bilete og mappe. Det som då skjer er at man lastar opp fila til eit program på internett (om man ikkje har eit på datamaskina allereie) som generera ein sjekksum for deg. Der kan du som regel velje fleire sjekksummar, men den som er nytta i Noark er SHA256 inntil vidare (Metadatakatalog, 2013, s. 61).

Både dokumenter og filer med metadata må påføres en sjekksum som gir garanti for at integriteten og autentisiteten opprettholdes, dvs. at dokumentene er det de utgir seg for å være, og at innholdet i dokumenter og metadata ikke blir endret etter at de er overført til arkivdepotet.

(Arkivverket 2013 s. 94). Dette blir spesielt nytta ved avlevering av digitalt materiale. Då ber Riksarkivet om å få heile avleveringa levert med ein sjekksum. Om denne ikkje stemmer overeins med sjekksummen dei har fått oppgitt av arkivskaper vil avleveringa

bli avvist med ein gong (Riksarkivaren 2012, s.19) Dette viser kor mykje ein stolar på sjekksummar og kor vanskelig det er å gjøre uautoriserte endringar utan at det blir oppdaga.

«Å gå ut i skya» er eit uttrykk som blir nytta innimellom, og med dette meina dei som har valt å nytte seg av eksterne skyløysingar, altså utanfor Noregs grenser. Dei har «tatt steget» ut i skya.

## Mine forventningar

Kva forventa eg å finne ved denne undersøkinga og skrivning av denne oppgåva? Det eg først og fremst er ute etter er om kommunane som eg spør i denne undersøkinga er medviten på kva risikoar det er med å nytte utanlandske leverandørar som ikkje held serverane sine i Noreg og under norsk lov.

Oppgåva mi er ei påminning om risikoane materialet blir satt ut for, og konsekvensane det kan ha for administrasjonen i kommunane og innbyggjarane. Er kommunane klar over at opplysningar kan komme i feil hender? Har dei tenkt på at jo lengre unna noko står, jo mindre kontroll har dei på det? Det er jo kommunane sitt ansvar at dei har opplysningar som innbyggjarane etterspør. Det kan komme endringar i filformatet, og korleis har kommunane sikra seg at dersom dei nyttar ei skybasert løysing at filformata blir endra på ein måte som lar seg etterprøve og samstundes bevarer integritet og autensitet? Dersom kommunane ikkje kan svare på førespurnadar frå brukarane som dei utan tvil skulle kunne svare på, for eksempel kva oppfølging ein person har fått, kan det bli rettsak. Dersom det er snakk om manglande oppfølging frå kommunane si side kan dei få store erstatningsansvar.

Om eg var arkivleiar ville eg stille spørsmål ved å nytte nettskyt hjå utanlandske leverandørar om serverane ikkje står i Noreg. Både fordi at dei då bryt arkivlova §9 bokstav b og det som har kommt fram dei siste åra ved at dei amerikanske myndighetane ved National Security Agency – NSA i spissen overvakar mange brukarar på nett utan at brukarane og leverandørane er klar over det. Dette vart avslørt 7. Juni 2013 av at Washington Post skreiv ein artikkel om ein mann med namn Edward Snowden.

Han avslørte blant annet at det i USA fantes et hemmelig overvåkingsprogram rettet mot utenlandske borgere, at NSA hadde hatt sine fingre langt inn i serverne til Microsoft og Google, og at selveste Angela Merkels telefon var blitt avlyttet. (Datatilsynet 2014).

Har arkivtenesta i dei små kommunane som eg intervjuar har tenkt seriøst på skybaserte løysingar? Eller er deira fokus på den kommande kommunereforma? Prioritera dei heller kommunereforma og vel å heller bli einige om eit felles arkivsystem seg i mellom når dei større kommunane er på plass? I tillegg undrar eg kva som får ei kommune som arkivskapar til å gå igjennom ein so omfattande prosess som å flytte sine løysingar ut i skya.

## Bruk av metode

Då eg byrja å skrive på oppgåva mi tenkte eg at eg skulle sende ut spørjeundersøking på e-post til mine utvalte kommunar. Etter å ha diskutert fram og tilbake med vegleiar, der vi blant anna har vært innom telefonintervju, har vi bestemt at eg skal gjøre eit intervju via e-post, altså at eg spør fleire og fleire spørsmål på e-post til arkivleiar. Det viste seg at arkivleiarar ikkje var so ivrige på å drive ein lang korrespondanse om deira skyløysingar, og dei kommunane eg spurde ville heller ha eit spørjeskjema å svare på. Dette kan være fordi dei følar det er tryggare, og at eg ikkje kjem med utdjupande tilleggsspørsmål som dei ikkje vil eller kan svare på. I tillegg kan dei då lese igjennom alle spørsmåla og svare på dei i den rekkefølja dei sjølve vil. Resultatet vart at alle kommunane har fått tilsendt spørjeskjema. Dette fører til at eg nyttar meg av kvalitativ metode.

Kommunane eg har valt å intervju ligg alle i forskjellige fylker og i forskjellige delar av landet. Dei er anonyme. Eg spør ei større kommune på Austlandet, ei lita kommune på Vestlandet og ei kommune i Nord-Noreg. Dette er for å få ulike svar og sjå om det er noko forskjell på om dei store kommunane har tenkt på skyløysingar eller om det er ulikt, samt om dei små kommunane har tenkt i so store banar eller om dei er mest opptatt av kommunereforma som er på veg.

## Status i dag

I dette kapittelet vil eg gå igjennom det som er status i arkiv-Noreg i dag. Eg vil sjå nærare på kva løysingar som er nytta, samt uttaler frå Datatilsynet og Riksarkivet. Eg vil sjå korleis skybaserte løysingar frå eksterne leverandørar blir nytta hjå nokre av dei kommunane som har valt denne løysinga. I dag er det tre kommunar som nyttar seg av skyløysingar frå utanlandske leverandørar. Desse er Alta kommune (Christensen, 2013), Narvik kommune (Kirkenes, 2012) og Moss kommune (Christensen, 2014). Narvik kommune nyttar Google Apps, medan Alta og Moss nyttar Office 365 som tilhøyrar Microsoft. Eg vil sjå nærare på andre alternativ i Noreg, i dette tilfellet Jottacloud og Riksarkivets eArkiv. Sjølv om Riksarkivets eArkiv fortsatt er under utprøving, tykkar eg det er eit interessant pust inn i debatten. Det har vore veldig stor ueinigheit om kva som er lov å nytte seg av, men Riksarkivet og Arkivverket er den utøvande myndigheita, og gjev ei endeleg løysing som gjer at arkivskapar ikkje bryt lover, er sikra autensiet, intergritet og kontroll på dokumenta og kven som kan sjå dei.

## Microsofts Cloud OS og Office 365

Microsoft har fått ein fot innanfor det norske marknaden ved bruk av Office 365 og Cloud OS. Høgskulane som nyttar Fronter og ItsLearning må no nytte Office 365. Fronter vart kjøpt opp av ItsLearning i 2015 (Lygre, 2015), og dette har ført til at Fronter har fått ekstern bruk av e-post, der det blir nytta Office 365. Då Moss kommune gjekk ut i skya var det med et ønske om lågare investerings- og driftskostnader. (Christensen, 2014). Problemet er at alt ikkje kan lagrast ute i skya.

