Arbeidsgrupperapport 2015

Kartlegging av hindringer i regelverk for bruk av skytjenester

Overlevert kommunal- og moderniseringsdepartementet 13. mai 2015

Arbeidsgrupperapport 2015

Kartlegging av hindringer i regelverk for bruk av skytjenester

Overlevert kommunal- og moderniseringsdepartementet 13. mai 2015

Rapport fra interdepartemental arbeidsgruppe med deltakelse fra Finansdepartementet (FIN), Justis- og beredskapsdepartementet (JD), Kommunal- og moderniseringsdepartementet (KMD), Kunnskapsdepartementet (KD), Kulturdepartementet (KUD), Nærings- og fiskeridepartementet (NFD) og Samferdselsdepartementet (SD)

Innhold

1. Sammendrag

Kommunal- og moderniseringsdepartementet har etablert en interdepartemental arbeidsgruppe for å kartlegge juridiske hindringer for bruk av skytjenester. Målet med arbeidet har vært å legge til rette for sikker og forutsigbar bruk av skytjenester innenfor rammene av norsk lov. Gjennom rapporten ønsker gruppen å synliggjøre skrankene for skytjenester, og klargjøre mulighetene både offentlige virksomheter og næringsliv har til å ta i bruk slike tjenester.

Arbeidsgruppen har funnet at det er særlig tre typer data som det stilles spesielle krav til behandlingen av: finansielle data, arkivdata fra offentlige virksomheter og personopplysninger. Virksomheter må derfor avklare hva slags data de behandler, og hvilke data de ønsker å behandle i en skyløsning. I tillegg må virksomheter være bevisste på sikkerheten til dataene de behandler, gjennom risikovurderinger og avklaringer av lovligheten ved behandlingen. Konfidensialitet, integritet og tilgjengelighet er viktige, generelle prinsipper for behandlingen av data, og disse må ligge til grunn for virksomhetenes vurderinger.

Arbeidsgruppen ser behov for utstrakt veiledning innen enkelte sektorer, for å bidra til å oppklare enkelte uklarheter regelverket oppstiller. Arbeidsgruppen ser også behov for at lovgiver er bevisst på de uklarheter som skapes i regelverk ved lovrevisjoner og etableringen av nytt regelverk. Teknologinøytralt regelverk må dreie seg om mer enn det å sidestille analoge og digitale løsninger. Andre, uforutsette teknologiske problemstillinger kan dukke opp i fremtiden, og grenseoverskridende teknologi slik som skytjenester er et eksempel på dette.

Teknologiutviklingen skaper utfordringer det er vanskelig for lovgiver å holde tritt med. Dette medfører behov for å tenke annerledes ved lovrevisjoner og -utforming for å sikre at man ikke skaper hindringer som gjør det vanskelig å ta i bruk de mest hensiktsmessige og kostnadseffektive løsningene.

Etter en gjennomgang og vurdering av eksisterende lovgivning, foreslår arbeidsgruppen blant annet:

- Å vurdere behov for endring av forskrift om offentlige arkiv, for å tillate lagring av arkiver fra offentlige virksomheter i skyløsninger med servere i utlandet
- Å vurdere forutsetninger og handlingsrom for å utvide antall land hvor man tillater lagring av bokføringsdata
- At det tas initiativ til å harmonisere tilsynspraksis når det gjelder data lagret i skytjenester.

2. Innledning

2.1 Formål og politisk forankring

Med grunnlag i Meld.St. 23 (2012-2013) *Digital agenda for Norge: IKT-politikk for vekst og verdiskapning* har Kommunal- og moderniseringsdepartementet igangsatt arbeid for å utforme en norsk politikk for bruk av skytjenester[1]. Det uttales i meldingen at departementet ønsker "*å legge til rette for sikker og forutsigbar bruk av slike tjenester innenfor rammene av det norske regelverket*." Regjeringen har også, som en del av satsingen "En enklere hverdag for folk flest", som mål å forenkle lover og regler. En gjennomgang av regelverket for å fjerne unødige hindringer og rydde opp i uklarheter vil kunne bidra til å legge til rette for sikker og forutsigbar bruk av skytjenester innenfor rammene av norsk lov. I Norge eksisterer det per i dag ikke noen offisiell politikk for bruk av skytjenester i offentlig sektor. Kommunal- og moderniseringsdepartementet vil derfor legge fram en nasjonal strategi for bruk av skytjenester i løpet av 2015. Den juridiske gjennomgangen presentert i denne rapporten danner et viktig grunnlag for strategiarbeidet.

Skytjenester vil kunne bidra til rimelige og fleksible IKT- løsninger, både for næringsliv og offentlige virksomheter. Kommunal- og moderniseringsdepartementet ønsker derfor å åpne opp mulighetsrommet slik at skytjenester kan være et reelt alternativ når virksomheter skal vurdere hvilke IKT-løsninger som er mest hensiktsmessige, og gir den mest kostnadseffektive løsningen, for deres behov. Kjøp av IKT-tjenester fra skyen reduserer eller fjerner behovet for store investeringer i datautstyr. Bruk av skytjenester kan dermed potensielt fremme konkurransekraften for næringslivet: Bruk av slike tjenester kan gi mer kostnadseffektive løsninger, senke kostnadene for nyetablering og fremme innovasjon både i offentlig og privat sektor. Vi forventer at bruk av skytjenester i offentlige virksomheter kan føre til betydelige kostnadsbesparelser og økt fleksibilitet. Det er derfor avgjørende å avklare hvilke hindringer, i form av skranker i regelverk, som foreligger, for å kunne ta stilling til i hvilken grad virksomheter kan ta slike tjenester i bruk.

2.2 Arbeidsgruppens mandat og organisering

Som en del av arbeidet med en nasjonal strategi for bruk av skytjenester har KMD opprettet en interdepartemental arbeidsgruppe som har hatt i oppdrag å kartlegge hindringer i regelverk for bruk av skytjenester.

Arbeidsgruppen har hatt deltakelse fra Finansdepartementet (FIN), Justis- og beredskapsdepartementet (JD), Kunnskapsdepartementet (KD), Kommunal- og moderniseringsdepartementet (KMD), Kulturdepartementet (KUD), Nærings- og fiskeridepartementet (NFD) og Samferdselsdepartementet (SD). Arbeidet har vært

[1] Kommunal- og moderniseringsdepartementet har valgt å følge amerikanske National Institute of Standards and Technology (NIST) sin definisjon av nettsky/skytjenester ("Cloud computing"), se kapittel 3.1

ledet av KMD, som også har besørget sekretariat for gruppen. Arbeidsgruppen har hatt jevnlige møter siden arbeidet startet opp i oktober 2014.
Gruppen har hatt følgende mandat:

"*Arbeidsgruppen skal foreta en kartlegging av juridiske hindringer for bruk av skytjenester, både i privat og offentlig sektor.*

Arbeidsgruppen skal identifisere lov- og regelverk hvor det foreligger hindringer eller uklarheter når det gjelder bruk av skytjenester, spesielt for offentlig sektor. Dette omfatter både regelverk hvor det er klare juridiske hindringer, og regelverk som gir rom for ulike tolkninger og slik kan skape usikkerhet hos brukerne.

1. *Identifisere lov- og regelverk der det kan være aktuelt å sette i gang arbeid med tilpasning til bruk av skytjenester.*
2. *Foreslå tiltak som kan gjøre det tydeligere for både tilbydere og innkjøpere hvilke regulatoriske rammer som finnes for bruk av skytjenester, ved å:*
   - *foreta juridiske avklaringer og presiseringer*
   - *foreslå eventuelle regelverksendringer.*"

Arbeidsgruppen har forstått mandatet slik at hovedoppgaven er å kartlegge konkrete hindringer i regelverk for bruk av skytjenester og foreta avklaringer rundt regelverk som kan fremstå som en hindring for virksomheter som ønsker å ta slike tjenester i bruk. Arbeidsgruppen har derfor undersøkt regulatoriske problemstillinger som det for en virksomhet er *relevant å forholde seg til* ved behandling av virksomhetens data. Det vil si regelverk virksomheter må forholde seg til i alminnelighet, men som oppleves som særlig relevante for skytjenester. Det presiseres at en hindring i regelverket kan være både nødvendig og ønskelig. Slike hindringer skal selvsagt opprettholdes. Samtidig vil den teknologiske utviklingen ofte ligge i forkant av regelverket og dette kan føre til uhensiktsmessige og utilsiktede regelverkskonsekvenser. Arbeidsgruppen har derfor sett det som relevant å belyse de skranker de har avdekket for bruk av skytjenester, både slike som anses nødvendige ut fra lovens formål, og slike som arbeidsgruppen dels anser som unødvendige.

Enkelte utfordringer ved bruk av skytjenester har vært mye omtalt i media eller gjennom henvendelser fra virksomheter, og disse har vært førende for hvilke spørsmål arbeidsgruppen har prøvd å trekke frem. Eksempler på slike problemstillinger er spørsmål om krav til lagring av dokumenter, tilgangsstyring, risikovurderinger, overføring mellom aktører og land, ulikheter i regelverk mellom offentlig og privat virksomhet, og ulikheter på tvers av sektorer.

Arbeidsgruppens gjennomgang av regelverk er forsøksvis uttømmende innen de sektorer som har deltatt i arbeidsgruppen. Det har likevel ikke vært mulig å gå gjennom samtlige lover i detalj. Slik avgrensning omtales under redegjørelsen for de enkelte sektorene. Dette innebærer også at arbeidet avgrenses mot regelverk underlagt de departementer som ikke har deltatt i arbeidet.

Gruppen har ansett at klargjørende vurderinger av personvernregelverket er gjennomført av Datatilsynet. Gruppen har derfor ikke gjort egne vurderinger av dette regelverket. Arbeidsgruppen har likevel ansett det som hensiktsmessig å sammenligne behandlingen av personopplysninger med behandlingen av andre data i skytjenester. Det refereres da til Datatilsynets vurderinger. Vi avgrenser i tillegg mot spesifikke sikkerhetskrav knyttet til kritisk infrastruktur og kommunikasjonstjenester.

I noen tilfeller har vi avdekket krav som innebærer at informasjon verken kan behandles eller lagres digitalt. Vi anser slike lover som å ligge utenfor gruppens arbeidsområde. Slikt regelverk utgjør først og fremst et hinder for *digitalisering*, og det anses ikke som relevant å drøfte skytjenester som et alternativ for data som ikke opptrer i digital form.

2.3 Andre, relaterte utredninger

Rapporten følger i rekken av flere tidligere utredninger og kartlegginger som er utført som har hatt som utgangspunkt å se på hvorvidt regelverket er tilpasset en digital hverdag. eRegelprosjektet[2] på starten av 2000-tallet hadde som hensikt å kartlegge og senere fjerne hindre for digital kommunikasjon. Som følge av eRegelprosjektet ble det foretatt flere endringer for å gjøre regelverk teknologinøytralt. Dette ble fulgt opp i kartleggingen av hindringer i regelverk for digital kommunikasjon[3] i 2013. En annen rapport som har sett på lignende utfordringer er kartleggingen av hindre for digitale forretningsprosesser i 2014.[4]

Disse tidligere kartleggingene er gode utgangspunkt for politikkutforming og regelverksrevisjon. Den juridiske gjennomgangen arbeidsgruppen har foretatt er ment å gi tilsvarende bidrag, og er derfor en viktig komponent i det større arbeidet med skytjenester.

2.4 Rapportens struktur og innhold

I rapporten vil det først redegjøres for de juridiske utgangspunkter for vurderingene som foretas. Deretter følger en redegjørelse for internasjonale kartlegginger, slik at vår rapport settes inn i en større sammenheng.

Etter disse to innledende kapitlene følger arbeidsgruppens funn innen hver enkelt sektor. Lover og forskrifter presenteres etter fagområde, hvor aktuelle paragrafer og tolkningen av disse drøftes opp mot bruken av skytjenester. Konkret gjelder regelverket som undersøkes typisk forhold som lagring av dokumenter, behandling av

---

[2] Ot.prp. nr. 108 (2000-2001) *Om lov om endringer i diverse lover for å fjerne hindringer for elektronisk kommunikasjon* og Ot.prp. nr. 9 (2001-2002) *Om lov om endringer i diverse lover for å fjerne hindringer for elektronisk kommunikasjon*

[3] Fornyings-, administrasjons- og kirkedepartementet (2013). *Rapport fra arbeidsgruppe: Kartlegging av hindringer i regelverk for digital kommunikasjon*

[4] KPMG (2014): *Kartlegging av hindre for digitale forretningsprosesser.* Rapport på oppdrag fra KMD

ulike data, flytting av data mellom systemer og over grenser, og tilgang på data. Dette vil, dersom det ikke er spesifisert nærmere, omtales som ”behandling av data”.

En lov eller forskrift kan utgjøre en absolutt hindring, eller den kan være et indirekte hinder gjennom å stille uklare eller kompliserte krav som må imøtekommes, eller tiltak som må iverksettes, før en nettskytjeneste kan tas i bruk. Lover og forskrifter vil i rapporten omtales som hindre i begge disse tilfellene. Det finnes en rekke lover hvor det har vært en antatt usikkerhet om forholdet til skytjenester. Arbeidsgruppen angir da i sin konklusjon hvorvidt loven/forskriften oppstiller enten ”ingen klar hindring”, en ”indirekte hindring” eller en ”klar/absolutt hindring” for bruk av skytjenester.

Der vi ser det foreligger hindringer, vil vi vurdere følgende:

- om det er aktuelt å foreta juridiske avklaringer og presiseringer til lovteksten
- foreslå endringer i loven, men slik at formålet bak loven kan opprettholdes med annen ordlyd
- foreslå andre tiltak for å avhjelpe uklarheter som måtte finnes

Der gruppen har kommet til at det ikke foreligger en hindring for bruk av skytjenester, tas det forbehold om det kan være situasjoner som vi ikke har tenkt på, som krever at fortolkningen må revurderes.

Avslutningsvis vil vi drøfte noen felles problemstillinger og betraktninger løsrevet fra sektoromtalen, før vi oppsummerer de tiltak arbeidsgruppen foreslår.

3. Juridiske utgangspunkter for kartleggingen

3.1 Nærmere om skytjenester

KMD har valgt å følge amerikanske National Institute of Standards and Technology (NIST) sin definisjon av nettsky ("Cloud computing")[5]:

Skytenester (*cloud computing*) er en modell som gjør det mulig å få tilgang til et sett konfigurerbare dataressurser (for eksempel nettverk, servere, lagring, applikasjoner og tjenester) som:

- er lett tilgjengelige over alt
- blir levert og priset etter behov (*on demand*)
- kan skaffes raskt og gjøres tilgjengelig med minimalt med administrasjon eller involvering fra tilbyderen

Det er mye som kan kalles en nettsky, og vi begrenser omfanget av tjenester til kjøp av prosessorkraft, og lagrings- og databearbeidingskapasitet som er skalerbar hos ekstern part med leveranse over eksterne nettverk. Avhengig av hva som tilbys av leverandøren deles tjenestene normalt opp i tre tjenesteformer: Platform as a service (PaaS), Software as a service (SaaS) og Infrastructure as a service (IaaS). Arbeidsgruppens vurderinger avgrenses ikke mot noen bestemte former for skytjenester, og følgende vurderinger gjelder generelt for tjenesteformene IaaS, PaaS og SaaS.

Vi deler ofte skytjenester inn i tre leveransemodeller: Den allmenne skyen ("public cloud") er tilgjengelig for hele markedet og serverene er ofte plassert flere ulike geografiske steder. Gruppeskyen er tilgjengelig for et utvalg virksomheter, gjerne innenfor samme sektor (for eksempel universiteter og høgskoler). En hybrid sky er en kombinasjon av en lukket, privat løsning, og allmenn sky eller gruppesky. En hybrid sky er en spesielt aktuell modell for virksomheter som behandler data av ulik karakter og som møter ulike regulatoriske krav til behandlingen av disse.

