FØYEN TORKILDSEN
ADVOKATFIRMA

KS FoU-prosjekt 144008:

Utredning av juridiske forhold ved bruk av nettsky i kommunal sektor – en mulighetsstudie

April 2015
Advokatfirmaet Føyen Torkildsen AS

KS FoU

Utredning av juridiske forhold ved bruk av nettskyløsninger i kommunal sektor – en mulighetsstudie

Forord

Bruk av nettskyløsninger er i ferd med å etablere seg i offentlig sektor, men det er fremdeles uklare juridiske forhold ved anskaffelse og bruk. Leverandører av skytjenester er ofte store aktører som leverer standardiserte tjenester. KS-Kommunesektorens organisasjon (heretter KS) har fått henvendelser fra flere kommuner og fylkeskommuner om kommuners bruk av skytjenester, og om det er lovlig og forsvarlig av kommunene å ta slike tjenester i bruk.

Advokatfirmaet Føyen Torkildsen AS (tidligere FØYEN Advokatfirma DA) har i den forbindelse fått i oppdrag å foreta en utredning som skal

> *«beskrive hva dagens lovverk faktisk tillater, hva kommunene faktisk kan ta i bruk av løsninger og hvordan de faktisk kan og bør rigge seg. Utredningen skal også se på om det er behov for endringer i lov- og regelverket, og hvilke endringer dette i så fall bør være.»*

Denne rapporten oppsummerer våre funn og anbefalinger. Særlig vil kommunal sektor ha nytte av de utarbeidede retningslinjene for bruk av skytjenester innen sektoren.

Dette dokumentet er et resultat av en rekke juridiske undersøkelser samt svar på en spørreundersøkelse som har blitt sendt ut til 30 kommuner og enkelte fylkeskommuner. I tillegg har det blitt utført dybdeintervju av tre kommuner og av fire leverandører av skytjenester.

Hovedformålet med dette dokumentet er å gi kommunal sektor forståelse for regelverket rundt skytjenester og gi praktiske råd om hvilke muligheter kommunal sektor har for å ta i bruk skytjenester. Innledningsvis må understrekes at det er et betydelig mulighetsrom for å ta i bruk nettskytjenester, men at dette kan gjøres enda større ved noen endringer i forvaltningspraksis, særlig hos Riksarkivaren.

Selv om denne utredning inneholder en rekke konkrete råd, må man merke seg at enhver situasjon er spesifikk og at utredningen ikke er ment og heller ikke anbefalt som erstatning for profesjonell, juridisk eller annen rådgivning.

Utredning er skrevet av advokatene Arve Føyen, Eva Jarbekk og Siv Owing Maanum.

Innhold

1 Bakgrunn

Advokatfirmaet Føyen Torkildsen AS har av KS fått i oppdrag å foreta en utredning som skal:

> *«..beskrive hva dagens lovverk faktisk tillater, hva kommunene faktisk kan ta i bruk av løsninger og hvordan de faktisk kan og bør rigge seg. Utredningen skal også se på om det er behov for endringer i lov- og regelverket, og hvilke endringer dette i så fall bør være».*

Denne utredningen vil ikke ta for seg alle mulighetene til å ta i bruk skytjenester, da det finnes et stort mulighetsrom for kommunene til å ta i bruk skytjenester. Hovedfokuser i utredningen vil være hva som er til hinder, da det er viktig å være klar over begrensningene i lovgivning ved en eventuell anskaffelse av skytjenester. Denne utredningen har derfor et større fokus på hindringer enn på muligheter.

Det vil i denne utredningen heller ikke bli gjort rede for konkrete systemer kommunen kan og ikke kan ta i bruk, da dette faller utenfor mandatet for denne utredningen.