Valget har falt på en hybridløsning med Microsoft Cloud OS og Storsimple. Med hybrid menes det her at sensitive data lagres lokalt som før, mens all annen data lagres ute i den store nettskyen (Christensen, 2014).

Dette vil då seie at sjølv om dei nyttar seg av skybaserte løysingar frå eksterne leverandørar vil dei likevel ha mykje data lokalt. Artikkelen seier ikkje kvifor Moss Kommune har valt å ikkje flytte alt ut i skya, men truleg vel kommuna dette fordi dei ikkje ser på skya som trygt nok. Det undrar meg då at dei meina skya er trygg nok for

40% av deira materiale, når dei likevel ikkje stolar heilt på leverandøren (Jørgenrud, 2015). Klart det er bra å være føre var, men når dei ikkje føler seg trygge nok til å flytte alt ut i skya, er eg ikkje sikker på om dei er trygge nok på til å flytte noko ut i skya.

Moss kommune byrja med å bruke Microsoft si Office 365 for e-post for dei fleste av sine tilsette, og har etter det tatt steget vidare med lagring, back-up og drift ut i den skybaserte løysinga til Microsoft. På Moss kommune si heimeside har dei ei e-postadresse for postmottak. Denne er merka med «Postmottak for dokumenter, brev og offisielle henvendelser» (Moss kommune, udatert). Man må ha eit vakent blikk for å lese i mellom linjene at ein brukar ikkje skal sende sensitive personopplysningar til denne e-postadressa. Det er vanleg å opplyse om dette i same teksten slik at den ikkje kan mistolkast, men det har ikkje Moss kommune gjort i dette tilfellet.

Moss kommune snakkar varmt om si skybaserte løysing som dei skaffa seg i 2014. Om ein ser på kommunal rapport frå 2013 må dei ha gjort noko dramatisk i løpet av det året. Her er et utklipp frå kommunal rapport (Venli, 2013):

### Undersøkelse om bevaring av elektronisk arkiv

Vis  linjer

Søk:

| Kommune      | Knr | - Skriftlig plan eller vedtak om bevaring av elektroniskarkiv? | Har arkivplanen oversikt over hvilke elektroniske arkiver som brukes? | Satt av en årlig sum til bevaringen av elektronisk arkiv? | Kompetanse til å bevare kommunens elektroniske arkiv? (Ja/nei) | Tilgang på elektronisk depot? (Ja/nei) | Besvart undersøkelsen? |
|--------------|-----|----------------------------------------------------------------|-----------------------------------------------------------------------|-----------------------------------------------------------|----------------------------------------------------------------|----------------------------------------|------------------------|
| Moss kommune | 104 | Nei                                                            | Nei                                                                   | Nei                                                       | Nei                                                            | Nei                                    | Ja                     |

Viser 1 til 1 av 1 linjer (filtrert fra 430 totalt antall linjer)

Som det kjem fram her har ikkje Moss kommune i 2013 planar for deira elektroniske arkiv på nokon måte. Diverre fann eg ikkje ei nyare undersøking med same spørsmåla.

Det hadde vore interessant å sjå om dette har endra seg etter at kommuna starta å nytte skybaserte løysingar frå Microsoft.

Hovudgrunnen for at Moss kommune har valt å gå ut i skya er for å spare pengar. Kommunen har lenge slitt med dårleg økonomi, og seier at dei sparar cirka 12 millionar kroner i kommande femårsperiode på hybrid-løysninga, kontra å nytte berre eigne lokale serverar (Jørgenrud, 2015). Det er klart at når det er snakk om so store summar er det fornuftig å vurdere det, men kunne kommuna finne eit alternativ i Noreg der dei også kunne spart pengar, men samtidig flytta alt ut i skya, i staden for berre 40%? (Jørgenrud, 2015).

### Jottacloud

Jottacloud er den største Norske leverandøren av skytenester. På heimesida si skrive dei at:

Jottacloud er en norsk skylagringstjeneste for privatpersoner og bedrifter som lar deg sikkerhetskopiere, synkronisere, lagre og dele filer fra alle dine enheter. Dataene som lastes opp lagres i henhold til norske personvernlover, som er blant verdens strengeste.

I utgangspunktet er Jottacloud eit bra alternativ i forhold til dei utanlandske leverandørane. Ved å bruke Jottacloud vil ikkje kommunane bryte den norske arkivlova, og vi veit at dei norske lovene er strenge når det gjeld personsikkerheit og deling av materiale. Personopplysningslova (2001) §29 seier at «Personopplysninger kan bare overføres til stater som sikrer en forsvarlig behandling av opplysningene.» I tillegg seier Personopplysningslova §33 at «Det kreves konsesjon fra Datatilsynet for å behandle sensitive personopplysninger.» Dermed må kommunane som nyttar skybaserte løysingar i utlandet ha konsesjon frå Datatilsynet før dei overfører opplysningar til utlandet. Dette skal eg sjå meir på i neste delkapittel.

Det Jottacloud og dei andre leverandørane eg tidlegare tek føre meg i oppgåva ikkje kan garantere, er oppdatering og vedlikehald av filene. Dersom filene skal migrerast til

eit nytt filformat, so må kommunane gjere det sjølv for å sikre autensitet og integritet. Dersom materialet hadde blitt avlevert på vanleg måte til Riksarkivet hadde dei tatt ansvar for å migrere og behalde dei gamle filene for framtidas dokumentasjon, og ordna sjekksummane slik at dei kunne bevise at endringane dei har gjort er i tråd med gjeldande forskrifter og at endringane er dokumenterte (Riksarkivaren 2012, s. 18-19, 4.2).

### Google Apps og Datatilsynet sin rapport

Datatilsynet kom 21. september 2012 med eit svar der dei avslutta saken mot Narvik kommunes bruk av Google Apps (Datatilsynets rapport 2012, s. 1). Denne har i pressen berre blitt kalla «Datatilsynet sin rapport» og vil vidare i denne oppgåva bli omtalt som det. «Saken dreier seg om kommunens eksisterende, og planlagt utvidede, bruk av produktet "Google Apps".» (Datatilsynet sin rapport 2012, s. 1.)

Datatilsynet sin rapport er prega av misnøye mot at Narvik nyttar seg av skyløysingar med serverar utanfor Noreg sine grenser. Likevel tyder innhaldet på at dei har eit ønske om å avslutte saka.

Fotnotane i denne rapporten er interessant. I rapporten på side 7, fotnote 10 står det at «Under forutsetning av at vilkårene i personopplysningsloven § 4 er oppfylt.». Personopplysningslova §4 omhandlar det geografiske virkeområdet til lova, som gjeld i Noreg. I tillegg står der i Personopplysningslova at den gjeld for «behandlingsansvarlige som er etablert i stater utenfor EØS-området dersom den behandlingsansvarlige benytter hjelpemidler i Norge.» (Personopplysningslova 2001). Altså vil Datatilsynet at Personopplysningslova skal gjelde for Narvik kommunes bruk av Google Apps. I rapporten (Datatilsynet sin rapport s. 7) står det at «Leverandøren vil i tillegg bli å regne som behandlingsansvarlig.» Der spesifiserar Datatilsynet at Google er å rekne som behandlingsansvarlig, og etter Personopplysningslova som tidligare nemnt betyr det at Google skal nytte seg av hjelpemiddel i Noreg. Datatilsynet pålegg Narvik kommune at Google Apps må nytte hjelpemiddel i Noreg. Det kjem

derimot ikkje fram av Datatilsynet sin rapport om Google Apps, altså den «behandlingsansvarlige» som lova omtalar, faktisk nyttar hjelpemiddel i Noreg.