Særlig aktuelle regulatoriske utfordringer knyttet til skytjenester er blant annet regler om:

- **lagring av data**. Her kan det være aktuelt å se på spørsmål om medium for lagring, lokalisering, tidsaspekt for lagring, tilgjengelighet, sikkerhet og jurisdiksjon. Hvilke plikter/ansvar har virksomheten selv?
- **tilgang til dataene**. Her er særlig tilgjengelighet, lokalisering, sikkerhet og jurisdiksjon aktuelle utfordringer
- **Datasikkerhet.** Her er særlig lokalisering, tilgang, tidsaspekt og oppbevaringskrav noen aktuelle tema

[5] Peter Mell og Timothy Grace (2011): *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology,* U.S. Department of Commerce, NIST Special Publication 800-145

3.2 Hva er en hindring i regelverk?

Det er ulike grunner til at en lov kan være til hinder for bruk av skytjenester, og hindringene følger enten direkte eller indirekte, av lovgivningen, eller gjennom praktisering av kontroll fra kontroll- og tilsynsorganer.

Som et utgangspunkt kan vi skille mellom absolutte hindringer for bruk av skytjenester, og de tilfeller hvor skytjenester kan benyttes, enten med eller uten krav til lokasjon. Lokaliseringskrav kan tilsi at bruk av skytjenester er mulig, men det foreligger krav til lagring av dataene for eksempel på servere innen Norge, Norden, eller EØS. For etterlevelse av lover med begrensninger på lokalisering møter vi enkelte særlige utfordringer. Dataene som behandles i en skytjeneste befinner seg fysisk på en eller flere servere. Den geografiske plasseringen av disse serverne avgjør ofte hvor dataene vil anses å bli behandlet, og således som regel jurisdiksjonen over dataene, med mindre noe annet avtales i databehandleravtale med leverandøren av skytjenesten. En alminnelig forutsetning for at dataene i en skytjeneste skal anses for å bli behandlet i Norge, er som regel at serverne befinner seg i Norge.[6]

For å kunne konkludere med at det ikke foreligger hindringer i en lov i det hele tatt har vi i arbeidsgruppen forutsatt at en også må kunne tillate bruk av skytjenester med servere plassert utenfor Europa (for alle praktiske formål definerer vi Europa som tilsvarende EØS-området) innen regelverket. Slike lokaliseringskrav følger som regel direkte av lov eller forskrift, men også praksis fra kontrollorganer vil kunne påvirke reglene.

Et annet forhold som kan påvirke lovligheten av bruk av skytjenester følger av begrensninger med utgangspunkt i sikkerhetsspørsmål. Disse kan følge av lovbestemte risikovurderinger som må foretas, eller konkrete krav til nivå på sikkerheten. Disse kravene følger enten direkte av lovverket, eller av praksisen til kontroll- og tilsynsorganer.

Et grenseområde til sikkerhetsspørsmål er regelverk som setter skranker for utkontraktering av virksomhetsoppgaver. Utkontraktering, også kjent som outsourcing av virksomhetsoppgaver, og bruk av skytjenester til behandling og lagring av data er både i praksis og rettslig sett ulike forhold, og ikke alltid sammenfallende. Likevel er det flere likheter ved disse to situasjonene, også ved bruk av skytjenester vil en tredjepart få en rolle ved behandlingen av data. Dette trekket ved skytjenester medfører at spørsmål knyttet til ansvarsforhold ved utkontraktering må drøftes også for bruk av skytjenester. Regler om utkontraktering følger direkte av regelverk.

[6] Nærmere omtalt i neste kapittel

3.3 Jurisdiksjon i skyen

Jurisdiksjonsspørsmål er som nevnt spesielt relevant for diskusjonen om skytjenester. Saklig og stedlig jurisdiksjon kan noen ganger avklares gjennom kontraktsvilkår, andre ganger vil lovgivningen vedrørende de berørte data være preseptorisk, ufravikelig. Det er særlig spørsmål om stedlig domsmyndighet som reiser uklarheter ved bruk av skytjenester.

Som et utgangspunkt kan det legges til grunn at bruk av skytjenester innebærer at dataene krysser landegrenser, og som regel lagres i flere land - ofte på en og samme tid. Noe regelverk tar utgangspunkt i hvor data befinner seg, mens annet regelverk vil kunne forholde seg til landet hvor leverandøren er etablert/har sitt hovedkontor eller brukerens bosted for å avgjøre jurisdiksjonen over dataene. Praksisen rundt dette er ulik også mellom land, og det foreligger ingen folkerettslig avtale som besvarer alle slike spørsmål. Det påpekes i en utredning fra Nordisk ministerråd at den fragmenterte lovgivningen, og en manglende åpenhet internasjonalt om regelverk som kan komme til anvendelse, er en risikofaktor ved behandlingen av data i skytjenester som det bør tas hensyn til.[7]

Noen ganger vil begrensingene som finnes i regelverket knyttet til geografi og lokalisering av data kunne ha sitt utgangspunkt i at det er viktig å sikre norske myndigheters tilgang til dataene, andre ganger handler det om å sikre at dataene behandles i tråd med norsk regelverk. En annen begrunnelse kan være at andre nasjoners myndigheter ikke skal kunne få tilgang til dataene. Også andre begrunnelser kan anføres.

Selv om utgangspunktet er at data krysser landegrenser ved plassering i en skytjeneste, finnes det flere skytjenester hvor man kan velge lagring innenfor spesifikke områder, for eksempel at kun servere innenfor EØS-land skal benyttes, eller om dataene kun beveger seg mellom servere innen ett enkelt land. Dette gjør det relevant å skille mellom regelverk som kun tillater lagring eller behandling av data innen et bestemt område og regelverk som ikke oppstiller lokasjonskrav i spørsmålet om hindringer for bruk av skytjenester.

Et annet utgangspunkt er at det foreligger norsk jurisdiksjon over materialet der informasjon behandles innen Norges grenser. Dersom serverne dataene behandles på befinner seg i Norge, er det ingen tvil om at dataene befinner seg i Norge.

Det finnes likevel en særproblemstilling rundt enkelte myndigheters tilgang også utenfor egne, nasjonale grenser. Skyleverandører kan være underlagt nasjonale regler fra andre land hvor de har virksomhet. En usikkerhet oppstår derfor også for servere plassert innen norsk jurisdiksjon, dersom selskapet som eier serverne også har virksomhet utenfor Norge.

[7] Nordisk Ministerråd (2013): *Legal guide to public cloud sourcing*

Flere land har lovverk som antagelig gir myndighetene rett til å få tilgang til for eksempel personopplysninger i nasjonale selskapers systemer, også dersom behandlingen av personopplysninger foregår utenfor det aktuelle landet. USA har for eksempel slike regler, blant annet gjennom regelverket USA Patriot Act[8], men antagelig også gjennom andre hjemler i amerikansk rett. Vi har sett et konkret eksempel på dette i en rettssak mellom amerikanske myndigheter og Microsoft. Myndighetene krevde tilgang til kundedata (e-post) lagret hos Microsoft i Irland, blant annet begrunnet med at Microsoft i USA også kunne aksessere disse dataene. Dommen er ikke rettskraftig per mars 2015, da Microsoft har anket den til en høyere rettsinstans.[9] Dersom utkommet av konflikten blir at amerikanske myndigheter kan kreve å få utlevert data fra Microsoft i USA, uavhengig av hvor dataene geografisk er plassert, og slik omgå internasjonale avtaler om utlevering av denne type data, vil dette kunne få konsekvenser for bruken av skytjenester i Europa. For behandlingen av personopplysninger vil det da oppstå en situasjon hvor det ikke er tilstrekkelig at skyleverandører tilbyr tjenester som garanterer behandling innenfor EØS-området, og dermed innenfor jurisdiksjonen til land som er underlagt EUs personverndirektiv.

Et annet spørsmål om jurisdiksjon med relevans for skytjenester, er hvorvidt det å flytte data mellom servere plassert i ulike stater tilsvarer å overføre data til en annen stat, altså om dataene har skiftet jurisdiksjon. For eksempel vil en kunne reise spørsmålet om det å "*føre noe ut av landet*"[10] også gjelder der det bare er tale om midlertidige og kortvarige bevegelser. Svaret på dette vil avhenge av tolkningen av det aktuelle regelverket, og i enkelte tilfeller også av regelverk i det landet data midlertidig befinner seg i. Utfordringen er at regelverket ofte ikke adresserer slike spørsmål, slik at det i siste instans kan bli opp til domstolene i siste instans å vurdere slike forhold.

Vi vil ikke drøfte disse og andre jurisdiksjonsspørsmål mer inngående i rapporten, men geografiske føringer i regelverk drøftes konkret der det er relevant.

[8] US Department of Justice. *The USA Patriot Act: Preserving Life and Liberty. http://www.justice.gov/archive/ll/highlights.htm*

[9] Microsoft Corporation (2015): *In the Matter of a Warrant to Search a Certain E-mail Account.* Brief for apellant http://digitalconstitution.com/wp-content/uploads/2014/09/Microsoft-Opening-Brief-12082014.pdf

[10] Jf. arkivlovens § 9 b.

4. Kartlegginger internasjonalt

Det er utført både enkelte juridiske, tekniske og sikkerhetsmessige kartlegginger og vurderinger av skytjenester tidligere, både innen Norge og innen land vi kan sammenligne vår lovgivning med. Flere land har utarbeidet strategier for bruk av skytjenester eller gjennomført juridiske utredninger, og det er relevant å se på noen utvalgte tilnærminger til spørsmålene vi stiller i denne rapporten.

4.1 En felles nordisk utredning

Nordisk Ministerråd, i samarbeid med de nordiske myndigheter, utarbeidet i 2013 en juridisk veileder for bruk av skytjenester for nordiske, offentlige virksomheter.[11] Veilederen tar utgangspunkt i behandlingen av personopplysninger, og den rettslige rammen for veilederen er EUs personverndirektiv[12] og de nordiske, nasjonale regelverkene om behandling av personopplysninger. Rapportens anbefalinger om bruk av skytjenester må derfor forstås i lys av ett bestemt sett regelverk, og kravene som følger av dette. Likevel kan veilederen også gi nyttige råd om behandlingen av andre data enn personopplysninger, både der det er relevant å trekke tilsvarende slutninger og som generelt gode råd ved overgangen til en skytjeneste. Arbeidsgruppen vil derfor supplere veilederens råd med noen generelle betraktninger, på tvers av regelverket.

Veilederen skisserer fire elementer en må ta hensyn til ved bruk av skytjenester:

1. Oversikt *over relevant, gjeldende lovgivning, herunder jurisdiksjonsspørsmål*. I veilederen henvises det til å avgjøre hva som er relevant personvernlovgivning, men dette er et råd som vil gjelde generelt. Regelverket kan sette ulike skranker for behandlingen av data, og en virksomhet bør redegjøre for hvilken lovgivning som kommer til anvendelse for de dataene en behandler, i tillegg til å avklare stedlig jurisdiksjon.

2. *Klarhet i ansvarsforholdet for dataene*. Selv om det benyttes en skytjeneste vil ansvaret for dataene fortsatt ligge hos virksomheten. Det er derfor viktig å klargjøre om skyleverandøren behandler dataene på en tilfredsstillende måte, for slik å ivareta det ansvaret virksomheten selv sitter med.

3. *Risikoanalyse*. En virksomhet som ønsker å ta i bruk en skytjeneste bør, som et første skritt, gjennomføre en grundig risikoanalyse. En risikoanalyse skal alltid foretas, uavhengig av om en tar i bruk en skytjeneste, setter IKT-drift ut lokalt eller utvikler og drifter IKT internt i virksomheten. Konfidensialitet, tilgjengelighet og integritet for dataene vil være avgjørende vurderingsmomenter. Disse prinsippene kan slå ut ulikt for ulike data. Derfor kan det være aktuelt å differensiere mellom dataene, på bakgrunn av disse momentene, for å foreta en vurdering av om en skytjeneste er egnet for de enkelte dataene virksomheten behandler.

[11] Nordisk Ministerråd (2013). *Legal guide to public cloud sourcing*
[12] Direktiv 95/46/EF om personvern

4. *Kontraktsvurdering*. Det er viktig og nødvendig å ha god kjennskap til innholdet i avtalen som inngås med skyleverandøren. I avtalen må det for eksempel fremkomme tilfredsstillende vilkår for behandling på grunnlag av aktuelt regelverk, akseptable vilkår for virksomheten knyttet til at ansvaret ikke kan overdras og sikkerhetsaspektet må ivaretas. For skytjenester inngår man gjerne standardkontrakter leverandøren bruker for alle sine kunder. Slike kontrakter må vurderes særskilt for å sikre at de ivaretar alle de nødvendige forhold og at relevant, gjeldende regelverk tas i betraktning.

4.2 EU – Cloud for Europe

Gjennom EUs 7. rammeprogram for forskning har EU-kommisjonen finansiert et omfattende prosjekt for å støtte offentlig sektors bruk av skytjenester. Målet med skyprosjektet er å identifisere hindringer, finne innovative løsninger og bygge tillitt til bruk av skytjenester i offentlig sektor i Europa.[13] Et viktig virkemiddel for dette er å stimulere europeisk næringsliv til å utvikle innovative skyløsninger rettet mot offentlig sektor gjennom innovative anskaffelser (PCP - pre commercial procurement). Prosjektet har innledningsvis kartlagt juridiske hindringer og utarbeidet en oversikt over juridiske krav og utfordringer en offentlig virksomhet i EU møter ved implementering av skytjenester i offentlig sektor.[14] De juridiske utfordringene deles inn i to kategorier: den første omfatter generelle utfordringer som påligger de fleste skytjenester, slik som jurisdiksjonsspørsmål, personvern, kontraktsrett, forbrukerrett og myndighetstilgang (tilsyn, kriminalitetsbekjempelse og lignende). Den andre omfatter spesifikk lovgivning for offentlig sektor, som anskaffelsesproblematikk, språkkrav, arkivlovgivning, nasjonal sikkerhet, finanslovgivning og sivil- og straffeprosess.

Kartleggingen foretatt av Cloud for Europe går bredere til verks enn denne rapporten, men er også mer overfladisk. Det europeiske perspektivet må ta utgangspunkt i bredden innen nasjonalt regelverk, og det er ikke foretatt omfattende henvisninger til konkrete, nasjonale skranker. Hensikten kan sies å først og fremst være å lage en veileder for nasjonal rett, hvor det påpekes generelle usikkerheter i regelverk, og vises til hvor det særlig er behov for veiledning. Kartleggingen sier således lite hva som er de konkrete hindringene, men mer om hvilke type hindringer som kan finnes i EU-rett og i nasjonal rett i det enkelte medlemsland. Enkelte av konklusjonene er likevel interessante også for vår rapport. Uklarheter i lovgivning nevnes som en typisk hindring i den europeiske kartleggingen. Videre vises det til at det finnes en del lovgivning som totalt avviser bruk av skytjenester, og dermed oppstiller absolutte hindringer. Det nevnes også som en utfordring konkrete krav som stilles i enkelte regelverk, for eksempel til sikkerhet, geografiske føringer og andre, generelle kontraktsvilkår.

[13] Cloud for Europe nettsider: http://www.cloudforeurope.eu/
[14] Cloud for Europe (2015): *D 2.1 Legal implications on cloud computing*

Cloud for Europe sin juridiske kartlegging er et godt verktøy for å få oversikt over utfordringer i regelverk på tvers i Europa, men den må, i likhet med Nordisk råd sin utredning, suppleres med nasjonale gjennomganger av regelverk for å avklare faktiske hindringer.