Noe av bakgrunnen for dette oppdraget er at bruk av nettskyløsninger er i ferd med å etablere seg i offentlig sektor, men mange opplever at det er uklare juridiske forhold ved anskaffelse og bruk. Leverandører av skytjenester er ofte store aktører som leverer standardiserte tjenester, dette innebærer at enkeltkunder i hovedsak må bruke leverandørenes standardavtaler. Dette kan komme i konflikt med krav i norsk regelverk, for eksempel kravene til informasjonssikkerhet i personopplysningsloven og kravet i arkivloven § 9 b om at arkiv ikke kan «..førast ut or landet».

Lagring i skyen betraktes som effektiv på grunn av at det er lett tilknytning, mobilitet, stor skalerbarhet for brukere og hos store leverandører garanteres god sikkerhetskopiering. Men det er ikke helt enkelt å velge skytjenester. Ofte er det reservelagring i annet land/kontinent av sikkerhetsårsaker, og man kjenner ikke alltid til hvilke(t) land dette er. Leverandør disponerer hele skyen og flytter data etter behov, noe som medfører lagring i andre land (transborder data flow), uten at oppdragsgiver vet hvor dataene befinner seg. Selv om lagring i skyen selges inn som «raskt, rimelig og trygt», kan det likevel være vanskelig å vite hvordan en i forbindelse med etablering av bruk av skytjenester skal forholde seg til personopplysningsloven, sikkerhetsloven, arkivloven og annen lovgivning.

Levering av databehandlingstjenester fra eksterne tjenesteleverandører er egentlig ikke noe nytt. Det har eksistert siden 1950-tallet i forskjellige former og under forskjellige navn. De tekniske og juridiske problemstillingene som oppstår ved bruk av tradisjonelle eksterne driftstjenester, er langt på vei de samme også ved bruk av skytjenester. Noen problemstillinger blir imidlertid mer fremtredende ved bruk av skytjenester.

Videre i denne utredningen vi vi først gi et sammendrag av våre funn, før vi går mer detaljert inn på tematikken for denne utredningen.

2 Sammendrag av utredningen

2.1 Innledning

Hovedformålet med rapporten er å gi kommunal sektor forståelse for regelverket rundt skytjenester og gi praktiske råd om hvilke muligheter kommunal sektor har for å ta i bruk skytjenester. Innledningsvis må understrekes at det er et betydelig mulighetsrom for å ta i bruk nettskytjenester, men at dette kan gjøres enda større ved noen endringer i forvaltningspraksis, særlig hos Riksarkivaren.

Under denne utredningen har det blitt fokusert på hva dagens lovverk ikke tillater, og hva kommunene faktisk kan og bør gjøre for å oppfylle kravene i gjeldende lovgivning hvis de ønsker å bruke skytjenester. Videre tar rapporten for seg hvorvidt det er behov for endringer i lov-regelverk, og hvilke endringer i så fall dette bør være.

Skytjenester er en samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett. Det er vanlig å skille mellom Software som tjeneste (Software as a Service), Plattform som tjeneste (Platform as a Service) og Infrastruktur som tjeneste (Infrastructure as a Service). Disse tjenestene kan leveres i form av offentlig tilgjengelig sky (Public Cloud), privat tilgjengelig sky) Private Cloud – benyttes innenfor en bedrift eller et konsern), eller en hybrid sky (Hybrid Cloud – som er en kombinasjon av de to andre leveranseformene). De juridiske og informasjonssikkerhetsmessige problemstillingene vil langt på vei være de samme, uavhengig av tjeneste- eller leveranseform, selv om de konkrete vurderingene og tiltakene som må iverksettes kan være forskjellige.

2.2 Juridiske utgangspunkter

Felles for større anskaffelser innenfor både outsourcing av IT og skytjenester er at det er en rekke juridiske rammebetingelser som skal oppfylles. Spesielt skytjenester er for mange virksomheter «upløyd mark», og man vet ikke alltid hvilke forhold som skal vektlegges og dermed heller ikke hvor mye tid og innsats som må settes av til å gjøre de nødvendige vurderinger. I tillegg møter man ofte store leverandører med sterk markedsposisjon og ofte også en sterk overbevisningskraft.