Det kjem ikkje fram av rapporten kva hjelpemiddel det er snakk om at Google skal nytte seg av. Sidan dette er ei vurdering frå Datatilsynets si side er det ikkje eit pålegg mot Google, men eit krav til Narvik kommune om å ha sett igjennom dei rettslige bindingane mellom dei og Google.

Datatilsynet skriv i sin rapport at «(...) data skal lagres og behandles i Googles datasentre innenfor EU/EØS og innenfor USA.» (Datatilsynet sin rapport s. 9, punkt 4, tredje avsnitt). No påpeikast det likevel i rapporten «at Google er sertifisert under Safe Harbor-regimet» (Datatilsynets rapport s. 9, punkt 4, tredje avsnitt), men det er ikkje spesifisert i Personopplysningslova at dersom nokon er sertifisert under Safe Harbor-regimet kan opplysningar lagrast utanfor EØS. Datatilsynet vurderer dette som sikkert nok likevel. Dette var i 2012. I Oktober 2015 kom det fram at «Safe Harbor» er kjent ugyldig av EU-domstolen. (Datatilsynet 06. Oktober 2015) Dette fører til at bedriftene som i dag overføra personopplysningar frå europeiske land til USA, frå og med den dagen må finne andre måtar å overføre opplysningane på for å unngå å bryte med felleseuropeiske personvernregelverket.

Regjeringa tolkar lova slik at «Personopplysningslova er i utgangspunktet ikkje til hinder for bruk av skytenester, så lenge data blir lagra og behandla innanfor EØS-området, eller i tråd med ordningar som er godkjende av EU.» (Regjeringen 2016, siste avsnitt). På nettsidene til Datatilsynet (16. Oktober 2015) finn eg dette:

I EU/EØS-land er personopplysninger beskyttet gjennom reglene i personverndirektivet (implementert i norsk lov gjennom personopplysningsloven). USA har ikke tilsvarende regler for vern av personopplysninger. Direktivet forbyr derfor som utgangspunkt overføring av personopplysninger til USA, med mindre den registrerte samtykker til overføringen, eller en del andre vilkår er oppfylt (se personopplysningslovens § 30, a til h.).

Her kjem det tydeleg fram at Datatilsynet forbyr overføringar av personopplysningar til USA. Unntaket gjeld om den som personopplysningane omtalar samtykkjer til overføringa. No er EU i gang med ei ny avtale med USA som dei kallar «EU-U.S. Privacy Shield» Dersom den blir vedtatt, fastslår kommisjonen at sikringstiltak som blir gitt når data overførast under den nye EU-U.S. Privacy Shield tilsvare datavernstandarden i EU. (European Comission 2016). Kommunal- og moderniseringsdepartementet (2016 s. 22) seier at

Det skal vere klare reglar for, og god kontroll med, når amerikanske styresmakter kan få tilgang til data som er overførte til USA innanfor det nye rammeverket. Dette var eitt av dei områda EU-domstolen meinte ikkje var varetatt under Safe Harbour.

Riksarkivet var seine i denne saka. Først i 2014 seier Riksarkivet tydeleg nei ved teksten «Etter vårt syn stiller arkivlova krav om at arkivdatabasen skal vere lagra og tilgjengeleg på server som er fysisk plassert i Noreg.» (Riksarkivet 2014). Datatilsynet har ikkje myndigheit til å vise til arkivlova sin §9 bokstav b fordi det er Riksarkivets myndigheitsområde. Oppsplittinga av offentlige myndigheitar er noko av det grunnleggande problemet når lovene gjev rom for ulike tolkingar. Dette er noko av problema som ligg bak skybaserte løysingar i eksterne serverparkar.

### Riksarkivets eArkiv

Riksarkivet har i kjølvatnet av at Moss og Narviks valde nytting av eksterne skybaserte løysingar hjå forskjellige leverandørar oppretta ei form for skybasert løysing hjå seg sjølve. Denne har dei valt å kalle eArkiv (Urtegaard, 2015)

eArkiv etablerer en moderne infrastruktur for arkivering og dokumentasjon, og åpner for automatisert overføring av arkivmateriale fra dagligarkiv hos arkiveier til en arkivkjerne (eArkiv) basert på Noark-standarden.

Dette eArkivet er under utprøving i 2016 hjå utvalte arkivskaparar. Denne skybaserte løysinga sikrar overføringar til Riksarkivet, men det er ikkje det same som ei avlevering. Riksarkivets eArkiv er bare ein «mellomstasjon» for arkivmaterialet medan det fortsatt er hjå arkivskapar. Meininga bak eArkiv er at det skal skje ei automatisert overføring til arkivkjerna basert på Noark-standaren frå arkivskapar. (Riksarkivet 2015) På denne måten vil Riksarkivet kunne halde ein betre kontroll på materialet dei skal få inn, og påpeike feil undervegs so dei kan bli retta opp raskt. Dette vil føre til at når den endelige avleveringa skal gjennomførast vil den gå mykje raskare en det som har vært vanleg til no.

Riksarkivet viser med dette at dei er bevisst på sitt ansvar. Arkivverket og Riksarkivet vil slik sikre at digitale avleveringar går raskare, både for seg sjølve og for arkivskapar. Det er klart at når prosessen kan overvakast undervegs og skapar kan få tilbakemelding medan dei fortsatt har saka friskt i minnet vil det være lettare for dei å rette opp i feilen utan at det tek for lang tid eller kostar for mykje. Dette vil også på sikt føre til at avleveringane går lettare, det vil ta kortare tid å få dei godkjent og det vil koste mindre enn det gjør i dag. I tillegg vil oppgåvene til Riksarkivet blir mindre ved avleveringar frå eArkiv, so dei kan bruke ressursar på andre prosjekt og gje betre hjelp til fleire arkivskaparar på kortare tid. Dette førar til ei meir effektiv forvaltning og ein meir framifrå arkivmyndigheit.

## Undersøkinga

Undersøkinga mi vart sendt ut til nokre kommunar rundt i landet. Eg sendte til ei stor kommune på austlandet, ei lita på vestlandet og ei mellomstor nord i Noreg. Dei er anonyme i denne teksten. Spørsmåla i undersøkinga mi gjekk på generell arkivdrift, men mest fokus var på kva skybaserte løysingar dei har vald og korleis dei er utført. Dersom dei har eigne skybaserte løysingar var spørsmåla meir retta mot sikkerheten i serverrommet og muligheita for uvelkomne å komme inn i romma, både gjennom hacking og fysisk innbrot. Dersom kommunar nytta seg av skybaserte løysingar frå ein anna leverandør var spørsmåla meir retta mot kontraktane og kva som skjer ved for eksempel endring av leverandør eller ved sletting og kassasjon.