4.3 Danmark

Danmark nedsatte i 2012 en arbeidsgruppe som har skrevet en rapport "*om love og regler der unødigt vanskeliggør anvendelsen af cloud computing*".[15] Bakgrunnen er den tverroffentlige digitaliseringsstrategien i Danmark hvor det i 2011 ble besluttet å iverksette et initiativ om "tidssvarende regler for cloud computing", altså en modernisering av regelverk for å gjøre det lettere å ta i bruk skytjenester. Arbeidsgruppen gjennomgikk dansk regelverk for å avdekke barrierer for bruk av skytjenester, med målsetting om å justere regelverk som unødig er til hinder. Det henvises blant annet til den danske regjeringens ønske om å "*fastholde beskyttelsen af borgernes og virksomhedernes følsomme oplysninger uden, at der sættes unødige barrierer for anvendelsen af cloud-teknologi, som kan give besparelser for dataansvarlige myndigheder og give en mere fleksibel service for borgere og virksomheder*."

En interessant avklaring som gjøres i den danske rapporten gjelder den danske bokføringsloven og regnskapsloven, som ligner mye på tilsvarende regelverk i Norge. Disse lovene anses ikke som hinder for bruk av skytjenester, selv om de i utgangspunktet fremholder oppbevaring av bokførings- og regnskapsmateriale innen Danmark eller Norden som hovedregel. Bakgrunnen er at det ikke er noe hinder for å behandle og oppbevare regnskapsmateriale i utlandet såfremt det tas en kopi, enten fysisk eller digital, hver måned, og denne kopien lagres på en server eller på papir i Danmark.

For øvrig omhandler større deler av rapporten nasjonale tilpasninger Danmark har inntatt i sin personvernlovgivning, i tillegg til EUs personverndirektiv. Det foreslås en rekke endringer i de delene av den danske personvernlovgivningen som ikke følger direkte av direktivet.

[15] Digitaliseringsstyrelsen (2012): *Notat om love og regler der vankeliggør cloud computing*

5. Kartleggingen av lover og forskrifter innen sektorene

5.1 Kulturdepartementet

Etter gjennomgang av regelverk som Kulturdepartementet har ansvar for, er det kun arkivloven med forskrifter som er identifisert som en hindring for bruk av skytjenester innen departementets ansvarsområde.

Arkivloven med forskrifter
Alle offentlige organ er underlagt en plikt til å ha arkiv.[16] Fordi arkivloven inneholder en begrensning på å føre arkiv ut av landet, er denne bestemmelsen en hindring for offentlige virksomheter som ønsker å ta i bruk skyløsninger med utenlandske servere.

Arkivloven ble vedtatt i 1992. Behandling i skyen av offentlige organers arkiver er ikke eksplisitt regulert i arkivloven og heller ikke omtalt i forarbeidene. Samtidig er loven generelt utformet, og den gjenspeiler i stor grad overordnede prinsipper som vil gjøre seg gjeldende både for papir og digitalt materiale.

Formål
Begrensningene som foreligger på lagring av arkivmateriale i skyløsninger med utenlandske servere kan særlig forstås på grunnlag av formålsbestemmelsen, § 1 i arkivloven. Også § 6 som presiserer arkivansvaret kan trekkes frem. Formålet med loven er å sikre at arkiv som inneholder forvaltningsmessig dokumentasjon eller rettighetsinformasjon blir tatt vare på og gjort tilgjengelig for ettertiden. Grunnene til at vi skal trygge offentlige organers arkiver er mange. Arkivmateriale skal behandles slik at vi ivaretar hensynet til personvern, partsrettigheter, organets styring av egen virksomhet, tilsyns- og kontrollmyndigheters styring, folkevalgt kontroll, offentlig innsyn, forskning og sikring av kulturelle verdier. Arkivene skal gi trygg tilgjengelighet til offentlige dokumenter når dokumentene er i aktiv bruk i forvaltningen og for fremtiden. Dette er kommet til uttrykk i lovens forarbeider: "*Arkivet skal vera innretta på ein slik måte at det ikkje berre dekkjer det kortsiktige forvaltningsmessige behovet som organet måtte ha for sitt eige arkivtilfang, men at det dessutan tryggjer det langsiktige, samfunnsmessige behovet for å ta vare på viktig dokumentasjon*." [17]

Etter arkivloven plikter offentlige organ å ha arkiv, og organet har selv ansvar for at arkivmaterialet er sikret slik at det er tilgjengelig både i dag og i fremtiden. Dette presiseres i § 6, som sier at materialet må være "*tryggja som informasjonskjelder for samtid og ettertid*". "*Å tryggja*" arkiv betyr først og fremst at arkivmaterialet skal være sikret mot å gå tapt, og reglene presiseres noe i forskrift til loven. I forskrift om offentlige arkiv § 2-9 presiseres at det for elektronisk journalføring skal benyttes "*eit arkivsystem som følgjer krava i Noark-standarden.*" Det fastslås videre i § 2-13 at "*saksdokument i offentlege arkiv kan lagrast elektronisk. Ein føresetnad for slik lagring er at det blir nytta fullgode system, rutinar, dokumentlagringsformat og lagringsmedium som*

[16] Med unntak av Stortingsorganer, jf. arkivloven § 5.
[17] Ot.prp.nr.77 (1991-1992) *Om lov om arkiv* s. 23.

er godkjende av Riksarkivaren gjennom generelle føresegner eller enkeltvedtak."
Bakgrunnen for reglene følger av at arkivmaterialet må bevare sin bevisverdi, opprettholde integritet og autentiset. I tillegg må arkivet være innrettet slik at krav til konfidensialitet[18] blir ivaretatt. Dette gjelder typisk taushetsbelagte opplysninger om noens personlige forhold og bedriftshemmeligheter, men også opplysninger om forvaltningens interne forhold som kan unntas fra offentlighet.[19]

Arkivloven § 1 og § 6 må forstås slik at offentlige organer må foreta en risikovurdering av lagringssystemene som skal benyttes, og en vurdering av om arkivplikten ivaretas i valgte løsning.

Utførselsforbud
I § 9 bokstav b i arkivloven er følgende fastslått: "*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*". Å lagre arkivmateriale fra offentlig virksomhet på utenlandske servere tolkes slik at det faller inn under lovtekstens ordlyd om å "føre arkiv ut av landet". Lagring av arkivmateriale fra offentlig virksomhet i en skyløsning med serverne plassert utenfor Norge vil stride mot denne bestemmelsen i arkivloven. Utførselsforbudet i arkivloven er derfor en hindring for bruk av skytjenester, med mindre serverne befinner seg i Norge.

I forarbeidene til arkivloven, jf. Ot.prp. nr. 77 (1991-92), er det gitt noen eksempler på hva som faller inn under unntaket "*naudsynt del av den forvaltningsmessige eller rettslege bruken av dokumenta*". Utførselsforbudet er ikke til hinder for at for eksempel Utenriksdepartementet kan ta arkivmateriale ut av landet som en del av den ordinære kommunikasjonen med utenriksstasjonene og ved internasjonale møter. Utførselsforbudet er heller ikke til hinder for at arkivdokumenter fra offentlige virksomheter krysser riksgrensen i forbindelse med samrådninger med kommuner i naboland, eller når dokumenter skal legges fram i en rettssak i andre land. Lovens forarbeider gir imidlertid liten veiledning utover det som er referert ovenfor i vurderingene som kan sies å være "*naudsynt*". Det er likevel arbeidsgruppens forståelse at bruken av en skytjeneste ikke vil kunne falle innunder dette unntaket.

Utførselsforbudet har ikke en grundig begrunnelse i lovens forarbeider og de gir få holdepunkter for å tolke bestemmelsene sett i lys av dagens teknologi. Igjen er det hensynene bak loven som må være førende for lovens tolkning for dagens situasjon, da forarbeidene er eldre, ikke utformet med tanke på IKT-systemer, og dermed naturlig nok ikke omtaler lignende situasjoner.

---

[18] Kryptering kan sikre konfidensialitet for arkivmaterialet. Samtidig kan kryptering vanskeliggjøre tilgjengelighet til dokumentasjonen. Arkivmaterialet skal være tilgjengelig både i samtid og ettertid, og kryptering kan skape store problemer for tilgjengelighet på sikt.

[19] Et perspektiv som videre kan drøftes er andre myndigheters mulige tilgang på arkivmateriale dersom dataene befinner seg på en server i utlandet. Dette er særlig aktuelt der serveren driftes av et utenlandsk selskap der myndighetene har hjemmel for å ta beslag, slik for eksempel USA hevder de har gjennom Patriot Act.

I arkivloven § 9 er det i første setning vist til mulig unntak i medhold av forskriftskompetanse i lovens § 12, og etter særskilt samtykke fra Riksarkivaren.

Arkivloven § 12 hjemler Kongens mulighet til å fastsette forskrift om dette spørsmålet, men slike presiseringer eller avgrensninger av utførselsforbudet er ikke gitt. Vedrørende muligheten for Riksarkivaren til å gi særskilt samtykke har ingen hittil søkt om dette for bruk av skyløsninger med servere i utlandet.

Arbeidsgruppen mener at det bør drøftes behov for endring av forskrift om offentlige arkiv, for å tillate lagring av arkiver fra offentlige virksomheter i skyløsninger med servere i utlandet. I tillegg bør det vurderes å klargjøre hva som skal til for at Riksarkivaren kan gi slikt særskilt samtykke. Arbeidsgruppen er kjent med at det antagelig vil komme søknader om dette fra offentlige organer som ønsker å kunne ta i bruk skytjenester for sin dokumentbehandling.

Tilsyn med arkivmateriale
Riksarkivaren har tilsynsansvar for arkivarbeidet for offentlige organ, jf. arkivloven § 7, og praktiserer såkalt stedlig tilsyn med fysiske besøk. Praktiseringen av det stedlige tilsynet oppstiller en hindring for bruk av skytjenester. Riksarkivaren kan "*krevja seg førelagt for godkjenning journalsystem, arkivnøklar, arkivinstruksar m.m.*" og har rett til å "*inspisera arkiv*". Hva som skal til for at arkivmateriale er å anse som "*førelagt*", altså at dette er tilgjengeliggjort for tilsynsmyndigheten, følger ikke av lovteksten. Heller ikke kravene til det å "*inspisere*" følger av lovteksten. Det kan argumenteres for at tilgjengelighet, tilgang, kan sikres ved at materialet, eller en identisk kopi av dette, befinner seg i Norge, eller at systemet befinner seg i Norge. Retten til å inspisere arkivsystemet vil likevel ikke nødvendigvis avhjelpes ved å ha en identisk kopi av selve materialet innen Norge, og er et spørsmål som bør avklares.

Dagens utførselsforbud i § 9 sikrer norsk jurisdiksjon over dataene. Tilsynsmyndighetene er dermed sikret juridisk tilgang til arkivmaterialet etter norsk regelverk, og det er norsk regelverk som styrer hvem som ellers skal ha tilgang til materialet.

Tilgang til arkivmateriale og tilhørende dokumentasjon kan også sikres på andre måter enn gjennom fysisk tilgang i Norge. Det er derfor relevant å vurdere om arkivverkets tilsynsmyndighet kan innrettes slik at den kan håndtere bruk av skytjenester. Spørsmålet om hvorvidt tilsynsmyndighetens behov for tilgang gir tilstrekkelig begrunnelse for opprettholdelse av utførselsforbudet bør vurderes av lovgiver. Tilsynet med arkivdanningen vil uansett kunne skje hos/overfor arkivskaper selv, da skylagringen i seg selv ikke reiser særegne problemstillinger. Det kan stilles spørsmål om tilsynet skal være systembasert, eller om det skal gjennomføres stedlig tilsyn, og i så fall hvilke behov et stedlig tilsyn dekker. Må for eksempel Arkivverket ha tilgang til alle serverne som inngår i skylagringen? Kan tilsyn gjennomføres dersom det ikke er kjent nøyaktig hvor dokumentene befinner seg? For å sikre at Arkivverket kan drive

tilsyn overfor leverandører og underleverandører, kan det være nødvendig at hjemmelen klargjøres i loven.

Til sammenligning fører Datatilsynet tilsyn med behandlingsansvarlige, blant annet for å kontrollere at denne har gjennomført tilstrekkelige sikringstiltak i samsvar med personopplysningsloven § 13. I forbindelse med tilsyn hos behandlingsansvarlig kan Datatilsynet godta dokumentasjon fra tredjepart som bekrefter lovoppfyllelse. Dette kalles ofte tredjepartsrevisjon (revisjon utført av en uavhengig tredjepart). I praksis er det også denne typen kontroll skytjenesteleverandørene åpner for, da det er både enklere, og gir større sikkerhet for kundene, enn om en rekke tilsynsmyndigheter fra ulike land skulle få tilgang til systemene.

Arkivmaterialet må for øvrig også være tilgjengelig for organet selv, for folkevalgtes kontroll, allmennhetens innsyn mv. Slik tilgjengelighet vil ikke være en utfordring ved bruk av et alminnelig dokumentbehandlingssystem, uavhengig av leveransemodell.

Arkivansvar
Arkivlovens system bygger på at arkivansvaret enten ligger hos arkivskaper, jf. arkivloven § 6, eller hos Arkivverket, jf. arkivloven § 10. Det overordnede arkivansvaret er etter arkivforskriften § 1-1 lagt til den øverste ledelsen i organet. Oppgaver og myndighet kan delegeres, men ikke ansvaret. Utkontraktering av virksomhetsoppgaver, og bruk av skytjenester til behandling og lagring av data er to rettslig sett ulike forhold. Noen trekk ved skytjenester medfører likevel at spørsmål knyttet til ansvarsforhold ved utkontraktering kan drøftes også for skytjenester; da en tredjepart får en rolle i behandlingen av dataene også her.

Utkontraktering av oppgaver innen arkivsektoren kan bare utføres på en slik måte at den arkivansvarlige faktisk er i stand til å ivareta ansvaret. I dette ligger det blant annet at den ansvarlige må ha rett til informasjon om utførelsen av oppgaven, mulighet til å kontrollere, samt mulighet til å trekke seg fra avtalen og gi oppdraget til andre. Det er viktig at arkivansvaret bevares gjennom gode kontrakter med skyleverandøren, og på dette området er det antagelig behov for bedre veiledning. En gjennomgang av avtalevilkår i avtaler mellom 10 skytjenesteleverandører i Nord-Amerika og Europa og deres klienter viser i følge Robert McLelland at kontrakter først og fremst beskytter interessene til tjenesteleverandører, og en slutning som kan gjøres er at disse vil komme til kort mht. å sikre behovene for arkivdanning som kundene til tjenesteleverandørene har.[20] Denne utfordringen gjenfinnes i IKT-forskriften for bank- og finanssektoren.

Konklusjon:
Arkivloven er et hinder for bruk av skytjenester til lagring av materiale utenfor Norge. Lagring av arkivmateriale i en skytjeneste med serverne plassert utenfor Norge strider

[20] McLelland, Robert, Yvette Hackett, Grant Hurley, Daniel Collins (2014). *Agreements between Cloud Service Providers and their Clients: A Review of Contract Terms*

mot arkivloven § 9 bokstav b. I tillegg er tilsynet slik det praktiseres i dag gjennom stedlig kontroll et hinder.

Tiltak:
Kongen har myndighet til å gi utfyllende bestemmelser som kan tillate utførsel av arkivmateriale fra offentlig virksomhet til utenlandske servere, jf. arkivloven § 12, og Riksarkivaren kan også gi særskilt samtykke til utførsel. Dette bør vurderes som aktuelle løsninger innen lovens rammer.

Arbeidsgruppen anbefaler at det også foretas en vurdering av om arkivloven § 9 b bør revideres.

Det bør undersøkes om tredjepartsrevisjon, dokumentasjon innhentet av en tredjepart, vil kunne ivareta Riksarkivarens ansvar for tilsyn og kontroll med offentlige organers arkiver.

Arkivverket prøver ut alternative løsninger for overføring av digitale dokumenter løpende fra virksomhetenes egne dagligarkiv til et sentralt mellomlager (eArkiv). En slik komponent vil kunne fungere sammen med en skytjeneste. Ved bruk av en skytjeneste for saksbehandling eller andre tjenester som produserer journalføringspliktige og arkivpliktige saksdokumenter, vil man da kunne sikre at selve arkiveringen likevel skjer i Norge i henhold til arkivloven § 9 bokstav b.