Hensikten med denne utredningen var å undersøke hvilke lover som *er* til hinder, eller som *oppleves* som et hinder for bruk av skytjenester, og hvorvidt det er behov for endringer i lovgivningen.

Skytjenester har berøringspunkter med flere regelverk og reiser derfor flere komplekse juridiske problemstillinger.

Rapporten tar for seg både forvaltningsloven, Lov om offentlige anskaffelser og GPA-avtalen, reglene om vern av personopplysninger, sikkerhetsloven, bokføringsloven og arkivloven. Den største juridiske utfordringen knytter seg til arkivloven og bokføringsloven. De øvrige regelverkene er i utgangspunktet ikke til hinder for bruk av skytjenester i kommunal sektor, men de stiller konkrete krav som må oppfylles.

Det er viktig å påpeke at kommunene, før de tar i bruk en konkret skytjeneste, må foreta en tilstrekkelig risikovurdering i henhold til personopplysningsloven og personopplysningsforskriften. Det er også viktig at kommunene sikrer at de inngår en tilstrekkelig databehandleravtale med leverandøren av skytjenesten. Hva kommunene bør

sikre at er regulert i en slik databehandleravtale fremgår av retningslinjene i den endelige rapporten.

Arkivloven

I følge arkivloven (LOV-1992-12-04-126) § 9 bokstav b er utgangspunktet at offentlig arkivmateriale ikke kan føres ut av landet uten etter særskilt samtykke fra Riksarkivaren. Denne bestemmelsen får stor betydning for kommunens adgang til å ta i bruk skytjenester.

Det kan stilles spørsmål ved i hvilken grad denne bestemmelsen - herunder unntakene – ut fra det opprinnelige formålet med bestemmelsen passer på, og får anvendelse på bruk av skytjenester levert fra utlandet. Denne regelen ble til for mer enn 20 år siden – det vil si i god tid før skytjenester i dagens form, eller databehandling og lagring i utlandet var en realitet.

Riksarkivet rettet i september 2014 en henvendelse til Kulturdepartementet vedrørende lagring av elektroniske arkiver på servere i utlandet. Der fremgår det at Riksarkivet mener at på bakgrunn av arkivloven § 9 bokstav b, kan arkiver ikke lagres på servere som befinner seg utenfor Norges grenser. Dette gjelder også sikkerhetskopier av arkiver. Slik regelverket er i dag, er det således, i følge Riksarkivets tolkning ikke mulig å bruke skytjenester for å lagre arkivverdig materiale. Så lenge arkivet og sikkerhetskopien av arkivet befinner seg i Norge, kan imidlertid andre kopier av arkivet befinne seg i utlandet.

Denne uttalelsen fra Riksarkivet er etter vår oppfatning noe inkonsekvent, når de vurderer det slik at arkivmaterialet ikke kan føres ut av landet. I arkivloven § 9 som Riksarkivet viser til, fremgår det at Riksarkivaren kan gjøre unntak gjennom samtykke. Dette innebærer at Riksarkivaren faktisk *kan* samtykke til at arkiv føres ut av landet.

Datatilsynet var opprinnelig skeptisk til bruk av skytjenester, men har etter hvert gjort seg kjent med teknologien og har gått over til å sette fornuftige kriterier for hvordan teknologien skal brukes. Vi mener Riksarkivaren har et juridisk handlingsrom for å velge en tilsvarende tilnærming. At Riksarkivaren velger å ikke benytte denne muligheten vurderes å være lite heldig, særlig med tanke på at formålet med denne bestemmelsen i arkivloven var å sikre at dataene ikke går tapt for ettertiden. Det kan gjøres på tilfredsstillende måte ved at det stilles krav i tilknytning til bruk av skytjenester.

Bokføringsloven

Bestemmelsene i Bokføringsloven om oppbevaring av regnskapsmateriale får anvendelse også på regnskapsmateriale i kommuner og fylkeskommuner jf. Forskrift om årsregnskap og årsberetning (for kommuner og fylkeskommuner) FOR-2000-12-15-1424 § 2.