Den første delen av undersøkinga gjekk til begge partar, både dei som nyttar skybaserte løysingar frå eksterne leverandørar og dei som hadde skybaserte løysingar sjølve. Her var spørsmåla meir retta mot tilsettingsprosessen, tilgangar til å endre brukarar og innsyn. Første spørsmålet handla om kven som kunne endre tilgangar inne i systemet. Det var samsvar mellom kommunane her, alle let arkivleiar og it-avdelinga endre tilgangar inne i systemet, og nokre kommunar hadde også eigne superbrukarar i tillegg.

Deretter fekk kommunane spørsmål om dei hadde bakgrunnssjekka personar før dei vart tilsette. Ingen hadde bedt om sikkerheitsklarering, men sjekka referansar. I kommune-Noreg er det ikkje lovpålagt med sikkerheitsklarering, men det skadar ikkje når man jobbar med taushetslagt informasjon. Det er klart at førre arbeidsgivar kan fortelje mykje om korleis ein person jobbar og kva fokus den personen har i løpet av ein arbeidsdag.

Først vil eg gå igjennom spørsmåla som vart stilt til kommunane som ikkje nyttar seg av eksterne skybaserte løysingar eller har laga sine eigne løysingar. Tilgangen til serverane er sterkt kontrollert hjå kommunane som eg har intervjuet. Berre tilsette med behov har tilgang til serverromma og har då tilgang med nøkkelkort. Leverandørar har berre tilgang ved avtale, og då berre saman med ein eller fleire tilsette i kommunen. All opninga av dører med nøkkelkort blir logga, der det blir registrert kven som var der sist.

Det viser seg at dei kommunane som er med i undersøkinga har tenkt godt når det gjeld sikkerheitskopiar og plassering av serverrom. Sikkerheitskopien er ikkje plassert i same bygg som resten av serverane, så i tilfelle brann er ikkje sikkerheitskopiane i noko fare. Sikkerheitskopiar blir tatt fortløpande, pluss full sikkerheitskopi kvart døgn. Ved brann blir serverrommet automatisk tømt for oksygen. Det er ikkje nemnt kva som skjer i tilfelle brann og det er personar inne i serverrommet.

Serverrommet ligg utan for flomfare, og serverane ligg so pass djupt inne i bygninga at lynnedslag ikkje vil råka serverane. I tillegg har serverrommet to sett med leidningar

som straum og fiber går igjennom, so dersom det skjer noko med den eine har serverrommet fortsatt straum og nett-tilgang. I tillegg står der eit diesel-aggregat som startar opp automatisk ved straumbrot. Når det gjeld hacking svarar kommunane at det er mange lag med sikkerheit som ligg bak, men at målretta angrep er vanskelig og umulig å være 100% sikra mot. I det store og heile ser eg at kommunane som har svart på undersøkinga har gjort seg flid med serverromma, og gjort sitt for ei grundig risikovurdering før og under bygging.

Når det gjeld kommunar som nyttar seg av skybaserte løysingar frå eksterne leverandørar er saka ein annan. Eg spurde om dersom dei skifta leverandør, om dei får hjelp av den gamle leverandøren til å flytte materialet over til den nye, og om det var stadfesta i kontrakta. Då fekk eg til svar at det kjem ann på kva dei krev i kravspesifikasjonen. Kravspesifikasjonen er kundens krav over kva produktet skal innehalde i forhold til funksjonalitet og kva lover som skal følgjast.

Dernest spurde eg kven sørgar for konvertering til nye filformat i tråd med Noark standaren. Eg spurde om det er ein jobb kommunane må gjøre sjølve eller er det noko leverandøren tek ansvar om? Er dette avtalt? Har kommunane rutinar for at skjekksummane blir bevart så materialet kan sporast og nyttast som bevis? Der fekk eg til svar at det gjørast enten av kommuna eller leverandør. Det er avtalefesta. Det som undrar meg då er om det er avtalefesta, veit ikkje kommuna med ein gong kven som skal gjøre det? Om det er kommuna eller leverandøren? Dette verkar noko usikkert. Deretter spurde eg om dei hadde søkt til Riksarkivaren om dispensasjon frå utførselsforbudet i arkivlova § 9 bokstav b, noko dei ikkje hadde gjort.

Heilt til slutt fortalde eg litt om Riksarkivet sitt eArkiv, og spurde om kommuna kunne tenkje seg å gå over til eArkiv seinare om det vart aktuelt. Det svarte dei at det kunne dei tenkje seg.

## Risikoar

Det vil alltid være store risikoar ved bruk av serverrom både lokalt og eksternt. Det er klart at jo nærare noko er, jo lettare er det å vedlikehalde og overvake. Dei kommunane

som har velt eksterne skyløysingar er dei med minst kontroll på både kven som har tilgang og kvar deira materale finst i verden. Nedanfor har eg gått igjennom dei risikoane som eg meiner er mest sannsynlege både for interne og eksterne serverparkar. Det må være opp til arkivskapar sjølve å vurdere kor store desse risikoane gjeld for deira serverar. Dersom arkivskapar nyttar eksterne skybaserte løysingar er det ikkje like lett for dei å gjennomføre ei risikoanalyse med tanke på kvar dei plassera serverane og tilgangar, men dei kan som arkivskapar likevel sette visse krav til leverandøren.

Dersom ei kommune nyttar interne skyløysingar er det opp til dei sjølve å vurdere risikoane. Det er klart at ikkje alle risikoane som eg nemner her gjeld for alle kommunar. Det er mange kommunar der flom ikkje er eit problem for eksempel. I «Forskrift om offentlege arkiv» kapittel IV (1999) er det mange gode retningslinjer for korleis eit arkivrom skal være for å sikre at dokumentasjonen blir tatt vare på. «Forskrift om offentlege arkiv» (1999) skriv i §4-1 at «Arkivlokala hos offentlege organ skal gi arkivmaterialet vern mot vatn og fukt, mot brann og skadeleg varme, mot skadeleg påverknad frå klima og miljø og mot skadeverk, innbrot og ulovleg tilgjenge.» Denne lova er skreve då det var mest papirarkiv og ikkje serverrom, men likevel er den eit godt peikepinn for kva risikoar man skal tenkje på når man byggjer serverrom.

### Øydelagde serverar

Undersøkinga mi viser at kommunane har tenkt godt igjennom kvar dei plasserar sine serverar. Ingen ligg i nærleiken av elver som kan fløyme over, og dei har tatt høgde for lynnedslag. Dette samsvarar med forskrift om offentlege arkiv §4-6 som stadfestar at «Ein må ikkje ta i bruk arkivlokale ein veit kan vere truga av flaum eller overfløyming.» (Forskrift om offentlege arkiv 1999). I tillegg har nokre dieselaggregat som startar opp ved straumbrot og dobbel fiber med to vegar inn i bygninga. Dette medfører at om ei leidning blir kutta, går det likevel ei leidning til inn i bygget som tek i mot materiale. §4-7. fyste ledd i same forskrift stadfestar at «Det elektriske anlegget skal utførast i samsvar med forskriftene for slike anlegg i branntrygge lokale.» Noko som sikrar at det ikkje er det elektriske anlegget som skal være problemet dersom det oppstår brann,

men at det skal være forskriftsmessig utført. I følge mi undersøking blir serverrommet tømt for oksygen ved brann, og då er serverane trygge i det rommet.