5.2 Kunnskapsdepartementet

En gjennomgang av det regelverket som forvaltes av Kunnskapsdepartementet har ikke avdekket hindringer for bruk av skytjenester. Som følge av eRegelprosjektet[21] er regelverket i Kunnskapsdepartementet i dag i all hovedsak teknologinøytralt. De lovene som er gjennomgått av arbeidsgruppen er: Barnehageloven, fagskoleloven, folkehøyskoleloven, forskningsetikkloven, voksenopplæringsloven, utdanningsstøtteloven, opplæringsloven, privatskoleloven, studentsamskipnadsloven, og universitets- og høyskoleloven.

Barnehageloven
Barnehageloven har imidlertid regler om innsyn og tilsyn som kan være egnet til å skape usikkerhet, og vil derfor presiseres her. I henhold til barnehagelovens § 8 og § 9 har kommunen og fylkesmannen rett til innsyn i dokumenter og adgang til lokaler. Dette medfører ingen hindring for bruk av skytjenester, da retten til tilsyn ikke kan forstås som at det foreligger noe krav om stedlig tilsyn av behandlingen av data. I likhet med andre innsynsregler kan heller ikke tilgangen til dokumenter utgjøre noen utfordring, da innsyn enkelt vil kunne sikres gjennom systemgrensesnittet, også ved bruk av skytjenester.

[21] Se Ot.prp. nr. 108 (2000-2001) og Ot.prp. nr. 9 (2001-2002)

Konklusjon:
Det er ingen klare hindringer for bruk av skytjenester i lovene som Kunnskapsdepartementet har ansvar for.

5.3 Samferdselsdepartementet

En gjennomgang av regelverk underlagt Samferdselsdepartementet har ikke avdekket noen klare hindringer for å kunne ta i bruk skytjenester. I likhet med andre sektorer eksisterer det imidlertid mer generelle krav til flere ulike typer av registre og systemer. Slike krav knytter seg til hvilke opplysninger som skal registreres og utveksles, og eventuelt hvilke format disse skal ha. Det er ingen krav til hvordan eller hvor data skal lagres. Utover de alminnelige krav til behandling av personopplysninger i tråd med personopplysningsloven, har ikke Samferdselsdepartementet identifisert hindringer for etablering av skytjenester.

Lov om edb-baserte reservasjonssystemer for passasjertransport m.v.
Et mulig unntak fra ovennevnte kan være *Lov om edb–baserte reservasjonssystemer for passasjertransport m.v. av 23. juni 2000, nr. 54*, som implementerer EUs Rådsforordning 2299/89. I artikkel 6 nr. 1 bokstav a) kreves det at: "*opplysninger som systemleverandøren innehar med hensyn til identifiserbare enkeltbestillinger, skal lagres frakoplet innen 72 timer etter at det siste element i enkeltbestillingen er ferdigbehandlet, og skal tilintetgjøres innen tre år. Det skal gis tilgang til slike opplysninger bare i tilfeller av tvist om fakturering.*"

Det er vanskelig å si sikkert hvor stor praktisk betydning denne konkrete bestemmelsen i EU-forordningen har for bruk av skytjenester, men den er sannsynligvis ikke stor. Denne regelen oppstiller krav om at data skal lagres frakoblet – det vil si analogt eller i et system som ikke er koblet til et eksternt nett – etter en viss tid, og hindrer således ikke bruk av skytjenester særskilt. Etter hva Samferdselsdepartementet kjenner til, har det så langt ikke vært grunn til å håndheve denne bestemmelsen fra myndighetens side.

Konklusjon:
Det er ingen klare hindringer for bruk av skytjenester i lovene som Samferdselsdepartementet har ansvar for.

5.4 Finansdepartementet

Arbeidsgruppen har hatt deltakelse fra skattelovavdelingen, og vært i dialog med finansmarkedsavdelingen i Finansdepartementet. Etter en gjennomgang av regelverk underlagt disse avdelinger har arbeidsgruppen funnet at ved behandlingen av finansielle data må en være bevisst på flere forhold ved bruk av skytjenester.

Virksomheter som behandler slike data, eller er underlagt sektorspesifikke krav, må være særlig oppmerksomme på:

- regelverk som setter klare geografiske føringer for lagring eller databehandling
- regelverk som setter krav til såkalt "stedlig tilsyn"

Bokføringsloven med forskrifter

Bokføringsloven har tidligere vært ansett som en av de lovene som oppstiller de største hindre for digitale prosesser. Med den relativt nylige revisjonen av bokføringsloven kan nå det aller meste av regnskapsmateriale oppbevares digitalt, og det er bedre lagt til rette for digitalisering av også de prosesser som berører regnskapsmateriale.

Bokføringsloven § 13 stiller krav om oppbevaring av regnskapsmateriale, og etter 2. ledd følger det at regnskapsmateriale som hovedregel skal oppbevares i Norge. Etter 5.ledd kan det i forskrift gjøres unntak fra bestemmelsene om oppbevaring. Etter bokføringsforskriften § 7-5 kan bokføringspliktige "*oppbevare elektronisk regnskapsmateriale i et annet EØS-land dersom avtale eller overenskomst med det aktuelle landet sikrer norske skatte- og avgiftsmyndigheter tilfredsstillende adgang til regnskapsinformasjonen for kontrollformål i oppbevaringstiden, og slik oppbevaring ikke vil være til hinder for effektiv norsk politietterforskning.*" De må videre "*skriftlig informere Skattedirektoratet om hvilket regnskapsmateriale som oppbevares i utlandet, hvor regnskapsmaterialet oppbevares, og hvordan kontrollmyndighetene til enhver tid kan få adgang til regnskapsmaterialet*". Det følger imidlertid av forskrift om oppbevaring av elektronisk regnskapsmateriale i andre EØS-land § 1 at kun de nordiske land p.t. oppfyller disse kravene.

Hovedregelen for elektronisk regnskapsmateriale blir dermed at dataene må være tilgjengelig på en server i Norge. Elektronisk oppbevaring vil også kunne foretas innen Norden når det er sendt melding til Skattedirektoratet om dette.

Bokføringspliktige kan også søke om dispensasjon for å oppbevare bokføringsdata på servere i utlandet etter § 13 siste ledd i bokføringsloven. Slike dispensasjoner innvilges regelmessig når oppbevaringen i utlandet skjer som ledd i en felles regnskapsløsning innen et konsern eller lignende sammenslutning, og lagringen skjer hos et konsernselskap eller lignende i utlandet eller under kontroll av et slikt selskap. Det settes som vilkår at det skal være elektronisk tilgang til regnskapsopplysningene fra Norge. Skattedirektoratet uttaler selv at ikke "*kostnadsbesparelser ved utenlandsk oppbevaring gir noe selvstendig grunnlag for dispensasjon. I de tilfeller hvor dispensasjon hittil er innvilget, er det lagt avgjørende vekt på om oppbevaringen i utlandet skjer som ledd i en felles regnskapsløsning innen et konsern eller lignende sammenslutning, og at lagringen skjer hos et konsernselskap eller lignende i utlandet eller under kontroll av et slikt selskap. Det er også lagt vekt på om lagringen skjer i et land som har skatteavtale med Norge. Det er videre stilt krav om at regnskapsmateriale som lagres i utlandet skal være tilgjengelig i lesbar form i Norge og at det skal kunne skrives ut på papir i hele*

oppbevaringsperioden fra terminal eller lignende i Norge. Det er videre en forutsetning at kontrollmyndighetene ikke hindres adgang til regnskapsmaterialet."[22]

At regnskapsmateriale må oppbevares innen Norge eller i de øvrige land i Norden vil være et klart hinder for bruk av skytjenester. Det er en forskjell på om hensikten bak begrensningen er å hindre data i å bli sendt ut av landet, eller å sikre at data er tilgjengelig i Norge. I det siste tilfellet kan det være interessant å vurdere hvorvidt slik tilgjengelighet tilsier at dataene faktisk må være fysisk lagret i Norge (eller annet område som er spesifisert i loven).

Begrunnelsen for lovens begrensinger er særlig knyttet til tilgjengelighet, ved at norske skatte- og avgiftsmyndigheter må være sikret tilfredsstillende adgang til regnskapsinformasjonen for kontrollformål. Bokføringsloven med forskrifter er likevel ikke til hinder for at data kan føres ut av landet i forbindelse med regnskapsføringen i utlandet. Det følger av bokføringsforskriften § 7-4 første ledd at regnskapsmaterialet da skal overføres til Norge innen en måned etter regnskapsårets slutt, og senest innen syv måneder etter regnskapsårets slutt. Virksomheter som ønsker å lovlig benytte skytjenester for behandling av bokføringsdata, kan slik tilfredsstille det norske regelverket gjennom å lagre en kopi av de dataene bokføringsloven krever i Norge. Dette er den samme løsning som er vurdert av gruppen som har sett på juridiske hindringer for bruk av skytjenester i Danmark, se kapittel 4.3. Arbeidsgruppen anser dette spørsmålet som delvis uavklart.

Finanstilsynsloven med tilhørende forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT) i bankvirksomhet (IKT-forskriften)
IKT-forskriften, som gjelder bruk av IKT innen bank- og finanssektoren, er særlig aktuell for virksomheter som behandler finansielle data og ønsker å benytte skytjenester. Forskriften omfatter IKT-systemer som er av betydning for foretakets virksomhet, og for eksterne brukere av foretakets IKT-systemer skal det foreligge avtaler som sikrer at forskriftens krav til sikkerhet og dokumentasjon ivaretas, jf. § 1.

Utkontraktering
Etter IKT-forskriften skal ethvert foretak som bedriver finansvirksomhet etterleve en rekke krav knyttet til sikker drift av IKT-virksomheten, jf. § 12, 1.ledd. I forskriften finner en blant annet kunnskapskrav om forhold som katastrofetest, årlig risikovurdering av leveransen, krav til endringshåndtering og hendelsesrapportering, samt tilgang til all informasjon om virksomhetens IKT-drift.

Dette gjelder også der hele eller deler av IKT-virksomheten er utkontraktert. Utkontraktering av virksomhetsoppgaver, og bruk av skytjenester til behandling og lagring av data er to ulike forhold. Men også ved bruk av skytjenester vil en tredjepart få en rolle ved behandlingen av data, og dette er således et trekk ved skytjenester som medfører at spørsmål knyttet til ansvarsforhold ved utkontraktering er relevant også

[22] Skattedirektoratet. URL: http://www.skatteetaten.no/en3/Radgiver/Rettskilder/Kunngjoringer/Dispensasjon-fra-enkelte-bestemmelser-i-bokforingsloven-og-bokforingsforskriften/

ved bruk av skytjenester. Ved å utkontraktere IKT-virksomheten stilles en del krav som må være oppfylt for at avtalen skal godkjennes av Finanstilsynet. Dersom kontrakten ikke utarbeides på tilfredsstillende måte etter forskriften, medfører det en hindring for bruk av IKT-systemene.

Tilsyn
Det følger av forskriften § 12, første og annet ledd, at avtalen for det første må sikre at foretaket selv under tilsyn "*gis rett til å inspisere og kontrollere de av leverandørens aktiviteter som er knyttet til avtalen*". Videre skal avtalen også "*sikre håndtering av taushetsbelagt informasjon*". For det tredje skal avtalen sikre at Finanstilsynet "*gis tilgang til opplysninger fra og tilsyn hos IKT-leverandøren der Finanstilsynet finner det nødvendig som et ledd i tilsynet med foretaket*". Dersom disse forhold ikke tilfredstilles gjennom kontrakten med leverandøren kan Finanstilsynet gi pålegg om endring eller opphør av kontraktsforholdet, jf. finanstilsynsloven § 4c.

Finanstilsynets oppgaver følger hovedsakelig av finanstilsynslovens § 3. Det fremkommer her ingen krav til såkalte stedlige tilsyn, som i teorien kan begrense bruken av skytjenester. Det kan derfor antas at loven ikke oppstiller hindringer gjennom selve tilsynsfunksjonen, og at lovens ordlyd kan oppfylles også ved bruk av skytjenester. Som del av sin tilsynsvirksomhet gjennomfører Finanstilsynet stedlig tilsyn. Et stedlig tilsyn innebærer en gjennomgang av virksomhetens drift, og et stedlig tilsyn kan omfatte hele virksomheten eller være fokusert mot enkelte risikoområder.

Forskriften gir ingen veiledning i hva som ligger i at Finanstilsynet "*gis tilgang*" til opplysninger, og bruk av skytjenester skal i alminnelighet ikke være et hinder for at opplysninger kan hentes ut av systemene og slik oppfylle plikten. Men IKT-forskriften stiller imidlertid i tillegg et krav om at avtalen også må sikre Finanstilsynet en rett til å utføre "*tilsyn hos IKT-leverandøren*", som kan forstås som et pålegg om stedlig tilsyn hos leverandøren av IKT-systemene. Avhengig av Finanstilsynets praktisering av dette, vil denne bestemmelsen kunne oppstille et hinder for bruk av skytjenester, dersom tilsynet stiller krav om fysisk tilgang til for eksempel lokaler, servere og systemer.

Det er mulig at finanstilsynsloven åpner for tredjepartsrevisjon, slik Datatilsynet praktiserer for tilsyn med skytjenester. Lovens § 2, fjerde ledd hjemler at Finanstilsynet "*kan engasjere statsautoriserte og registrerte revisorer og personer med annen sakkyndighet til å utføre oppdrag innenfor tilsynets arbeidsområde.*" Slik tredjepartsrevisjon vil kunne gjøre det lettere å utføre tilsyn på tvers av landegrenser. Tilsyn med betalingssystemer og annen finansiell infrastruktur er den del av Finanstilsynets tilsynsstrategi for 2015-2018.[23] Det er grunn til å tro at bruken av skytjenester ikke vil gå nedover, men heller øke, innen denne sektoren[24], og Finanstilsynet vil i økende grad måtte ta stilling til disse spørsmålene fremover. Finanstilsynet har i 2010 som koordinerende tilsynsmyndighet etablert et tilsynskollegium for DnB NOR-konsernet. Denne type tilsynssamarbeid er nå et direktivkrav fra 2010 for grensekryssende bankvirksomheter.

[23] Finanstilsynet (2014): *Strategi 2015-2018*
[24] Accenture (2012): *A new era in banking. Cloud computing changes the game*

Finanstilsynet deltar også som vertslandsmyndighet i andre tilsynskollegier for utenlandske konsern med virksomhet i Norge.

Risikovurdering
For virksomheter innen bank- og finanssektoren som ønsker å ta i bruk skytjenester, er det også nødvendig å følge IKT-forskriftens § 3 og § 5 om sikkerhet. § 3 stiller krav om at virksomheten minst en gang årlig gjennomfører en risikoanalyse for å påse at risiko styres innenfor akseptable grenser med tanke på foretakets virksomhet. Bruken av skytjenester, i likhet med annen lagring og behandling av data, må derfor vurderes opp mot den konkrete risikoen, og kan hindre bruk av enkelte skytjenester også innen Norge, dersom tjenesten ikke fremstår tilfredsstillende i en risikoanalyse. De nærmere krav til sikkerhet følger av § 5, og Finanstilsynet har utarbeidet en veileder til bestemmelsen.[25]

Finanstilsynet har i et rundskriv av 2010 om utflytting av bankenes IKT-oppgaver uttalt seg om plikter til å vurdere risiko ved flytting av virksomhet utenlands. Det uttales blant annet at *"Utkontraktering av IKT-oppgaver skal i følge IKT-forskriften § 3 inngå i bankenes risikoanalyse. Flytting av IKT-virksomhet ut av Norge vil normalt medføre en høyere operasjonell risiko for den enkelte bank, avhengig av hvilke type oppgaver som utkontrakteres og til hvilket land utkontrakteringen skjer. Endringer som omfatter flytting av data og/eller tilgang til data må vurderes ut fra sikring av:*

- *konfidensialitet (beskyttelse mot innsyn/kryptering)*
- *integritet (sikring mot uautorisert endring)*
- *tilgjengelighet (kontroll mot definert tilgjengelighet) (ISO 27001)".*[26]

Oppsummering
IKT-forskriften er ikke en direkte hindring for å benytte skytjenester i et annet land, men kontraktsforholdet må være grundig utført og dekke alle aspekter ved virksomhetens ansvar, og utkontrakteringen skal inngå i foretakets risikoanalyse. I og med at regelverket allerede tar høyde for utkontraktering, burde det i utgangspunktet også kunne håndtere skytjenester, såfremt det ikke stilles spesifikke krav til geografi. IKT-forskriften kan derfor fremstå som en opplevd hindring for bruk av skytjenester, både nasjonalt og internasjonalt, på grunn av kompliserte kontraktskrav og praktisering av tilsyn, eller dersom eventuelle sikkerhetsforhold tilsier at skytjenesten ikke er egnet for de aktuelle dataene. Det er uklart hvorvidt Finanstilsynets krav til tilgang på data kan medføre en hindring for bruken av skytjenester.