I henhold til bokføringsloven § 13 annet ledd, skal som hovedregel regnskapsmaterialet oppbevares i Norge. Dette er med på å begrense muligheten til å bruke skytjenester, hvor leverandørene ikke har servere plassert i Norge. Det finnes imidlertid enkelte unntak, bokføringsmateriale kan oppbevares i Danmark, Sverige, Finland og Sverige, samt i andre land ved dispensasjon fra Skattedirektoratet.

Til tross for unntakene, vil bokføringsloven fort være til hinder for bruk av enkelte typer skytjenester. Noe av grunnen til dette er at de store leverandørene ofte ikke tilbyr mulighet for å oppbevare opplysningene i de ovennevnte EØS landene, men på servere andre steder i verden. I tillegg er Skattedirektoratet restriktive med å gi dispensasjon.

2.3 Hovedfunn i intervjuer – kommuner

Under denne mulighetsstudien har det blitt foretatt dybdeintervju av Alta, Narvik og Moss kommune. På bakgrunn av disse intervjuene er det klart at kommunene har ulikt syn på bruk av skytjenester.

Blant annet vurderte Alta kommune det som for dyrt å ta i bruk skytjenester, fordi ikke alt kunne flyttes i nettskyen, og IT-avdelingen i kommunen ønsker å ha fokus på drift og stabilitet av IT-systemene. Det var også stor skepsis til bruk av skytjenester på grunn av overføring av data til andre land.

Narvik kommune har derimot i stor grad tatt i bruk skytjenester, og bruk av skytjenester er en del av kommunen sin strategi. Det fremgår blant annet av deres strategi at bruk av internettbaserte tjenester skal vurderes når det er hensiktsmessig og kostnadsbesparende. Det skilles i kommunen mellom hva som kan legges i skyen og ikke, sensitive personopplysninger skal ikke behandles i skyen.

Driverne for at Narvik kommunen har tatt i bruk skytjenester er; økonomi, standardisering, skalerbarhet, ressursdeling og fleksibilitet.

Moss kommune har lagt store deler av sine systemer ut i nettskyen og de mener at på kort sikt er det ikke rimeligere å gå over til nettsky, men at det på lang sikt vil lønne seg. For å kunne gjennomføre prosjektet har kommunen hatt en tett dialog med Datatilsynet underveis. De mener at det største hinderet for å ta ut full gevinst ved bruk av skytjenester er arkivloven.

For å kunne gå over til nettskyen har det løpende blitt foretatt risikovurderinger av de enkelte elementer som flyttes etter hvert som de i større og større grad har tatt i bruk nettskyløsninger.

2.4 Hovedfunn intervjuer – leverandører

I forbindelse med denne mulighetsstudien har det også blitt gjennomført dybdeintervju av fire leverandører av skytjenester; Evry, Microsoft, Visma og Google Norway.

Leverandørenes hovedsynspunkt var at det var stor variasjon i kommunene i forhold til hvor bevisste kommunene er rundt bruk av skytjenester og at det er varierende forståelse av hva som ligger i begrepet skytjenester. Enkelte av leverandørene mener at det er mye usikkerhet og ubegrunnede oppfatninger i kommunene vedrørende lovligheten av bruk av skytjenester og at dette i hovedsak skyldes frykt, usikkerhet og tvil. Usikkerheten rundt bruk av skytjenester har ikke nødvendigvis grunnlag i hvorvidt lovgivningen tillater bruk av skytjenester eller ikke.

Leverandørene ga også klart uttrykk for at de ønsker å levere skytjenester til kommunene, og at de i enda større grad kommer til å gå over til å levere tjenester basert på nettsky. I dag legges det ut veldig få offentlige anbud som tilrettelegger for at leverandørene kan tilby sine skytjenester. Slik konkurransegrunnlagene er utformet, vil det være umulig eller svært vanskelig for de enkelte kundene å sammenligne prisene for skytjenester med IKT-tjenester basert på en mer tradisjonell plattform. Dette gjør det vanskelig for leverandørene å kunne tilby skytjenester ved offentlige anbud. Leverandørene ser imidlertid at det har begynt å skje en utvikling på dette området, særlig i de anbudene hvor kunden etterlyser funksjonalitet i stede for tekniske krav.