I det store og heile er faren for at serverane blir øydelagt eit problem uansett kvar man har dei. Servera kan bli øydelagt av naturkatastrofar her som i alle andre land, men det er noko tryggare å ha arkivmaterialet ståande her i Noreg enn i andre stadar, både med tanke på krig, tilgjengelegheit, politisk stabilitet og naturkatastrofar.

### Innbrot i serverrom

«Bygningsdelar som avgrensar arkivlokalet, skal vere utforma slik at arkivmaterialet er fullgodt sikra mot innbrot og mot at uvedkomande elles kan sleppe inn.» (Forskrift om offentlege arkiv, 1999, §4-9). Undersøkinga mi viser at dersom det kjem eit fysisk innbrot frå utanforståande vil vaktelskapet rykke ut og samstundes varsle. Katastrofeplan med risikoanalyse ligg føre, og det er viktig at personar vil bli varsla i rett rekkefølje.

Dersom det skulle være uærleg tilsette eller leverandørar som er problemet, vil loggingssystemet vise kven som sist tok seg inn med hjelp av nøkkelkort. Undersøkinga mi viser at leverandørar har ikkje tilgang til serverrommet, berre etter avtale. Tilsette som har nøkkelkort er berre dei som har behov. Ved hjelp av dette vil risikoane for at tilsette eller leverandørar bryt seg inn være minimale og lett å spore. Undersøkinga mi viser at ingen av dei tilsette innan arkivet har blitt sikkerheitssjekka gjennom attest frå politiet. Referansar blir sjekka opp, men ikkje om søkjaren har ei kriminell fortid, med spelegalskap eller rusproblem. Dette vil ein sikkerheitssjekk vise.

### Hackar-angrep

Innbrot direkte på serverar utanfrå vil alltid være eit problem. For å gjere det vanskelegare å stogge innbrot direkte på serverane er gode brannmurar viktig. I tillegg er det viktig å undersøke at det man legg til ikkje er virus før man legg det inn på serverane. Likevel kan det skje om nokon ikkje tenkjer over kva dei opnar av e-post på

datamaskina si. Kommunane som er intervjuar opplyser at brannmuren deira er gode, men målretta angrep er ofte vanskeleg å forhindre.

## Migrering

Omgjering til nye format er kanskje noko av det mest dramatiske elektroniske dokument skal igjennom. Før eller seinare må dei konverterast til nye format, og då er det viktig at det blir gjort på rett måte for å bevare autensitet og integritet. Autensitet tyder at dokumentet er det det gir seg ut for å være. Kunsten blir å bevare det på ein slik måte at sjølv om filformatet blir endra, beheld den det opprinnelege innhaldet, både når det gjeld tekst og bilete. (Riksarkivaren 2012 3.1 s 12) Dette kan være eit problem då endring av filformat gjør at innhaldet kan endre seg. For eksempel kan bilete bli flytta på, overskrifter endra størrelse på eller liknande. Derfor nyttar arkivdepot sjekksummar når arkivdepotet gjør endringar i filformatet.

Endring av filformat er viktig, samstundes som det er ein risiko å ta. Når filformatet vert endra, kan det gjøre endringar inne i dokumentet og. Det kan endre formateringa så tekst ligg over bilete eller at tekst ikkje blir ført over til ny linje og teksten «forsvinn» ut av dokumentet, eller flytte rundt på bilete. Diverre er det er dette betre enn å ikkje endre filformatet. Filformatet arkivdepot mottar er spesifisert i «Forskrift om utfyllende tekniske og arkivfaglige bestemmelser om behandling av offentlige arkiver» (Behandling av offentlige arkiver, 2000), betre kjent som «Riksarkivens forskrift». I denne forskrifta er filformatet dokument skal avleverast i spesifisert til PDF/A, som er formatet som er nytta mest innan arkivfaget. Dersom dei seinare vel å bytte ut dette filformatet må filer migrerast til det nye filformatet. Dersom det ikkje blir gjort kan det være slik at ein om 10-15 år ikkje lengre kan opne fila. Det vere seg at fila er i PDF/A og man ikkje har program til å lese av denne filtypen lengre. Då vil alle dokumenta være tapt.

På grunn av dette er det viktig å migrere til nye filformat, og dokumentere kvifor det vart gjort. Då kan arkivdepotet vise til loggen som seier at denne personen gjorde denne endringa. Arkivdepotet kan sjå på loggen at dette var dokumentet som vart tatt

ut, fordi den har den sjekksummen. Då endringane vart gjort vart det generert ein ny sjekksum for dokumentet, som viser andre tal. På den måten viser arkivdepotet at dei har gjort endringar med heimel i denne lova, og på denne måten kan arkivdepotet dokumentere uautorisert tilgang. Sjekksummar visar ikkje kva som har blitt gjort, berre at det har blitt gjort ei endring. Det er viktig at alt som blir gjort med filer blir dokumentert slik at dei bevarer sin integritet og fortsatt kan brukast som bevis.

### Sletting og kassasjon

Blir materialet verkeleg sletta for all ettertid? Dette er noko man berre kan være sikker på om man tek ut harddisken materialet ligg på og øydelegg den. Det er klart at om ein har lokale serverar kan man formatere og skrive over, og dermed være ganske sikker på at materialet er sletta, spesielt sida man sjølv har tilgang til serverane og kan hindre at noko blir gjenoppretta ved ei seinare anledning. Dette er ein derimot ikkje sikker på om en server som står i utlandet. Dei kan seie at alt materialet er sletta, men dei kan ha overført det til ein annan lokasjon eller berre sperra kommunane sine tilgang til filene. Sjølv om noko står i ei kontrakt kan man som kommune eller privatperson aldri være heilt sikre på at det blir følgt opp av leverandøren.

### Utgåtte kontraktar

Kva skjer om kontraktane går ut, eller delar av den? Kommunane som deltok i mi undersøking svarte ikkje på om dei måtte gjere noko i forhold til at «Safe Harbor» ikkje lengre var kjent gyldig. Datatilsynet har laga ein vegvisar for kva som kan gjerast no når «Safe Harbor» ikkje lengre er gyldig og fram til «EU-U.S. Privacy Shield» kjem på bana. Vegvisaren fortel om tre standardkontraktar som er laga av EU-kommisjonen. Datatilsynet seier sjølve at desse standardkontraktane aldri vil gi et like godt vern som ved nasjonal lovgiving, men i mangel på en internasjonal avtale er dei kontraktane det best å nytte seg av no (Datatilsynet 23. Oktober 2015).

### Overgang til ein annan leverandør

Kva skjer med materialet om kunden velje å gå over til ein annan leverandør? Korleis kan kunden være sikker på at alt blir med og at det er autentisk? Kommunane i mi

undersøking hadde ikkje noko godt svar på dette, anna enn at «det står i kontraktane at leverandøren skal hjelpe med å flytta over data og slette det hjå seg sjølve når det er gjort». Alle kommunane som var med i undersøkinga var positive til Riksarkivets eArkiv og ville gjerne vurdere den når den er klar.