Verdipapirfondloven og verdipapirhandelloven
Verdipapirfondloven kan være relevant for behandlingen av digital informasjon, da den regulerer informasjon på et varig medium eller nettsted. Etter § 1-2 nr 10 defineres *"varig medium"* i loven som *"en innretning som gjør det mulig for en investor å lagre informasjon adressert personlig til vedkommende investor. Informasjonen må være tilgjengelig for fremtidig bruk i et tidsrom som er tilstrekkelig for informasjonens formål, og*

[25] Finanstilsynet (2013): *Veileder til IKT-forskriftens § 5 "sikkerhet"*
[26] Finanstilsynet (2014): *Rundskriv. Utflytting av bankenes IKT-oppgaver.* RFT-2010-14

informasjonen må kunne reproduseres uforandret." Antagelig vil ikke dette kravet kunne påvirke bruken av skytjenester, såfremt lovens krav er tilfredsstilt. Loven gir ellers ingen føringer som kan påvirke bruken av skytjenester.

Verdipapirhandellovens formål er å legge til rette for sikker, ordnet og effektiv handel i finansielle instrumenter. Tilsyn med verdipapirforetaks- og sentrale motparters virksomhet utføres av Finanstilsynet. De samme forhold som er drøftet under finanstilsynsloven gjelder også her. Det stilles i § 15-3 krav om utskrift fra lagringsmedium. Dette medfører ingen hindring for bruk av skytjenester, da det må forutsettes at det er mulig å ta utskrift via et systemgrensesnitt mot skytjenesten.

Andre lover under Finansdepartementet
Arbeidsgruppen har undersøkt også annet regelverk innen sektoren uten å avdekke bestemmelser som kan være, eller oppfattes som, en hindring for bruk av skytjenester. Gruppen har blant annet vurdert kapitalkravsforskriften, forskrift om tilsyn med finansinstitusjoner og forvaltningsselskap som har hovedsete i annen EØS-stat og som driver virksomhet i Norge m.v., samt skatteloven og skattebetalingsloven.

Konklusjon:
Det foreligger til dels hindringer for bruk av skytjenester i bokføringslov og IKT-forskrift. Enkelte hindringer i regelverk innen bank- og finanssektoren forekommer på grunnlag av praktiseringen av tilsyn og krav i forskrift.

Tiltak:
Det bør vurderes utstrakt veiledning, eventuelt utformes sjekklister, rundt kontraktsforhold som gjelder bruk av skytjenester innen bank- og finanssektoren. Det er antagelig ikke hensiktsmessig å foreta endringer i bokføringsloven eller IKT-forskriften. Vedrørende bokføringsloven vil det imidlertid være aktuelt å avklare forutsetninger og handlingsrom for å utvide adgangen til å lagre slike data i utlandet. Som en del av dette arbeidet bør det vurderes om det vil være mulig å utvide listen over land hvor oppbevaring er tillatt til å omfatte hele EØS-området.

Det kan være grunn til å redegjøre for tilsynsfunksjonen innen sektoren knyttet til skytjenester.

Arbeidsgruppen vil på generelt grunnlag anbefale regjeringen å foreta en gjennomgang av tilsynsfunksjonen innen flere sektorer samlet for å vurdere forhold rundt økende bruk av skytjenester og tilsynsproblematikk knyttet til dette. Spørsmål om praktisering av stedlig tilsyn og tilsyn over landegrenser peker seg ut som aktuelle temaer som flere tilsynsmyndigheter møter. Selv om ulike sektorer kan ha ulike behov innen tilsynsfunksjonen, er det mange like utfordringer som med fordel kan drøftes samlet.

5.5 Justis- og beredskapsdepartementet

Arbeidsgruppen har hatt deltagelse fra Justis- og beredskapsdepartementets rednings- og beredskapsavdeling og fra lovavdelingen. En gjennomgang av reguleringen underlagt Justis- og beredskapsdepartementet har ikke avdekket noen klare hindringer for å ta i bruk skytjenester, med unntak av mulige begrensninger vedrørende utøvelsen av tilsyn.

Regelverk som særskilt er undersøkt, og som kan trekkes frem her, er skifteloven, produktansvarsloven, storulykkeforskriften, forskrift om håndtering av eksplosjonsfarlig stoff, forskrift om landtransport av farlig gods, brann- og eksplosjonsvernloven, forskrift om sikkerhet ved arbeid i og drift av elektriske anlegg og sivilbeskyttelsesloven. Det har ikke vært mulig å avdekke hindringer for bruk av skytjenester i disse lover og forskrifter.

Arbeidsgruppen ser det likevel som hensiktsmessig å komme med noen betraktninger rundt enkelte lover underlagt Justis- og beredskapsdepartementet.

El-tilsynsloven

I lov om tilsyn med elektriske anlegg og elektrisk utstyr (el-tilsynsloven) § 5 fjerde ledd heter det at "*Enhver som er underlagt tilsyn etter denne lov, skal når tilsynsmyndigheten krever det og uten hinder av taushetsplikt fremlegge opplysninger som anses nødvendige for utøvelsen av tilsynet. Tilsynsmyndigheten kan bestemme i hvilken form opplysningene skal gis.*" Tilsyn etter denne loven foretas av Direktoratet for samfunnssikkerhet og beredskap (DSB). Det er i forarbeidene[27] påpekt at det er viktig at "*tilsynsmyndighetene ikke utestenges fra steder hvor dokumentasjon befinner seg*", altså det som kan kalles "stedlig tilsyn". Lovteksten er ment å skulle ivareta dette hensynet, men bruk av skytjenester i seg selv er ikke i direkte strid med ordlyden i bestemmelsen. Bruken av skytjenester behøver ikke medføre at tilgangen på opplysninger blir dårligere for tilsynsmyndigheter, men en utfordring i praktiseringen trer inn når opplysninger er lagret på servere det kreves tilsyn med, og disse er plassert i ulike land. Eventuelle begrensninger på bakgrunn av denne loven følger av praktiseringen av tilsynet, og de premisser tilsynsmyndigheten krever foreligge for å tilfredsstille et stedlig tilsyn. Det kan diskuteres om tilsynsmyndighetene har behov for tilgang til fysiske steder for at virksomheter skal oppfylle plikten i lovens § 5 fjerde ledd.

Arbeidsgruppen er ikke kjent med at Direktoratet for samfunnssikkerhet og beredskap stiller krav om at skytjenester ikke kan benyttes for virksomheter underlagt dette regelverket.

Tvangsfullbyrdelsesloven

I forbindelse med tilsyn av el-anlegg kan også tvangsfullbyrdelsesloven § 13-14 om fullbyrdelse av handleplikter komme til anvendelse. Det kan anføres at dersom el-anlegget styres i en skytjeneste er det liten realitet i hjemmelen som her foreligger til å

[27] Ot.prp.nr.67 (1999-2000) s. 16

stenge ned anlegget. Dette spørsmålet er ikke problematisert i praksis, og oppstiller en teoretisk utfordring inntil videre.

Tvangsfullbyrdelsesloven inneholder videre en bestemmelse om at "*Kongen kan gi bestemmelser om føring, arkivering, oppbevaring og tilintetgjøring av namsbøker og andre dokumenter*", se § 5-19. Forskrift som loven henviser til er ikke gitt per i dag, og ingen hindring i regelverket foreligger etter denne bestemmelsen.

Vergemålslov med forskrift
Regelverk som innehar tilsynsfunksjon kan i enkelte tilfeller gi føringer for bruk av IKT-systemer på grunnlag av tilsynsmyndighetenes behov for tilgang, og det kan være vanskelig for rettsanvendere å avgjøre om det foreligger en hindring i regelverket. Etter vergemålsloven § 6 kan Fylkesmannen føre tilsyn med vergene i sitt område, og etter § 7 kan den sentrale vergemålsmyndigheten føre tilsyn med fylkesmannen. Regler om begge tilsynsfunksjoner er gitt i forskrift til vergemålsloven, se særlig §§ 2 og 5. Tilsynet vil kunne medføre krav om tilgang til steder personopplysninger oppbevares, og aktuelle systemer for behandling av disse. Siden disse spørsmål angår personopplysninger vil videre spørsmål ikke berøres her.

I vergemålsforskriften § 5, tredje ledd, siste setning, heter det imidlertid at "*Den sentrale vergemålsmyndigheten skal føre tilsyn med at det er etablert systemer og rutiner som sikrer at de eiendelene som forvaltes av fylkesmannen etter vergemålsloven, forvaltes på en forsvarlig måte, og at eventuelle økonomiske misligheter forebygges og avdekkes.*" Tilsynsmyndigheten kan her føre tilsyn med systemer, men med grunnlag i at det ikke finnes krav i lov eller forskrift til oppbevaring av data på bestemte måter, er det vanskelig å foreta noen antagelse om at vergemålsloven med forskrift kan være en hindring for bruk av skytjenester. I likhet med innsynsregler i annet lovverk, vil ikke tilgangen til dokumenter utgjøre noen utfordring, da innsyn enkelt vil kunne sikres også ved bruk av skytjenester. Innsyn og tilgang til data er derfor ikke til hinder for bruk av skytjenester, men tilsyn med systemene som behandler disse kan være det.

Etter forskriftens § 20 skal kvitteringer og andre bilag "*oppbevares som dokumentasjon i tre år etter utløpet av regnskapsåret.*" Selv om noe skal "*oppbevares*" over tid kan bruken av en skytjeneste klart oppfylle dette kravet. Arbeidsgruppen antar at kravet om oppbevaring over tid baserer seg på at dokumentasjonen skal kunne fremlegges også senere, ikke at dette handler om å sikre "god drift" av en virksomhet for eksempel. Så lenge tilsynsmyndigheten kan få seg forelagt dokumentene og dataene som skal oppbevares, er dette ingen hindring for bruk av skytjenester. Tilsynsmyndighetene kan for øvrig velge å kreve at slik oppbevaring skjer under visse forutsetninger om for eksempel konfidensialitet, integritet og tilgjengelighet - alminnelige sikkerhetsprinsipper som ofte benyttes både for skytjenester og andre IKT-systemer. Det vil antagelig ikke være grunn til å oppstille strengere regler her, enn for eksempel det som kreves av bank- og finansinstitusjoner, se omtale av denne sektoren i kapittel 5.4.

Vergemålsloven er et godt eksempel på den type uklarheter i regelverk som kan medføre virksomheter er usikre på om de kan ta i bruk skytjenester. Arbeidsgruppen anser at det ikke er noe i vergemålslov med forskrift som er til hinder for bruk av skytjenester.

Konklusjon:
Det er ingen klare, direkte hindringer for bruk av skytjenester i regelverket som Justis- og beredskapsdepartementet har ansvar for. Enkelte begrensninger kan imidlertid følge på bakgrunn av praktiseringen av stedlig tilsyn fra tilsynsmyndigheter, og noen uklarheter finnes i regelverket. Arbeidsgruppen viser her til anbefaling om gjennomgang av tilsynsfunksjon på tvers av sektorer, som presentert i kapittel 5.4.

5.6 Nærings- og fiskeridepartementet

Det har ikke vært mulig å avdekke hindringer i regelverk innen Nærings- og fiskeridepartementets ansvarsområde. Til tross for dette trekkes ofte anskaffelsesregelverket fram som et regelverk som gjør det vanskelig for IKT-næringen å tilby skytjenester som alternativ når de leverer tilbud til offentlige virksomheter. Offentlige virksomheter som ønsker å anskaffes skytjenester viser også til at anskaffelsesregelverket skaper usikkerhet for dem. Direktorat for forvaltning og IKT (Difi) har bidratt til arbeidsgruppens vurderinger på dette området.

Lov om offentlige anskaffelser med forskrift
Anskaffelsesregelverket innebærer ikke i seg selv noen begrensinger for oppdragsgivers mulighet til å anskaffe eller benytte skytjenester. Loven gir de overordnede rammene for offentlige anskaffelser, mens de detaljerte prosedyrereglene er nedfelt i tilhørende forskrifter. Ved informert bruk av virkemidler innen anskaffelsesregelverket vil virksomheter kunne anskaffe gode løsninger tilpasset sitt behov, herunder også i form av skytjenester. Mulighetene lov og forskrift om offentlige anskaffelser gir er interessant i et overordnet skyperspektiv. Å se nærmere på rammene anskaffelsesregelverket oppstiller er relevant for andre deler av arbeidet med sky, særlig tilrettelegging og eventuelt samordning av innkjøp av skytjenester.

Imidlertid kan det være utfordringer ved selve gjennomføringen av offentlige anskaffelser av skytjenester. Disse er ikke nødvendigvis unike for skytjenester, men enkelte problemstillinger synes å være spesielt relevante for denne type anskaffelser.

Det er utfordringer knyttet til det å sammenligne ulike tilbudte løsninger og sikre reell konkurranse på bakgrunn av tildelingskriterier. Det kan for eksempel være spesielt utfordrende dersom man skal anskaffe programvare, hvor enkelte tilbydere kan tilby dette som et nedlastbart produkt (med lokal installasjon), mens en skyleverandør vil tilby dette som en tjeneste, hvor også drift og forvaltning er inkludert. Det er opp til den som anskaffer å spesifisere tjenestebehovet. Det er da viktig å spesifisere på funksjon, slik at man ikke utelukker noen teknologiske plattformer fra starten av. Dette løser imidlertid ikke nødvendigvis alle utfordringer med sammenligning av tilbud, hvor forutsetningen for prising er ulik.

En sentral anskaffelsesproblematikk er knyttet til forholdet til leverandørenes tilbud og standardvilkår, og om disse vilkårene kan forhandles eller ikke. Valg av konkurranseform vil ha betydning for offentlige oppdragsgiveres mulighet til å forhandle. Åpen anbudskonkurranse vil i utgangspunktet være en lite egnet anskaffelsesprosedyre, fordi det regelmessig vil være behov for å kunne ha mulighet til å tilpasse tilbudene.

Valg av kontraktsform er ikke alltid gitt dersom man kjøper programvare som en tjeneste, med forvaltning og drift i ett. Det er også utfordrende at skytjenester som regel selges som hyllevare med standard kontraktsvilkår fra leverandøren. Leverandørens standardbetingelser vil ikke sjeldent kunne inneholde avvikende bestemmelser fra kundens innkjøpsavtale, for eksempel en SSA (Statens Standardavtaler). Kundene må derfor på forhånd, i planleggingsfasen av en anskaffelse, undersøke om leverandørenes vilkår kan stride mot de kravene som stilles. En tilgrensende problemstilling er usikkerhet knyttet til hvilken standard kontraktsmal man skal velge.