Videre påpeker leverandørene at ut i fra regelverket så er det i hovedsak arkivloven som er det største problemet, dette er blant annet en av grunnene til at et par av leverandørene satser på lagring i Norge i stede for i andre land.

2.5 Retningslinjer for bruk av skytjenester

Utredningen inneholder også retningslinjer for hvilke vurderinger som må gjøres ved bruk av skytjenester, herunder; personopplysningslovens krav til vurdering av dataene som skal legges ut og risikoanalyser som må gjennomføres, krav til sikkerhet, avveining av risiko, vurdering av landrisiko etc.

Retningslinjene spesifiserer blant annet hva en må tenke på i den forberedende fasen og ved inngåelse av avtale ved anskaffelser av skytjenester. Videre hvilke forhold en særlig bør være oppmerksom på vedrørende personvern og bruk av skytjenester.

Retningslinjene går også inn på hvilke typer informasjon som vanligvis kan være aktuelle å legge inn i en nettskytjeneste, som for eksempel opplysninger av intern administrativ karakter i kommunen.

Også personopplysningslovens krav til å etablere og etterleve et internkontrollsystem og sikkerhetsløsninger blir nærmere gjennomgått. Blant annet at det må etableres et system for informasjonssikkerhet, videre må det settes mål for informasjonssikkerheten, hvilket sikkerhetsnivå man skal ha og hvordan bedriften skal arbeide med risikohåndtering. Hvis virksomheten skal ta i bruk nettskyen for tjenester, må systemet for informasjonssikkerhet omfatte vurderinger og tiltak som også omfatter skytjenesteleverandøren med eventuelle underleverandører – slik at hele kjeden av leverandører og ikke minst underleverandører er dekket.

Retningslinjene inneholder også en matrise for risikovurdering, blant annet et eksempel på en risikotabell og eksempel på en risikovurdering.

Disse retningslinjene er utarbeidet som et hjelpeverktøy for kommunene som kan brukes både i forberedelsene og ved gjennomføringen av anskaffelsen av skytjenester.

2.6 Oppsummering

Det er klart at det er et betydelig mulighetsrom for å ta i bruk nettskytjenester i kommunal sektor, men dette kan gjøres enda større ved noen endringer i forvaltningspraksis, særlig hos Riksarkivaren. Når man skal vurdere å ta i bruk nettskytjenester, så er det en rekke vurderinger som må gjennomføres.

Det første man må gjøre, er å kartlegge hvilke regelsett som er relevant for de opplysningene som skal legges ut. Slik arkivloven og bokføringsloven tolkes i dag, er det lettest å legge ut opplysninger som ikke omfattes av disse regelverkene. Dersom disse myndighetene endrer praksis, vil omfanget av opplysninger som kan legges i skyen, øke.

3 Generell introduksjon

3.1 Innledning

I dette kapittelet vil vi kort gjøre rede for noen nøkkeldefinisjoner og forklare enkelte begreper og ord som vil bli brukt i denne utredningen. Det vil også bli redegjort for behovet for utredningen og vi vil gå nærmer inn på hva nettskytjenester er, hvilke tjenester som finnes og forskjellen på nettskytjenester og tradisjonelle IKT-tjenester.

3.2 Nøkkeldefinisjoner og forklaringer

I denne rapporten vil vi benytte en rekke ulike begreper, som vi kort har definert/beskrevet i dette punktet. I den grad det finnes lovbestemte definisjoner vil disse bli benyttet.

- Behandling av personopplysninger: enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.

- Behandlingsansvarlig: den personen/selskapet/kommunen som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Kategoriseringen av «behandlingsansvarlig» og «databehandler» (jf. under) kan være vanskelig, og det er vesentlig forskjellige rettslige krav som gjelder avhengig av om en part er «behandlingsansvarlig» eller «databehandler».