### Sikkerheitskopiar

Sikkerheitskopien, eller back-up som det ofte kallast, er ein kopi av alt som ligg på serverane. Denne blir som regel oppdatert i løpet av natta. Det er tydeleg at det har vært fokus på sikkerheitskopien når dei spurde kommunane byggjer serverrom og sikkerheitskopi-rom. Dei fleste praktisera det anbefalte frå «Forskrift om lagringsplikt for bestemte data og om tilrettelegging av disse data», også kjent som Datalagringsforskrifta (2013) §3-5, og tek sikkerheitskopi dagleg, sjølv om dei ikkje ligg under denne forskrifta eller at den har tredd i kraft enda. Den gjeld for «data som skal lagres for å avdekke, etterforske og straffeforfølge alvorlig kriminalitet.» (Datalagringsforskrifta 2013, §1). Det er då innforstått at det er greitt å miste ein dags arbeid om systema som er nytta skulle krasje.

### Innsyn

I dei elektroniske systema nytta i dag viser det seg at kommunane har dei åra som er digitaliserte tilgjengelige gjennom sitt arkivsystem. Materiale som er frå før det er ofte allereie avlevert då dei fleste i dag har nytta digitale arkiv dei siste 6-7 åra. Kven ser materialet som ligg lagra på serverane, og vil det bli sendt vidare til en tredjepart? Kvar blir det av opplysingane og kva blir dei brukt til?

Undersøkinga viser at dei som i dag nyttar skybaserte løysingar hjå eksterne leverandørar har også interesse for å seinare nytte Riksarkivets eArkiv når det er tilgjengelig for andre. Dette kan være fordi dei allereie nyttar skybaserte løysingar og dermed veit korleis det fungerer, og at det då er lettare å gå over til andre bedrifters tenester.

## Kva har løysingar har arkivskaparar vald sjølv?

Grunnlaget for undersøkinga mi er i hovudsak bygd på kva arkivskapar har vald sjølv av lokale eller eksterne serverparkar.

### Eksterne serverparkar

For det første er det ingen av kommunane i mi undersøking som har søkt til Riksarkivaren om dispensasjon frå utførselsforbodet i §9 bokstav b i arkivlova før dei flytta sine løysingar ut i skya. For det andre har Datatilsynet har gjeve løyve, men dei går rett i mot kva Riksarkivet meiner, med arkivlova på si side. Dette fører til ein kollisjon mellom myndigheitene og at kommunane som nyttar skybaserte løysingar frå eksterne leverandørar ikkje har lova på si side. Riksarkivet meiner skyløysingar er ulovleg (Riksarkivet 2014), og dei som vil nytte seg av dette må søke dispensasjon frå §9 bokstav b i arkivlova. Dette har ikkje blitt gjort hjå dei kommunane som eg har intervjuet.

### Lokale serverparkar

Ei av dei små kommunane eg intervjuet kom med eit spennande svar. I Sogn og Fjordane har 7 små kommunar gått saman om ei felles ordning for deira arkivsystem. Dei har i fellesskap oppretta eit lite serverområde som dei kallar Nordfjordnett, som kommunane sjølv eig og driftar (Jobbportalen for ingeniører og teknologer, 2015).

«Hos Nordfjordnett har de samlet kompetansen og fordelt utstyr på to høytliggjengelige datasentre som ved hjelp av fibernett forbinder de samarbeidende kommunene med samordnede tjenester.» (Angell-Dupont, 2014).

Dette samarbeidet har nok oppstått av feire grunnar. For det første er det dyrt at alle små kommunar skal ha eigne serverrom og IT-tilsette når det kan samkøyrast og få til ei felles løysing. For det andre slepp dei alle å lønne sju forskjellige IT-sjefar når dei berre kan lønne ein. For det tredje sikrar dei at kommunane gjør jobben likt og har samla kompetansen på eitt sted; men likevel lokalt.

Desse kan lett gå over til Riksarkivets eArkiv når det blir ferdig, for å få tilrettelagt si sakshandsaming etter kvart og retta opp feil undervegs. Denne løysinga bryt ikkje med arkivlova sin §9 bokstav b, og er likevel ei fullgod lokal løysing; både for å spare pengar og sikre kompetanse. Det er klart at denne løysinga krev ein del utbygging for å få det til, men dei har bygd ut fiber, (Angell-Dupont, 2014) og då går det raskt å få overført data til serverane som står i Måløy i Sogn og Fjordane.

Ei anna kommune eg intervjuar hadde ikkje denne typen samarbeid med andre kommunar, men jobba for seg sjølve. Dei kom med gode svar på kva som skjer ved brann og innbrot, og har tydelig tenkt igjennom korleis dei har bygd sine serverrom og funne noko som fungerer for seg der.

## Konklusjon og oppsummering

I denne oppgåva har eg, motivert av mitt fag, hatt eit ønske om å lære meir om skybaserte løysingar innan arkivfaget.

Lenge har interessa auka for skybaserte løysingar og deira forhold til arkivlova §9 bokstav b. Denne paragrafen hindrar utførsel av arkivmateriale til andre land, med mindre det er for signering eller skanning for seinare tilbakeføring. Noko som vil tilseie at å føre arkivmateriale ut or landet er ulovlig. I praksis har dette blitt gjort mot Riksarkivet, sidan det ikkje er søkt om dispensasjon frå arkivlova.

Noko av det som overraska meg mest var at småkommunane har funne ei skybasert løysing basert på at dei samarbeida, medan dei større kommunane ser ut til å være meir bestemt på å løyse problema sjølve. Det viser seg også at dei kommunane som har valt å gå ut i skya er gjerne dei som ikkje har blitt med på eit slikt samarbeid mellom andre kommunar, og funne ut at det er for dyrt å halde serverane sine i drift i den størrelsen som dei har før dei gjekk ut i skya.

Datatilsynet og Riksarkivet har ulike meiningar når det gjeld utførsel av arkivdokument. I utgangspunktet skal kommunane søke til Riksarkivet om å få lov til å føre

arkivdokument ut or landet, men det har ikkje blitt gjort. Datatilsynet har godkjent at kommunane nyttar skybaserte løysingar frå utanlandske leverandørar, medan Riksarkivet heile tida har vore tydelege på at dette ikkje er lov, med heimel i arkivlova sin §9 bokstav b. Dersom kommunane nyttar eit firma der serverane står i Noreg derimot, er det fullt lovleg å nytte skybaserte løysingar. Då Datatilsynet let Narvik kommune gå ut i skya var det fortsatt noko som heitte «Safe Harbor» som er omtala i rapporten. Denne er kjent ugyldig av EU-domstolen og ei ny avtale er undervegs (Datatilsynet 06. Oktober 2015).

Riksarkivets eArkiv vekker stor interesse hjå kommunane i min undersøking, og dei fleste er glade for tilbodet som no er under utprøving. Det viser seg i undersøkinga at dei kommunane som allereie nyttar skybaserte løysingar er mindre skeptiske enn dei kommunane som enda ikkje gjer det. Det kan være fordi dei kommunane som allereie nyttar skybaserte løysingar kjenner risikoane ved bruk og veit at det er mykje enklare for dei å nytte Riksarkivet si løysing enn deira utanlandske leverandørar sine løysingar.