Et annet forhold som kan nevnes er finansieringsmodellen som særlig benyttes for skytjenester. Skytjenester er ofte rimelige, det kan være enkeltbeløp langt under kr. 100 000 per transaksjon. En utfordring som oppstår for virksomheter er der behovet for oppskalering av tjenesten inntrer, og anskaffelsens samlede verdi over tid overstiger grensen for kunngjøringsplikt. Samme problematikk gjelder for store organisasjoner med flere enheter som kjøper inn mindre tjenester hver for seg, hvor verdien av samlet innkjøpsvolum over tid overstiger grensen for kunngjøringsplikt. I tillegg er det en generell risiko for at denne typen tjenester med lav verdi ikke konkurranseutsettes i det hele tatt. Disse utfordringene er ikke unike for skytjenester, men er spesielt aktuelle på grunn av slike tjenesters relativt sett rimelige finansieringsmodell.

Konklusjon:
Det er ingen klare hindringer for bruk av skytjenester i regelverket som Nærings- og fiskeridepartementet har ansvar for. Noen utfordringer, og muligheter, følger likevel av anskaffelsesregelverkets kompleksitet. Anskaffelsesregelverket gir offentlige virksomheter mulighet til å anskaffe gode og funksjonelle IKT-systemer - også skytjenester. Men det er en særlig utfordring at mange virksomheter mangler tilstrekkelig anskaffelsesfaglig kompetanse til å gjøre egne vurderinger på området.

Tiltak:
En ser at det innen anskaffelsesområdet kan være behov for å utarbeide sjekklister og veiledere for anskaffelser av skytjenester. Arbeidsgruppen anbefaler likevel ikke at det utarbeides en egen SSA for kjøp av skytjenester spesifikt, da er viktig at løsninger som fyller samme behov, men som er basert på ulike leveransemodeller, kan konkurrere om en kontrakt. Det er samtidig viktig å sikre at de kravspesifikasjonene som utarbeides ikke hindrer kjøp av skyløsninger gjennom å være for tett knyttet til de eksisterende avtalemalene virksomhetene kan velge mellom.

5.7 Kommunal sektor

Kommunalavdelingen i KMD har ansvar for de sektorspesifikke lovene som berører kommunene, herunder kommuneloven, valgloven, lov om interkommunale selskaper, inndelingslova og forsøksloven. Kommunalavdelingen har ikke funnet noen hindringer for bruk av skytjenester i regelverket som avdelingen har ansvaret for.

Kommunal- og moderniseringsdepartementet har i arbeidet med en nasjonal strategi for bruk av skytjenester hatt et samarbeid med KS. KS har på selvstendig grunnlag fått gjennomført en omfattende utredning av regelverk som kommunene må forholde seg til ved bruk av skytjenester. Heller ikke KS sin utredning viser at det er spesielle hindringer i det kommunespesifikke lovverket. De hindringene som er avdekket for kommunene er de samme hindringene som arbeidsgruppen har identifisert generelt.

Konklusjon:
Det er ingen klare hindringer for bruk av skytjenester i regelverket som kommunalavdelingen i Kommunal- og moderniseringsdepartementet har ansvar for.

6. Juridiske betraktninger

Gjennom kartleggingen av hindre i regelverk har arbeidsgruppen funnet at det er særlig tre typer data som det stilles spesielle krav til behandlingen av: finansielle data, arkivdata fra offentlige virksomheter og personopplysninger. I tillegg reises sikkerhetsspørsmål for virksomhetens behandling av data generelt. Vi ser videre at det er fellestrekk ved deler av lovgivningen rundt behandling av data i ulike sektorer, men det er også enkelte ulikheter.

Arbeidsgruppen har også diskutert noen juridiske forhold av mer generell art, og spørsmål med grenseflater til sektorregelverket som belyser sentrale spørsmål for virksomheter som ønsker å benytte skytjenester. Under vil vi oppsummere de funn arbeidsgruppen har gjort på tvers av sektorene, og trekke frem noen overordnede utfordringer. Hensikten med en slik tverrgående oversikt, er å bidra til å belyse forhold virksomheter generelt bør være oppmerksomme på ved bruk av skytjenester til behandling av data, men også forhold lovgiver bør være bevisst på og ta hensyn til ved utforming av regelverk.

6.1 Lovstruktur og harmonisering

Ulikheter i utformingen av og ordlyden i regelverk kan medføre at det oppstår usikkerhet om hvorvidt et regelverk er til hinder for at det offentlige eller private aktører benytter skytjenester. Eksempelvis kan krav om at dokumentasjon eller dokumenter skal oppbevares på et "varig medium" reise tvil om ordlyden stenger for at dokumentasjon og dokumenter kan oppbevares i en skytjeneste, eller om slik oppbevaring bare kan skje etter en vurdering av hvorvidt kontraktsforholdet mellom tjenesteyter og tjenestemottaker tilfredsstiller nærmere angitte krav. Videre kan innholdet av begrepet "varig medium" være gitt én definisjon i ett regelverk, mens det samme begrepet gis en annen definisjon i et annet regelverk. Hvis virksomheten er underlagt flere regelverk i et slikt tilfelle, vil usikkerhet om tolking av regelverket i seg selv være en hindring for bruk av skytjenester.

Et sitat hentet fra NOU 2013:2 *Hindre for digital verdiskaping* viser at dette er en utfordring som kan identifiseres flere steder. I denne sammenheng dreier det seg om sikkerhetskrav:

"*De ulike reguleringer knyttet til å sikre digital informasjon er i seg selv en utfordring for industrien. Manglende samkjøring av regelverk er en byrde snarere enn styrking av formålet med reguleringene. Digitutvalget merker seg at det til dels er stor forskjell på språkbruk og krav i de ulike lovene og forskriftene. Det er eksempelvis stort sprik i måten tiltak beskrives i IKT-forskriften og sikkerhetsloven.*"[28]

En særlig utfordring oppstår når virksomheter ønsker å ta i bruk en skytjeneste for flere typer av data. Det kan være utfordrende å skulle ta i bruk samme tjeneste for to

[28] NOU 2013:2: *Hindre for digital verdiskapning*, kapittel 2.3.3

eller flere typer av virksomhetsdata, når dataene er underlagt ulikt regelverk og med det ofte ulike krav til forhold slik som sikkerhet, krav til teknisk løsning, back-up-rutiner, eller lokaliseringskrav. Det er sjelden regelverk er harmonisert på slike detaljer, som kan føre til en opplevd hindring for bruk av skytjenester.

Det kan for det første være utfordrende å sammenligne krav til behandlingen i ulikt regelverk, for eksempel de tekniske sikkerhetskravene som stilles til ulike datatyper eller omfanget av en risikovurdering som må utføres. Det kan videre være utfordrende å avgjøre og sile ut hvilke data som fullt ut kan behandles i skytjenesten, eller om det finnes begrensninger på at kun prosessering er greit, men ikke lagring og permanent oppbevaring av data. Strenge rettslige krav for én type data kan medføre at virksomheten ikke tar i bruk skytjenesten heller for andre typer av data, selv om det både kan være tillatt og svært fordelaktig å benytte skytjenester for disse andre.

6.2 Utdatert regelverk

Store deler av det norske regelverket er tidligere gjennomgått og revidert for å sørge for at reglene er teknologinøytrale, og for å muliggjøre bruk av digitale løsninger. Likevel ser vi at det fremdeles er enkelte lover som ikke er tilpasset nyere teknologiske løsninger og muligheter. Vi har regelverk som setter til dels unødige begrensninger for bruk av sky der det samtidig skal kunne utøves tilsyn, eller hvor geografiske føringer for behandlingen av data oppstiller barrierer for bruk av skytjenester. Vi ser også at forarbeider ikke i tilstrekkelig grad gir veiledning på dette området, fordi teknologiutviklingen har gitt muligheter som ikke var mulig å forutse da lovene ble opprettet.

Regelverk som er utdatert vil medføre unødige hindringer for bruk av nye, mer moderne tjenester, på tross av at hensynet bak regelverket kan ivaretas i løsningene. Det er for eksempel mulig å lagre identiske data på flere steder ved å bruke skytjenester, og regelverk som oppstiller geografiske føringer om oppbevaring innen Norge kan til dels sies å være utdatert nettopp av den grunn. Arkivloven er et eksempel på dette.

6.3 Sikkerhetsspørsmål

Forsvarsdepartementet har ikke deltatt i arbeidsgruppen, slik at særskilt regelverk innen forsvarssektoren ikke er gjennomgått. Dette har heller ikke vært ansett som et spesielt relevant lovområde i denne sammenheng. Likevel bør sikkerhetsloven, som faller inn under Forsvarsdepartementets ansvarsområde, nevnes i sammenheng med bruk av skytjenester. En juridisk gjennomgang av sikkerhetsloven faller utenfor arbeidsgruppens rekkevidde, slik at kun enkelte aspekter ved loven nevnes her. Forsvarsdepartementet er for øvrig i gang med en revisjon av sikkerhetsloven.

Loven gjelder for forvaltningsorganer, og for rettssubjekter som leverer sikkerhetsgraderte anskaffelser til forvaltningsorganer, jf. § 2, første ledd. Formålet

med sikkerhetsloven er å legge forholdene til rette for å motvirke trusler mot rikets selvstendighet, sikkerhet og andre vitale nasjonale sikkerhetsinteresser, ivareta den enkeltes rettssikkerhet, og trygge tilliten til og forenkle grunnlaget for kontroll med forebyggende sikkerhetstjeneste.

Dersom en virksomhet behandler materiale som er underlagt sikkerhetslovens bestemmelser, er det flere forhold som kan være til hinder for bruken av skytjenester. Når informasjon må beskyttes av sikkerhetsmessige grunner, kalles den sikkerhetsgradert informasjon, og informasjonen blir merket enten med sikkerhetsgraden strengt hemmelig, hemmelig, konfidensielt eller begrenset, jf. § 11. Nasjonal sikkerhetsmyndighet må godkjenne informasjonssystemet for angjeldende sikkerhetsgrad før skjermingsverdig informasjon behandles, lagres eller transporteres i et slikt system, jf. § 13. Her vil de tekniske løsningene, sammenholdt med skjermingsgrad over dataene, avgjøre hvorvidt det foreligger en hindring for bruk av skytjenester eller ikke.

Sikkerhetsloven inneholder i tillegg regler om virksomhetens plikter for å ivareta sikkerhet, monitorering av systemer og særlige regler om anskaffelser som er viktig å ivareta. En konkret bestemmelse som kommer til anvendelse dersom en tredjepart skal involveres i virksomheten, for eksempel en leverandør av en IKT-tjeneste, er § 28 om leverandørklarering. Før en leverandør kan få tilgang til skjermingsverdig informasjon sikkerhetsgradert konfidensielt eller høyere, eller dersom det av andre grunner anses nødvendig, skal leverandøren ha gyldig leverandørklarering for angitt sikkerhetsgrad. Leverandørklareringen gjelder for det enkelte oppdrag og Nasjonal sikkerhets-myndighet er klareringsmyndighet. I tillegg må en sikkerhetsavtale inngås, jf. § 27, og denne skal være inngått før leverandøren kan få tilgang til skjermingsverdig informasjon. Sikkerhetsavtale med utenlandske leverandører kan bare inngås etter godkjenning av Nasjonal sikkerhetsmyndighet.

Sikkerhetsloven setter en klar skranke for bruk av skytjenester, og vil antagelig være en absolutt hindring for bruk i de fleste tilfeller der skjermingsverdig informasjon behandles. Det vil kun være Nasjonal sikkerhetsmyndighet som eventuelt kan gi tillatelse til bruk av skytjenester for disse dataene i virksomheter som ønsker å ta i bruk slike tjenester.

Sikkerhetsspørsmål er også diskutert av arbeidsgruppen på friere grunnlag, og gruppen er kommet til at klare sikkerhetskrav i regelverk i praksis kan utgjøre en hindring for bruk av skytjenester. Dette kan skyldes bestemte risikovurderinger som må foretas, og som kan påvirke om det er mulig å ta i bruk en bestemt IKT-løsning, eller konkrete krav til nivå på sikkerheten som kan leveres i skytjenesten. Regelverk omtaler som regel kun de overordnede påbud om at risikovurderinger skal foretas, mens de nærmere krav og eventuelle standardiseringskrav følger ofte av forskrift, instrukser eller av praksis fra kontroll- og tilsynsorganer. Det vil være opp til virksomheten selv å vurdere hvorvidt en aktuell skyleverandør tilfredsstiller virksomhetens krav til sikkerhet.

Det oppstilles konkrete føringer med virksomheters bruk av IKT-systemer i flere regelverk. Utover tilsynsmyndighetenes krav om tilsyn med selve systemene, stilles det ofte også krav til bruk av sikre tekniske løsninger og risikovurderinger som må foretas der enkelte typer av data behandles. Slike krav kan noen ganger være en hindring for bruk av enkelte skytjenester, der det for eksempel stilles såpass strenge sikkerhetskrav at det ikke finnes skytjenester på markedet som det vil være lønnsomt å benytte. Likevel vil dette gjelde generelt for alle IKT-systemer, og det kan dukke opp tilfredsstillende løsninger på et senere tidspunkt.

Slike sikkerhetskrav kan også være en opplevd hindring, fordi kravene er kompliserte og kanskje ikke tilstrekkelig redegjort for. Dette kan føre til usikkerhet rundt lovligheten av bruk av skytjenester, og gjøre at man velger å ikke bruke slike tjenester. I tillegg kan en virksomhet oppleve ulike sikkerhetskrav for sine ulike systemer, som følge av fragmentert regelverk. Under kapittelet om lovstruktur så vi nevnt et eksempel på sikkerhetskrav som fremkommer ulikt i henholdsvis IKT-forskriften og i sikkerhetsloven. Fragmenterte sikkerhetskrav for virksomheter kan i seg selv være en indirekte hindring for bruk av skytjenester, og skaper spesielt problemer for virksomheter som er underlagt flere ulike sektorregelverk (slik som kraftselskaper som også tilbyr kommunikasjonstjenester).

Det er også verd å nevne at informasjon som lagres i felles datasentre eller skytjenester som i utgangspunktet ikke er skjermingsverdig etter sikkerhetsloven kan bli skjermingsverdig dersom informasjonen til flere samfunnsfunksjoner samles på ett sted. Da vil skadepotensialet ved tap av den samlede informasjonen kunne få betydning for rikets sikkerhet. Dette er et forhold som også kan bidra til å komplisere de risikovurderingene som må gjøres, ettersom man risikerer å måtte vurdere ikke bare egne data, men også konsekvensen av å lagre egne data på samme sted som andre virksomheter.

6.4 EØS-regelverket

Arbeidsgruppen har drøftet noen begrensninger som følger av EØS-avtalen. EØS-relevant EU-regelverk påvirker norsk lovgivning og setter rammer for regler vi utarbeider nasjonalt som gjelder flyt av varer, tjenester, kapital og arbeidskraft. EØS-avtalens hoveddel gjelder etter EØS-loven § 1 som norsk lov. Det følger av EØS-avtalen artikkel 36 nr. 1 at "*det ikke [skal] være noen restriksjoner på adgangen til å yte tjenester innen avtalepartenes territorium for statsborgere i en av EFs medlemsstater eller en EFTA-stat som har etablert seg i en annen av EFs medlemsstater eller EFTA-stat enn tjenesteytelsens mottager*". Bestemmelsen medfører at det som et utgangspunkt ikke kan diskrimineres mellom tjenesteleverandør etablert i Norge og tjenesteleverandør etablert i en annen medlemsstat. Av EØS-lovens § 2 følger det at regler i EØS-lovgivningen som et utgangspunkt har forrang ved motstrid mot annet regelverk. Ut fra EU-domstolen sin rettspraksis legges det nå til grunn at tiltak som gjør det *vanskeligere* å utøve tjenester mellom medlemsstatene enn innenfor én medlemsstat utgjør en

restriksjon etter bestemmelsen. Restriksjonsforbudet skal etter artikkel 39 jf. artikkel 33 "ikke *hindre at bestemmelser om særbehandling av fremmede statsborgere får anvendelse når de er fastsatt ved lov eller forskrift og begrunnet med hensynet til offentlig orden, sikkerhet og folkehelsen*". Etter rettspraksis kan restriksjoner være tillatt dersom de er begrunnet i læren om "*allmenne hensyn*". Utgangspunktet er dermed at restriksjoner på bruk av skytjenester med bakgrunn i at tjenesteyter er etablert i en annen EØS-stat ikke er lovlig, med mindre restriksjonen likevel er tillatt etter de nevnte unntakene ovenfor. Av samme grunn må det utvises varsomhet med å stille krav om for eksempel lagring innen Norge i en anskaffelse, særlig ved anskaffelser over terskelverdiene som EU oppstiller i anskaffelsesregelverket.