- Databehandler: enhver person/selskap/kommune, annet enn ansatte hos den behandlingsansvarlige (eller at den behandlingsansvarlige har adgang til å instruere), som behandler personopplysninger på vegne av behandlingsansvarlig.

- Offshoring: Bruk av menneskelige ressurser, som oftest fra lavkostland med rimelige timepriser, til å utføre ulike tjenester innen data

- Overføring av personopplysninger: enhver overføring fra behandlingsansvarlig til en annen person/selskap/kommune/juridisk enhet.

- Overføring til utlandet: enhver overføring av personopplysninger til land utenfor Norges landegrenser og behandling av personopplysninger fra utlandet selv om opplysningene befinner seg lagret i Norge (typisk offshoring). Kalles «transborder data flow» på engelsk.

- Personopplysning: opplysninger og vurderinger som kan knyttes til en enkeltperson

- Sensitive personopplysninger: opplysninger om rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning. Opplysninger om at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, helseforhold, seksuelle forhold, medlem i fagforeninger.

- Skytjenester: er samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett. Det er vanlig å skille mellom Software som tjeneste (Software as a Service), Plattform som tjeneste (Platform as a Service) og Infrastruktur som tjeneste (Infrastructure as a Service). Disse tjenestene kan leveres i form av offentlig tilgjengelig sky (Public Cloud), privat tilgjengelig sky) Private Cloud – benyttes innenfor en bedrift eller et konsern), eller en hybrid sky (Hybrid Cloud – som er en

kombinasjon av de to andre leveranseformene). Vi kommer nærmere inn på innholdet i disse i punkt 15. De juridiske og informasjonssikkerhetsmessige problemstillingene vil langt på vei være de samme, uavhengig av tjeneste- eller leveranseform, selv om de konkrete vurderingene og tiltakene som må iverksettes kan være forskjellige.

3.3 Behovet for denne utredningen

Denne utredningen er utarbeidet for å bidra til å skape et grunnlag for bruk av skytjenester i kommunal sektor.

Det er i dag en opplevd usikkerhet om lovligheten ved bruk av skytjenester. En av hovedgrunnene til dette er at leverandørene av skytjenester ofte er virksomheter etablert i mange land, med internett som underliggende bæretjeneste for levering av tjenesten. Databehandlingsressursene som benyttes er i mange tilfelle lokalisert fysisk utenfor Norge og utenfor Europa. Dette innebærer at data blir lagret utenfor Norge, og dette skaper blant annet usikkerhet i forhold til arkivloven hvor det fremgår at arkiv ikke skal «førast ut or landet», og i forhold til personopplysningslovens krav om at personopplysninger bare kan overføres til land, eller ved hjelp av rettslig bindende instrumenter, som sikrer «adequate level of data protection».

Ofte er det også reservelagring i andre land/kontinent av sikkerhetsårsaker, og man kjenner ikke alltid til hvilke(t) land dette er. Leverandøren disponerer «hele skyen» og «flytter data rundt» etter behov og uavhengig av landegrenser (transborder data flow), uten at kunden vet hvor dataene befinner seg.

Det er viktig å vite hvor dataene faktisk er lagret, ettersom det i utgangspunktet er lovverket i det landet der serveren står, som gjelder for dataeiers tilgang til dataene. Det er ikke alltid at regler om innsyn, skjerming og personvern; deling eller salg av data; styresmaktenes rett til å vite; ansattes integritet og ærlighet eller dataeiers rett til tilgang til egne data er i tråd med de lover og regler som gjelder i Norge.

Bruk av nettsky kan bidra til kostnadseffektivitet og fleksibilitet, blant annet fordi en kun betaler for faktisk bruk. I stedet for at kommunen må kjøpe servere selv, kan kommunen leie kapasitet og tjenester etter behov, og bare betale for den kapasiteten og de lisensene som til enhver tid forbrukes. I tillegg kan en ved bruk av skytjenester kjøpe de tjenestene man ønsker og for den perioden det er ønskelig med de aktuelle tjenestene, i stedet for å kjøpe lisenser, installere og drifte selv. Dette kan gi en forutsigbarhet for kommunene i forhold til driftskostnader.