I framtida kan eg sjå for meg at arkivskapar kan avlevere direkte til arkivdepot via nett. Då kan arkivdepotet sjå igjennom avleveringa med ein gong og påpeike dei feil som eventuelt er der. Utfordringane som kan bli er å få sendt filene til avlevering, er å få laga ei rutine på det. Spesielt for Riksarkivet som plutselig vil få mykje meir jobb på avleveringsfronten. Samstundes ser eg for meg at større offentlege etatar som for eksempel Kartverket som har store filer det tek lang tid å avlevere kan spare mykje tid på å halde Riksarkivet «oppdatert» med dei karta som ikkje lengre er nytta hjå dei.

Mi eiga undersøking viser i det store og heile at arkivskaparane i kommunane har funne løysingar som begrensa risikoane før dei har bygd egne serverrom. Dessverre er dei som nyttar skybaserte løysingar ikkje like heldige slik eg ser det. Jo meir eg har jobba med denne oppgåva jo meir usikkert og lite gjennomtenkt verkar det å nytte skybaserte løysingar der serverane er plasserte i eit anna land. For det første kjem det fram at «Safe Harbor» ikkje er so trygt som var venta, og for det andre fordi eg har satt med meir inn i Snowden-saka. Eg tenkjer at når det amerikanske etterretningsorganet

NSA klarar å ha ei so omfattande overvåkning utan at nokon oppdagar det, bør arkivskapar revurdere tryggleiken til materialet som ligg i skya.

Hadde det ikkje vore for Snowden er det ikkje sikkert at denne avsløringa ville skjedd på mange år enda. Konsekvensane ville vært at vi ikkje var like skeptiske til skybaserte løysingar og at NSA fekk tilgang til mykje tausheitslagt materiale om norske innbyggjarar.

Deretter utgreia eg om risikoar knytt til skybaserte løysingar. Dette gjeld både for dei kommunane som nyttar eigne løysingar lokalt og dei som har tatt steget ut hjå dei utanlandske leverandørane. Her har eg nemnt øydelagde serverrom, tilgangar frå uvelkomne både fysisk i serverromma og via internett, altså hackar-angrep. Deretter har eg nemnt migrering og risikoane det inneber, sletting og kassasjon. Blir verkeleg det kommunane lagrar i skya sletta når dei ber om det? Kva skjer om kontraktane går ut? No var det akkurat det som skjedde med «Safe Harbor», og kva konsekvensar fekk det for kommunane som har valt utanlandske leverandørar for sine skyløysingar?

Det visar seg at kontraktane til kommunane som nyttar utanlandske leverandørar for sine skyløysingar inneheld rutinar for kva som skjer om ei kommune går over til ein annan leverandør. Likevel har ingen har hittil prøvd det so det er ingen som veit korleis dette fungerer i praksis. Sikkerheitskopiar er noko som alle med eigne serverrom bør ha tilgjengeleg dersom uhellet er ute og systema er under angrep. Kommunane som svarte på dette svarte at det dei mister er maks ein arbeidsdag, sidan ein sikkerheitskopi verte tatt kvar natt, noko som er innanfor det man både som innbyggjar og tilsett kan krevje. Kommunane har det digitale materialet tilgjengeleg for innsyn, medan det som er eldre enn deira saks- og arkivsystem er avlevert til deira tilknytte Interkommunalt Arkiv eller IKA for kort.

Innleiingsvis spurde eg kva forhold kommunane har til skybasert datalagring i dag. Slik eg ser det etter å gjennomført undersøkinga og snakka med kommunane kan forholda delast inn i to grupper: Dei som nyttar eksterne skybasert løysingar allereie og dei som ikkje gjør det.

Dei som nyttar skybaserte løysingar er godt nøgde med bruka av skybasert datalagring og er opne for å fortsette med det. Arkivskapar ser problema med at det krigar med diverse lovar, og eg trur at arkivskaparane etter kvart vil nytte seg skybaserte løysingar internt i Noreg. Enten når Riksarkivets eArkiv kjem på plass eller hjå nokon andre.

Dei kommunane som ikkje nyttar skybaserte løysingar har eit anna forhold til den store skya. Dei har følgd debattane, datatilsynet og Riksarkivet på avstand, og ser at einigheita er fråverande. Eg trur ikkje kommunane kjem til å kaste seg ut i skya utan å gjøre godt forarbeid først, og kanskje til og med då vil dei berre nytte norske leverandørar slik at serverane står i Noreg. Då veit kommunane at dei ikkje bryt nokon lovar, og det er ein mykje enklare kommunikasjon som skjer. Slik sett er det bra at nokre kommunar har tatt steget ut i skya, slik at andre kommunar får sjå konsekvensane og kva dei eventuelt ikkje skal gjøre sjølve dersom dei vil nytte seg av skya.

Kor mykje har egentlig kommunane spart på å nytte seg av skybaserte løysingar? Dei einaste tala eg har funne er frå Moss Kommune, der dei fortel at dei vil spare 12 millionar i løpet av ei femårsperiode ved å leggje 40% av deira IT-plattform og databehandling (Jørgenrud 2015).

Konklusjonen min er at slik arkivlova er no, er skybaserte løysingar frå eksterne leverandørar ulovleg. Kommunane som nyttar skybaserte løysingar frå utanlandske leverandørar utan å søke til Riksarkivet om å få føre sine arkiv ut or landet bryt med arkivlova sin §9 bokstav b. I tillegg bryt dei med Personopplysningslova §4 og 30 bokstav a til og med h. Slik eg ser det kan Riksarkivet bli flinkare til å informere om forskjellige måtar å unngå å føre materiale til utlandet. Riksarkivet og Arkivverket kan alliere seg med IKA'er og Datatilsynet slik at alle er einige om kva som skal seiast til kommunane når dei kjem og spør.

## Litteraturliste

Angell-Dupont, Maria. (28. Mars 2014). Raskere nett samler Norge til ett rike. *Fiberbloggen.no* Henta 13. Mars 2016 frå <http://fiberbloggen.no/raskere-nett-samler-norge-til-ett-rike/>

Arkivlova (1999). *Lov om arkiv*. Henta 14. Januar 2016 frå <http://lovdata.no/lov/1992-12-04-126/>

Behandling av offentlige arkiver (2000). *Forskrift om utfyllende tekniske og arkivfaglige bestemmelser om behandling av offentlige arkiver*. Henta 04. Mai frå <https://lovdata.no/dokument/SF/forskrift/1999-12-01-1566>

Christensen K. (05. Februar 2013, kl.07:20) Alta kaster seg inn i skyen. *ComputerWorld*. Henta 04. Mars 2016 frå <http://www.cw.no/artikkel/nett-tjenester/alta-kaster-seg-inn-skyen>

Christensen K. (06. Mars 2014, kl.14:15) Flytter Moss ut i skyen. *ComputerWorld*. Henta 04. Mars 2016 frå <http://www.cw.no/artikkel/cloud-computing/flytter-moss-ut-skyen>

Datalagringsforskriften (2013) *Forskrift om lagringsplikt for bestemte data og om tilrettelegging av disse data*. Henta 20 April 2016 frå <https://lovdata.no/dokument/SF/forskrift/2013-05-14-484>