Arbeidsgruppen har ikke grunn til å tro at hindre som er avdekket i rapporten strider mot EØS-avtalen, men vil minne om skrankene som finnes ved etablering av nytt regelverk, dersom for eksempel geografiske føringer for behandlingen av data vurderes.

6.5 Forvaltningsspørsmål

En rekke lover inneholder regler om rett til innsyn, enten for allmennheten eller for tilsynsmyndigheter, blant annet offentleglova. Det forutsettes for gjennomgangen av regelverket innen de ulike sektorer at regler om rett til innsyn i dokumenter i disse lovene kan ivaretas innenfor en skytjeneste. Dette må ikke forveksles med tilsynsmyndigheters rett til tilgang til systemer og kontroll av behandlingen av data. Der tilsynsmyndigheter imidlertid har rett på tilgang til dokumenter eller opplysninger forutsettes det at dette ivaretas også ved bruk av skytjenester, med mindre annet følger av den konkrete lov.

Noen betraktninger kan gjøres rundt taushetspliktbestemmelser i lovgivningen. Etter forvaltningsloven § 13 første ledd har "*[e]nhver som utfører tjeneste eller arbeid for et forvaltningsorgan*" taushetsplikt for opplysninger om noens personlige forhold og forretningsrelaterte opplysninger som det vil være av konkurransemessig betydning å hemmeligholde. Dersom et organ inngår avtale med et privat firma om drift av en skytjeneste hvor organets dokumenter lagres, vil derfor de personene i dette firmaet som eventuelt får kjennskap til taushetsbelagt informasjon, selv ha taushetsplikt. Benytter derimot det private firmaet seg av underleverandører som står for vedlikeholdet av skytjenesten, og disse igjen kanskje bruker underleverandører, er det uklart hvor langt man kan si at de ulike aktørene "*utfører tjeneste eller arbeid for et forvaltningsorgan*" og dermed er underlagt taushetsplikten uten at det foreligger en egen avtale. På et tidspunkt vil det gå en grense, og virksomheter må være bevisste på dette ved kontraktsinngåelse med eksterne leverandører av tjenester.

Det er til en viss grad uklart i hvilken grad man kan overlate ansvaret for taushetsbelagt informasjon til private aktører. Forvaltningsloven § 13 første ledd innebærer at man aktivt søker å hindre at uvedkommende får tilgang til taushetsbelagt informasjon. Dersom bruk av skytjenester medfører at mange personer utenfor organet får eller kan

få tilgang til slik informasjon, kan dette i seg selv tenkes å medføre brudd på taushetsplikten. Dette gjelder først og fremst dersom ikke alle disse personene selv blir omfattet av lovfestet taushetsplikt. Vi kan ikke se at forvaltningsloven § 13 b første ledd, som presiserer hovedregelen, vil gi noen generell hjemmel for overlating av taushetsbelagte opplysninger i slike tilfeller, det må eventuelt vurderes helt konkret i det enkelte tilfellet.

E-forvaltningsforskriften gir konkrete føringer ved bruk av elektronisk kommunikasjon i et forvaltningsorgan, blant annet i forskriftens § 5. Det vises her til at risiko for uberettiget innsyn i opplysningene, ved bruk av elektronisk kommunikasjon, må "*være forebygget på tilfredsstillende måte*", jf. § 5, første ledd. Etter tredje ledd følger videre at "f*orvaltningsorganet skal opplyse generelt om hvordan taushetsbelagte opplysninger og personopplysninger sikres under behandling i forvaltningsorganet*." Elektronisk kommunikasjon omhandler her ikke direkte skytjenester, men illustrerer at sikkerhetsvurderinger må foretas ved bruk av IKT-løsninger generelt, og at forvaltningsregelverket i seg selv ikke er et hinder for bruk av IKT.

6.6 Personvern

Personvernreglene, herunder personopplysningsloven spesifikt og personvernspørsmål i annen lovgivning, er ikke drøftet inngående i arbeidsgruppen. Arbeidsgruppen anser det likevel som relevant å omtale personvernspørsmål i sammenheng med de andre områdene som rapporten tar for seg.

I en rekke sektorlover er det gitt bestemmelser med grunnlag i personvernregulering, eller det vises til at personopplysningslovens bestemmelser også gjelder innen sektoren. Arbeidsgruppens forutsetning om at hindringer ikke foreligger i slikt sektorregelverk tar derfor forbehold om skranker i de bestemmelser som gjelder behandlingen av personopplysninger.

Personopplysningsloven stiller ingen direkte rettslige skranker for bruken av sky-tjenester, men det er relevant å trekke frem de geografiske føringene for behandlingen av personopplysninger. Personopplysninger "*kan bare overføres til stater som sikrer en forsvarlig behandling av opplysningene*", jf. personopplysningsloven § 29, og kan derfor ikke uten videre overføres til land utenfor EØS-området. Det foreligger likevel en del unntak, se lovens § 30. Blant annet kan enkeltvise overføringer forhåndsgodkjennes av Datatilsynet, og dersom det inngås avtaler med databehandler ved bruk av EUs standardkontrakter, foreligger lovlig grunnlag for overføringer. I tillegg er enkelte land utenfor EU godkjent av EU som trygge mottakerstater, og det foreligger sertifiseringsmulighet gjennom "Safe Harbour"-prinsippene. Loven oppstiller dermed til dels skranker for bruk av skytjenester til lagring av personopplysninger dersom skyleverandøren, det vil i praksis si databehandleren, befinner seg utenfor EØS, utenfor de EU-godkjente landene eller ikke er omfattet av "Safe Harbour".

Datatilsynet har utformet en sjekkliste basert på regelverket og beste praksis[29] som virksomheter må vurdere før en skytjeneste tas i bruk for å behandle personopplysninger:

- Det gjennomføres grundige risikovurderinger i forkant, herunder en risiko- og sårbarhetsanalyse.
- Det må inngås en tilfredsstillende databehandleravtale i tråd med norsk regelverk med tjenesteleverandøren. Det er den behandlingsansvarlige, den enkelte virksomhet, som har ansvar for at lovens krav følges.
- Bruken av nettskytjenester må jevnlig revideres. Det vil si at en selv eller en tredjepart gjennomfører en sikkerhetsrevisjon og sikrer at databehandleravtalen følges.
- Den behandlingsansvarlige må sørge for at overføring av data til andre land følger loven.
- Det må sørges for sikker kommunikasjon og kryptering av kommunikasjonen.
- Løsningen som benyttes må være tilstrekkelig dokumentert, og dokumentasjonen må kunne fremlegges, slik at kontroll kan utføres.

Denne sjekklisten gir gode anbefalinger som er relevante også for behandling av andre typer data enn personopplysninger, og vil være et godt utgangspunkt for virksomheter som ønsker å ta i bruk skytjenester uavhengig av type data. Arbeidsgruppen minner om at personopplysningsloven ikke er drøftet for å avklare eventuelle hindre i denne loven, eller for å komme med anbefalinger om tiltak innen dette området. EU utarbeider nå en ny personvernforordning, og arbeidsgruppen mener derfor det er hensiktsmessig å avvente et slikt arbeid før det foretas en mer inngående vurdering av den norske personopplysningsloven opp mot bruken av skytjenester. Slik det norske regelverket er utformet i dag, og slik det tolkes og praktiseres av Datatilsynet og Personvernnemnda, mener gruppen at dette regelverket gir stort handlingsrom for virksomheter som ønsker å lagre og behandle personopplysninger i allmenne skytjenester.

6.7 Geografiske føringer

Regelverk som oppstiller geografiske føringer for lagring eller behandling av data er en av de klareste direkte hindringene for bruk av skytjenester, og kan være en absolutt hindring for bruk av skytjenester til behandlingen av enkelte typer data. En alminnelig forutsetning for at dataene i en skytjeneste skal anses for å bli behandlet i Norge, er som regel at serverne befinner seg innen norske grenser. Geografiske hindringer har ofte flere ulike begrunnelser innen samme regelverk, noe som gjør det utfordrende å avdekke den reelle begrunnelsen for hindringen.

Slike lokaliseringskrav kan tilsi at bruk av skytjenester er mulig, men at det foreligger krav til lagring av dataene innen et bestemt område, for eksempel enten på servere innen Norge, Norden, eller EØS. Dette medfører at ikke alle skytjenester kan benyttes.

[29] Datatilsynet: *En veiledning i bruk av skytjenester*

Kravene følger enten direkte eller indirekte av loven, eller gjennom praktisering fra kontrollorganer. Enkelte ganger kan en anta at reglene ikke lenger har tilstrekkelig begrunnelse, og at regelverket er utdatert. Dette gjelder de tilfellene der geografiske føringer ikke lenger kan begrunnes tilfredsstillende med at nasjonale grenser er en nødvendig barriere. Andre ganger følger det av tilsynsmyndighetenes presumptive behov for å kunne utføre stedlige tilsyn. Men også andre aktuelle begrunnelser kan tenkes, blant annet behovet for nasjonal jurisdiksjon, at andre myndigheter ikke skal kunne få tilgang på dataene, eller at det foreligger for stor usikkerhet rundt oppbevaringen dersom den ikke finner sted i Norge. Geografiske føringer for lokaliseringen av data kan derfor ha både gode og mindre gode begrunnelser. Der et regelverk oppstiller slike føringer, er det avgjørende at virksomheten som ønsker å ta i bruk skytjenester er bevisst hvilke data som behandles i tjenesten, og kjenner til hvor serverne til skyleverandøren er plassert.

6.8 Aspekter ved kontraktsforholdet mellom kunde og skyleverandør

En rekke opplevde hindringer for bruk av skytjenester dreier seg om forhold som kan avgjøres i kontrakten med skyleverandøren. Enkelte ganger må en slik kontrakt godkjennes av en kontrollmyndighet, andre ganger er det virksomheten selv som må avgjøre om de nødvendige forhold er kontraktsrettslig avklart. Arbeidsgruppen har ikke gått gjennom alle kontraktuelle forhold som bør tas hensyn til ved inngåelse av en kontrakt, men bemerker at virksomheter må være oppmerksomme på kontraktsaspektet når skytjenester tas i bruk, herunder også kontrakter med eventuelle underleverandører som benyttes. Gjennom kartleggingen av regelverk har vi imidlertid kommet over et par kontraktuelle forhold som kan trekkes fram.

Det er enkelte forhold en virksomhet både *kan* og *må* forholde seg til ved inngåelse av en kontrakt om bruk av skytjeneste med en tjenesteleverandør. Komplekse krav i regelverket er ikke en direkte hindring for bruk av skytjenester, men kan oppleves slik for mange virksomheter. Kontraktsforhold en *må* forholde seg til, for eksempel sikkerhetskrav som følger av regelverk på området, kan i likhet medføre en opplevd hindring for bruk av skytjenester dersom regelverket er komplekst, uklart eller ikke gir tilstrekkelig veiledning i de forhold som må tas i betraktning.

Her er bruken av standardkontrakter mange tjenesteleverandører benytter en særlig utfordring. Kompetansen rundt de individuelle tilpasninger en virksomhet må foreta, med grunnlag i hvilke data som skal behandles i skytjenesten, vil variere, og manglende veiledning er en klar barriere for å ta i bruk slike tjenester.

Flere lover oppstiller geografiske føringer for hvor data kan behandles. Hvor dataene behandles, som vi kan ta som utgangspunkt er der hvor serverne er plassert, vil ofte, men ikke alltid, oppgis i en tjenestekontrakt. Det er derfor gode grunner å sjekke hvorvidt dette er spesifisert i den kontrakten som inngås. Ved bruk av skyleverandørers standardkontrakter bør virksomhetene være ekstra oppmerksomme på dette forholdet

dersom finansielle data, arkivdata eller personopplysninger skal behandles i skytjenesten.

Et annet relevant forhold er regler om utkontraktering av virksomhetsoppgaver. Et eksempel finnes i IKT-forskriften for bank- og finanssektoren. Utkontraktering av virksomhetsoppgaver og bruk av skytjenester til behandling av data er to rettslig sett ulike forhold. Men også ved bruk av skytjenester vil en tredjepart få en rolle ved behandlingen av data gjennom for eksempel tilgang til materialet og gjennom utføring av serviceoppgaver. Dette er et særegent trekk ved skytjenester som medfører at ansvarsforhold ved utkontraktering også bør drøftes ved bruk av skytjenester. Da det ikke er mulig å utkontraktere ansvaret for forhold som konfidensialitet, integritet og tilgjengelighet for dataene virksomheten har ansvaret for, må virksomheten kunne stå inne for eventuelle ansvarsfraskrivelser tjenesteleverandøren gir. Dette kan gjelde for eksempel nedetid, risiko for sletting av data, om det er mulig å endre dataene i ettertid og lignende. Et konkret forhold som må vurderes, er om sikkerheten ved skytjenesten er tilfredsstillende, og det vil kunne være relevant å oppstille hvilke krav en har til sikkerhet i selve kontrakten for å sikre etterlevelse.

Et viktig aspekt ved kontrakten er også de vilkår som omhandler terminering av avtalen, uavhengig av termineringsgrunn. Det er viktig at kontrakten sikrer at kunden kan få tilbakeført sine data, eventuelt overført dataene til en ny leverandør. Det er også viktig at kontrakten klart stadfester kundens eierskap til dataene, inkludert til data som genereres som et resultat av selve driften, for eksempel statstikker knyttet til bruk av en tjeneste. Regler som skal ivareta dette er for øvrig foreslått inntatt som et absolutt krav ved behandlingen av personopplysninger i den nye personvernforordningen som er til drøfting i EU per vår 2015.

Hvilke forhold virksomheten må ta i betraktning, og kontrollere kontraktsvilkårene opp mot, vil følge av det enkelte regelverk behandlingen av virksomhetens data er underlagt.

6.9 Tilsyn med IKT-systemer

Innen flere sektorer er det et antatt behov å kunne kontrollere IKT-systemene som benyttes i virksomheter, og systemene som benyttes i behandlingen av virksomhetens data. En rekke tilsynsorganer praktiserer derfor såkalt stedlig tilsyn innen sitt ansvarsområde. Stedlig tilsyn kan begrunnes i behovet for tilgang og kontroll med databehandling hos kontrollobjektet, med krav til sikkerhet eller med behov for kontroll av selve driften og de tekniske systemer. Slike tilsynskrav kan medføre en hindring for bruk av skytjenester, gjennom krav om at tilsynsorganet fysisk skal kunne kontrollere IKT-systemene som benyttes. For skytjenester, som er basert på ressursdeling, og gjerne at dataene flyttes mellom flere lokasjoner, kan slik fysisk inspeksjon være vanskelig å få til. De fleste skyleverandører vil også av sikkerhetsmessige grunner ønske å begrense antall personer som slipper inn i de fysiske datasentrene, hvor også andre kunders data er lagret. Dette er i denne

rapporten beskrevet som en hindring for bruk av skytjenester både i forbindelse med tilsyn med arkivmateriale og finanstilsynets kontroll med bokføringsdata og IKT-systemer innen bank- og finanssektoren. Arbeidsgruppen antar at det er flere regelverk med tilhørende tilsyn som kan være berørt av denne problemstillingen.