Datatilsynet (12. Februar 2014) *Årsmelding for 2013*. Henta 21. April 2016 frå <https://www.datatilsynet.no/Om-Datatilsynet/Arsmeldinger/Arsmelding-for-2013/>

Datatilsynet (06. Oktober 2015) *Safe Harbor-beslutningen kjent ugyldig*. Henta 20. April 2016 frå <https://www.datatilsynet.no/Nyheter/2015/Safe-Harbor-beslutningen-kjent-ugyldig/>

Datatilsynet (16. Oktober 2015) *Safe Harbor - prinsipper om overføring av opplysninger til USA*. Henta 18. April 2016  
<https://www.datatilsynet.no/Regelverk/Internasjonalt/Overfoering/Safe-Harbor-prinsippene/>

Datatilsynet (23. Oktober 2015) *Hvordan overføre personopplysninger til utlandet etter Safe Harbor*. Henta 26. April 2016 frå  
<https://www.datatilsynet.no/Regelverk/Internasjonalt/Hvordan-overfore-personopplysninger-til-utlandet-etter-Safe-Harbor/>

Datatilsynet sin rapport (21. september 2012). *Saken avsluttes - Ny e-postløsning i Narvik Kommune – Google Apps*. Henta 04. Mars 2016 frå  
[http://www.media.allerinternett.no/km\\_fil/6/4518026.pdf](http://www.media.allerinternett.no/km_fil/6/4518026.pdf)

Dørum, A M (2014) Arkivering i skyen. I A. Neergaard (Red.), *Dokumentasjonsforvaltning og arkiv i det 21. århundre*. (s. 121-136). Oslo: Fagbokforlaget Vigmostad og Bjørke AS

European Comission 29. February 2016) *Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield*. Henta 20. April 2016 frå [http://europa.eu/rapid/press-release\\_IP-16-433\\_en.htm](http://europa.eu/rapid/press-release_IP-16-433_en.htm)

Forskrift om offentlege arkiv (1999). *Forskrift om offentlege arkiv*. Henta 26. April 2016 frå <https://lovdata.no/dokument/SF/forskrift/1998-12-11-1193>

Jobbportalen for ingeniører og teknologer (04. Mai 2015). *Vil du være med på å forme fremtiden for IT-drift?* Henta 13. Mars 2016 frå <http://jobb.tu.no/jobs/it/54023-vil-du-vaere-med-paa-aa-forme-fremtiden-for-it-drift>

Johannessen, C. & Gaarder, T. A. (13. August 2015). Arkivloven og skytjenester – sikring eller hindring? *Riksarkivet*. Henta 28. Januar 2016 frå

<http://arkivverket.no/arkivverket/Arkivverket/Om-oss/Aktuelt/Nyhetsarkiv/Arkivloven-og-skytjenester-sikring-eller-hindring>

Jottacloud (udatert). *Om Jottacloud*. Henta 21. Februar 2016 frå

<https://www.jottacloud.com/nb/om-oss/>

Jørgenrud, M. (Oppdatert 10. Februar 2016.) Moss går ut i nettskyen. *Digi.no*. Henta 28. April 2016 frå <http://www.digi.no/bedriftsteknologi/2014/04/10/moss-gar-ut-i-nettskyen>

Kirkenes, L. M. (24. september 2012, kl.13:02) Datatilsynet snur i Narvik-saken. *ComputerWorld*. Henta 04. Mars 2016 frå <http://www.cw.no/artikkel/offentlig-sektor/datatilsynet-snur-narvik-saken>

Kommunal- og moderniseringsdepartementet (18. April 2016) *Nasjonal strategi for bruk av skytenester*. Henta 20. April 2016 frå [https://www.regjeringen.no/contentassets/4e30afec51734d458596e723c0bdea0e/nasjonal\\_strategi\\_skytenester.pdf](https://www.regjeringen.no/contentassets/4e30afec51734d458596e723c0bdea0e/nasjonal_strategi_skytenester.pdf)

Lygre, E. T. (9. November 2015 kl. 12:42) Itslearning kjøper sin største konkurrent i Norge. *Digi.no*. Henta 08. Mars 2016 frå <http://www.digi.no/avtalerkontrakter/2015/11/09/itslearning-kjoper-sin-storste-konkurrent-i-norge>

Metadatakatalog (13. Mars 2013) Vedlegg 1 til Noark 5. Henta 20. April 2016 frå <https://www.arkivverket.no/arkivverket/content/download/12860/124477/version/2/file/Vedlegg+1+Metadatakatalog+v.+3.1.pdf>

Moss kommune (udatert). *Kontaktinformasjon*. Henta 28. April 2016 frå <http://www.moss.kommune.no/kontakt-oss/>

Personopplysningsloven (2001). *Lov om behandling av personopplysninger*. Henta 04. Mars 2016 frå <http://lovdata.no/lov/2000-04-14-31/>

Regjeringen (18. April 2016) *Offentlege verksemder skal vurdere skytenester*. Henta 20. April 2016 frå <https://www.regjeringen.no/no/aktuelt/offentlege-verksemder-skal-vurdere-skytenester/id2484511/>

Riksarkivaren (08. Juni 2012) *Vel bevart! Rapport fra samarbeidsprosjektet DIAS – Digitalt arkivpakkestruktur*. Henta 20. April 2016 frå [http://www.arkivverket.no/arkivverket/content/download/11137/110188/version/1/file/DIAS\\_Sluttrapport-Del1.pdf](http://www.arkivverket.no/arkivverket/content/download/11137/110188/version/1/file/DIAS_Sluttrapport-Del1.pdf)

Riksarkivet (22. Mars 2013) *Noark 5 v. 3.1: Standard for elektronisk arkiv*. Henta 31.03.2016 frå <https://www.arkivverket.no/arkivverket/content/download/12962/125147/version/2/file/Noark+5+v.+3.1.pdf>

Riksarkivet (29. September 2014) *Riksarkivaren seier nei til skyarkivering i utlandet*. Henta 12. April 2016 frå <http://arkivverket.no/arkivverket/Arkivverket/Om-oss/Aktuelt/Nyhetsarkiv/Nyhetsarkiv-2014/Riksarkivaren-seier-nei-til-skyarkivering-i-utlandet>

Riksarkivet (04. November 2015). *eArkiv*. Henta 04. Mars 2016 frå <http://arkivverket.no/arkivverket/Offentleg-forvalting/eArkiv>

Urtegaard, G. (20. Januar 2015). *Innføring av eArkiv i offentlig forvaltning. Riksarkivet*. Henta 14. Januar 2016 frå <http://arkivverket.no/arkivverket/Arkivverket/Om-oss/Aktuelt/Nyhetsarkiv/Innfoering-av-eArkiv-i-offentlig-forvaltning>

Venli, V. (19 September 2013 09:22) Sjekk planer for elektronisk arkiv. *Kommunal rapport*. Henta 28. April 2016 frå [http://kommunal-rapport.no/artikkel/sjekk\\_planer\\_for\\_elektronisk\\_arkiv](http://kommunal-rapport.no/artikkel/sjekk_planer_for_elektronisk_arkiv)