Det kan være vanskelig for rettsanvendere å avgjøre om det foreligger en faktisk hindring for bruk av skytjenester innen deres område. Praksisen til tilsynsmyndighetene følger ikke nødvendigvis av ordlyden i regelverket, men ofte fra forarbeider, instrukser og gjennom etablert tilsynspraksis. Disse rettskilder er ikke alltid lett tilgjengelige for virksomhetene. En særlig utfordring oppstår der tilsynsmyndigheter ikke har tatt stilling til behovet for stedlig tilgang til de konkrete servere hvor data lagres og behandles. En usikkerhet rundt dette kan medføre at virksomheter avstår fra å ta i bruk skytjenester også der dette ikke er nødvendig.

Tilsynsmyndigheten kan for eksempel ha hjemmel til å føre tilsyn med *systemer* som benyttes i en virksomhet. Dette burde i utgangspunktet ikke utgjøre et hinder for bruk av skytjenester, med mindre det spesifiseres at det er tale om IKT-systemer, og det foreligger særlige krav til oppbevaring av data for å kunne sikre en viss drift, i tillegg til at tilsynsmyndigheten praktiserer såkalt stedlig tilsyn. Der det ikke finnes krav i lov eller forskrift til oppbevaring av data på bestemte måter, er det vanskelig å foreta noen antagelse om at lovgivningen kan være et rettslig hinder for bruk av skytjenester.

I likhet med innsynsregler i annet lovverk vil ikke en hjemmel til rett på tilgang til dokumenter utgjøre noen utfordring, da innsyn enkelt vil kunne sikres gjennom et systemgrensesnitt mot den aktuelle skytjenesten. Så lenge tilsynsmyndigheten kan få seg forelagt dokumentene og dataene som skal oppbevares, er dette ingen hindring for bruk av skytjenester. Tilsyn med *systemene* som behandler disse kan imidlertid være det, dersom tilsynsmyndigheten fremholder stedlig tilsyn av IKT-systemene som krav.

7. Arbeidsgruppens forslag til tiltak

Under følger en oppsummering av arbeidsgruppens forslag til tiltak og regelverksarbeid som kan iverksettes for å gjøre det lettere for virksomheter som ønsker det å ta i bruk skytjenester. Arbeidsgruppen foreslår både konkrete tiltak innen sektorregelverket vi har gjennomgått, men også mer generelle tiltak for regelverksarbeid.

7.1 Lovgiver bør foreta revisjon av utdatert regelverk

Regelverk som er utdatert vil medføre unødige hindringer for bruk av nye, mer moderne tjenester, på tross av at hensynet bak regelverket kan ivaretas. At teknologien utvikler seg, og ikke alltid gir forutsigbare utfordringer i fremtiden er et viktig hensyn som skal ivaretas ved utviklingen av nytt regelverk. For eksisterende lover som ikke tilrettelegger for nye teknologiske løsninger, vil arbeidsgruppen anbefale at det foretas en revisjon. Revisjonen kan ta for seg de deler av loven hvor en ser de faktiske utfordringene, eller det kan gjennomføres en total revisjon og modernisering dersom dette er nødvendig. Hensikten må være å fjerne unødige hindringer, samtidig som viktige hensyn bevares.

Arbeidsgruppen anbefaler at Kulturdepartementet ser nærmere på behovet for endring i arkivloven § 9 b om utførselsforbud.

Det er antagelig ikke hensiktsmessig å foreta lov- eller forskriftsendring av bokføringsloven eller IKT-forskriften. Vedrørende bokføringsloven vil det imidlertid være aktuelt å avklare forutsetninger og handlingsrom for å utvide listen av land hvor man kan tillate lagring. Det bør vurderes om det er hensiktsmessig å opprettholde begrensningen på oppbevaring av regnskapsmateriale kun til de nordiske stater i forskrifter til bokføringsloven, fremfor innen hele EØS.

Det bør også avklares i hvilken grad det er tilstrekkelig med periodisk sikkerhetskopiering av bokføringsdata til et av landene hvor lagring er tillatt etter forskriften, og hvor ofte slik kopiering eventuelt må foretas.

7.2 Lovgiver bør foreta vertikal og horisontal harmonisering av regelverk

Lovstrukturelle utfordringer medfører uklarheter og usikkerhet for virksomheter. Strukturelle utfordringer i regelverket kan enten løses ved å legge nærmere bestemte normer til grunn for utforming av regelverk (lovteknikk), ved å gjennomgå regelverket enkeltvis (vertikal regulering) eller ved å gi regler som medfører en horisontal harmonisering. Et eksempel på vertikal regulering er finansavtaleloven § 8 om bruk av elektronisk kommunikasjon. Et eksempel på horisontal harmonisering er e-signaturloven § 6 med tanke på godkjent elektronisk signatur.

Tilsvarende kan regelverk som fremstår som fragmentert med tanke på bruk av skytjenester, harmoniseres med et horisontalt regelverk. Eksemplet med ulik definisjon for eksempel av begrepet "varig medium" kan løses horisontalt ved å gi bestemmelser om at med mindre annet uttrykkelig er bestemt, skal alle lagringsmetoder som oppfyller nærmere bestemte vilkår kunne anses som "varig medium". En kombinasjon av vertikal og horisontal regulering av spørsmål knyttet til bruk av skytjenester vil etter arbeidsgruppens syn være å foretrekke.

Forhold som dette bør lovgiver være særlig bevisst på ved utforming av regelverk, og lovgiver bør vurdere å foreta vertikal og horisontal harmonisering av regelverk ved revisjon.

7.3 Det bør utføres en samlet gjennomgang av tilsynspraksis

Arbeidsgruppen anbefaler at det sees nærmere på praktiseringen av stedlig tilsyn, og krav som stilles til dette på tvers av sektorer. Det bør avklares om tilsynsorganene har et reelt behov for fysisk tilstedeværelse hos kontrollobjektene, hva som skal kontrolleres, og hvorvidt tilsynenes behov kan løses på andre måter som også muliggjør bruk av skytjenester. Arbeidsgruppen foreslår at dette utredes samlet for flere sektorer, slik at spørsmålene får en overordnet behandling, og det kan etableres felles praksis. Dette er ikke minst viktig av hensyn til de virksomhetene som forholder seg til flere ulike tilsynsorganer.

Det bør som en del av dette undersøkes om tredjepartsrevisjon vil kunne tilfredsstille behovet for tilsyn og kontroll med offentlige organers arkiver, og med oppbevaringen av finansielle data.

Datatilsynet er et eksempel på et tilsynsorgan som kan godta dokumentasjon fra en tredjepart som bekreftelse på oppfyllelse av personopplysningsloven. En slik tredjepart kan være den databehandleren som den behandlingsansvarlige har avtale med, men det kan også være en revisor som gjennomfører uavhengige kontroller for data-behandleren. Dette kalles ofte tredjepartsrevisjon (revisjon utført av en uavhengig tredjepart). I praksis er det også denne typen kontroll skytjenesteleverandørene åpner for på generelt grunnlag, og det kan være enklere og sikrere enn å gi mange ulike tilsynsmyndigheter tilgang til sine systemer hvor også andre kunders data behandles. Bruken av tredjepartsrevisjon er en løsning som antakelig vil kunne tilfredsstille behovene til flere tilsyn, og som vil kunne gjøre det lettere å utføre tilsyn på tvers av landegrenser. Det bør i en felles utredning vurderes om tredjepartsrevisjon vil kunne tilfredsstille behovet for tilsyn og kontroll med virksomhetene innen de aktuelle regelverkene som omfattes.

7.4 Lovgiver bør begrense geografiske hindringer

Det bør være et mål å hindre at det oppstilles unødvendige geografiske føringer i regelverk, og der disse allerede finnes bør det avklares hvorvidt disse føringene er nødvendige.

Funksjoner i personopplysningsloven vil kunne ha overføringsverdi på flere områder. Som nevnt kan tredjepartsrevisjon være et hjelpemiddel for å fjerne krav om lokal (nasjonal) lagring av data. Personopplysningslovens regler om utførsel av personopplysninger til utlandet vil også kunne gi veiledning til andre sektorer. Både de kontraktsordninger loven henviser til, og godkjenningsordninger for land, gjør behandlingen av personopplysninger enklere i en verden hvor teknologien stadig endrer premisser for behandlingen av data, og hvor tjenestetilbudet blir stadig mer globalisert.

Det bør lages en sammenstilling av beste praksis for praktiseringen av tilsyn og behandling av data som behandles eller lagres i utlandet.

7.5 Lovgiver bør benytte muligheter i regelverket fullt ut

Med tanke på at det er utfordrende å utforme regelverk som fullt ut er teknologinøytralt og tilpasset den løpende teknologiutviklingen, vil arbeidsgruppen anbefale som et utgangspunkt å benytte den forskriftskompetansen som foreligger der det er egnet.

I tillegg anbefaler arbeidsgruppen at det foretas en gjennomgang av vilkår for å gi dispensasjon der lovverk er en hindring for bruk av skytjenester uten at lovens hensyn gir tilstrekkelig begrunnelse.

Arkivloven gir Kongen myndighet til å gi utfyllende forskrifter til loven. Det bør vurderes om det er behov for endring av forskrift om offentlige arkiv, for å tillate lagring av arkiver fra offentlige virksomheter i skyløsninger med servere i utlandet. Riksarkivaren kan i tillegg gi særskilt samtykke til utførsel, og gruppen anbefaler at det utformes vilkår for dette.

Tilsvarende bør det vurderes med grunnlag i dagens lovverk og hensyn om dispensasjonsreglene etter bokføringsloven med forskrifter kan benyttes for å utvide lagringsområdet for bokføringsdata.

7.6 Veiledning i komplisert regelverk

Arbeidsgruppen anbefaler at det vurderes utstrakt veiledning, eventuelt at det utformes sjekklister rundt kontraktsforhold som gjelder bruk av skytjenester innen bank- og finanssektoren.

En ser at det innen anskaffelsesområdet kan være behov for sjekklister og veiledere for anskaffelser av skytjenester. Arbeidsgruppen anbefaler likevel ikke at det utarbeides en egen standardavtale for kjøp av skytjenester spesifikt. Det er imidlertid viktig å ikke hindre slike kjøp gjennom de andre, eksisterende avtalemalene virksomhetene kan velge mellom. Det er viktig at man kan innhente tilbud på løsninger med ulike leveransemodeller innen samme utlysning. Arbeidsgruppens anbefaling er at det gis veiledning i anskaffelsesprosessen slik at utlysninger ikke sperrer for kjøp av skytjenester, og i hvilket avtaleverk som er egnet for de tjenestene virksomheten ønsker å anskaffe.

Arbeidsgruppen anbefaler at rapporten *Legal guide to public cloud sourcing* fra Nordisk Ministerråd oversettes til norsk.

Vedlegg 1: Oversikt over lover og forskrifter arbeidsgruppen har drøftet eller som omtales i rapporten

Arbeidsgruppen har forsøkt å foreta en gjennomgang av all relevant lovgivning innen ansvarsområdet til de deltakende departementer. I tabellen under vil lovene som omtales spesifikt i rapporten nevnes, men gruppen har gjennomgått flere lover enn disse. Dette gjøres det rede for under omtale av hver sektor. På grunn av ulikt omfang på regelverk departementene har ansvar for, har ikke alle departementer hatt mulighet til å foreta en fullstendig, detaljert gjennomgang av eget regelverk. Da er det tatt utgangspunkt i de lover og forskrifter hvor det er antatt det kan foreligge hindringer, blant annet på bakgrunn av kartlegginger av utfordringer knyttet til bruk av skytjenester hos offentlige virksomheter og næringsliv.

Lov eller forskrift som er drøftet eller omtalt	
Arkivloven med forskrift	Hindring i lov og forskrift
Barnehageloven	Ingen klar hindring
Bokføringsloven med forskrifter	Hindring i lov og forskrift
Brann- og eksplosjonsvernloven	Ingen klar hindring
eForvaltningsforskriften	Ingen klar hindring
Ekomloven	Ingen klar hindring
Fagskoleloven	Ingen klar hindring
Finanstilsynslov med tilhørende forskrifter	Hindring i praktisering av lov og forskrift
Folkehøyskoleloven	Ingen klar hindring
Forskningsetikkloven	Ingen klar hindring
Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT)	Hindring i forskrift
Forskrift om håndtering av eksplosjonsfarlig stoff	Ingen klar hindring
Forskrift om landtransport av farlig gods	Ingen klar hindring
Forskrift om sikkerhet ved arbeid i og drift av elektriske anlegg	Ingen klar hindring
Forsøksloven	Ingen klar hindring
Forvaltningsloven	Ingen klar hindring
Inndelingslova	Ingen klar hindring
Kapitalkravsforskriften	Ingen klar hindring
Kommuneloven	Ingen klar hindring
Lov om edb-baserte reservasjonssystemer for passasjertransport	Ingen klar hindring, men særlige krav til tjenestene
Lov om interkommunale selskaper	Ingen klar hindring
Lov om offentlige anskaffelser med forskrifter	Ingen klar hindring
Lov om tilsyn med elektriske anlegg og elektrisk utstyr (el-tilsynsloven)	Mulig hindring i praktisering av lov

Opplæringsloven	Ingen klar hindring
Personopplysningsloven	Ingen direkte hindring
Privatskoleloven	Ingen klar hindring
Produktansvarsloven	Ingen klar hindring
Sikkerhetsloven	Hindring i lov
Sivilbeskyttelsesloven	Ingen klar hindring
Skattebetalingsloven	Ingen klar hindring
Skatteloven	Ingen klar hindring
Skifteloven	Ingen klar hindring
Storulykkeforskriften	Ingen klar hindring
Studentsamskipnadsloven	Ingen klar hindring
Tvangsfullbyrdelseslov	Ingen klar hindring, men kan oppstille en indirekte hindring i lov i særtilfeller
Universitets- og høyskoleloven	Ingen klar hindring
Utdanningsstøtteloven	Ingen klar hindring
Valgloven	Ingen klar hindring
Vergemålsloven	Ingen klar hindring
Verdipapirfondlov	Ingen klar hindring
Verdipapirhandellov	Ingen klar hindring
Voksenopplæringsloven	Ingen klar hindring

Vedlegg 2: Deltagere i arbeidsgruppen

Deltagende departementer er Finansdepartementet (FIN), Justis- og beredskapsdepartementet (JD), Kunnskapsdepartementet (KD), Kommunal- og moderniseringsdepartementet (KMD), Kulturdepartementet (KUD), Nærings- og fiskeridepartementet (NFD) og Samferdselsdepartementet (SD)

Hovedsakelig har disse vært representert ved følgende personer:

Bernhard Eggesbø, FIN, Skattelovavdelingen
Alexander Behringer, FIN, Finansmarkedsavdelingen
Hans Kaiser, JD, Lovavdelingen (avtalerett og kontraktsrett)
Christian Mathiessen, JD, Rednings- og beredskapsavdelingen
Gustav Birkeland, KD, Universitets- og høyskoleavdelingen
Maria Jongers, KUD, Kulturvernavdelingen
Magnar Nordtug, KUD, Kulturvernavdelingen
Steffen Gulbrandsen/Håvard Mork, NFD, Næringspolitisk avdeling
Kurt Arne Sandvik/Knut Aksel Wadet, SD, Luft-, post- og teleavdelingen

Charlotte Elise Thuesen, KMD, avdeling for IKT og fornying
Christine Hafskjold, KMD, avdeling for IKT og fornying
Jesper Tangenes Bæverfjord, KMD, avdeling for IKT og fornying
Mette Bredengen, KMD, avdeling for IKT og fornying
Linn Ising, KMD, Kommunalavdelingen

Arbeidet i den interdepartementale arbeidsgruppen har vært ledet og ført i pennen av Charlotte Elise Thuesen, KMD.

Kontaktperson for arbeidet med en nasjonal strategi for bruk av skytjenester er Christine Hafskjold, KMD.