Selv om lagring i skyen selges inn som raskt, rimelig og trygt kan det likevel være vanskelig i forhold til personopplysningsloven, sikkerhetsloven, arkivloven og annen lovgivning. Hvordan kan kommuner og fylkeskommuner velge riktig?

Det er grunnleggende at virksomheter som tar i bruk skytjenester fremdeles er juridisk ansvarlig for bruk av tjenestene, selv om man får bistand fra en ekstern leverandør. Virksomheten må derfor sørge for at personopplysninger og annen informasjon og dokumenter mv som skal behandles konfidensielt, håndteres i henhold til personvernregelverket, og annet relevant regelverk som gir anvisning på taushetsplikt, og fortrolig behandling av relevante opplysninger.

Det mest sentrale og relevante for kommuner, vil være det man ofte kaller Software as a Service. Dette er den mest komplekse tjenesten, og den vil gjerne omfatte de to andre hovedtypene av tjenester (Platform as a Service og Infrastructure as a Service).

En stor utfordring for kommuner som bruker slike tjenester er å sørge for at avtalen med leverandøren er i samsvar med norsk lovgivning, slik at gjeldende krav i norsk lovgivning til behandling av opplysninger og sikkerhet til enhver tid kan oppfylles.

På bakgrunn av dette er det viktig å kartlegge kommunesektorens adgang til å benytte seg av skytjenester.

3.4 Hva skiller skytjenester fra tradisjonelle IKT-tjenester

Skytjenester innebærer en dynamisk tilgang til skalerbare IT-ressurser levert som en tjeneste over internett, ved behov. Normalt leveres tjenestene som standardiserte tjenester med betaling etter bruk.

Skytjenester innebærer i stor grad leveranse av samme type tjenester som tradisjonelle IKT-tjenester sett fra kundesiden. Forskjellen ligger i hovedsak i forretningsmodellen, samt styring og eierskap til det som inngår i forretningsmodellen. Videre leveres gjerne skytjenester på tvers av landegrenser. Dette er imidlertid ikke nødvendigvis alltid tilfellet, og flere leverandører reklamerer nå med at de leverer «norske», eller «europeiske» skytjenester.

Tradisjonelle IKT-tjenester innebærer derimot at en virksomhet har behov for å kjøpe servere (eller serverkapasitet og lagring). Dette gjøres normalt ved at man enten kjøper eller leaser et antall servere med betydelig mer kapasitet enn man til enhver tid benytter(eller leier server- eller lagringskapasitet av et visst omfang). Videre kjøper man også gjerne lisenser for programvare til et nærmere angitt brukere (ofte må man kjøpe i «blokker» à 10, 50 eller andre bestemte angitte antall av lisenser, og man betaler ofte mer enn det som rent faktisk blir benyttet til enhver tid). Skytjenester er derimot kjennetegnet ved at de ressursene som benyttes (Plattform, Infrastructure og Software) er laget for dynamisk skalering. Dette innebærer at en svært ofte kan ta i bruk tjenester og skalere opp og ned ved bruk av selvbetjeningsløsninger over internett. Det innebærer at datakraft kan tilpasses kapasitetsbehov, og kunden betaler bare for de ressursene som til enhver tid faktisk blir benyttet.

En annen forskjell er at tradisjonelle IKT-tjenester i større grad kan tilpasses etter ønskene fra den enkelte bedrift/kommune (spesialtilpasning), mens skytjenester normalt kjøpes som et ferdig produkt, hvor en f.eks. underveis på en svært fleksibel måte kan legge til ytterligere tjenester/applikasjoner.

De tradisjonelle IKT-tjenester stiller større krav til kommunenes IT-kompetanse, og avhengig av kompleksiteten ved kommunenes IT-infrastruktur vil det være et større behov for eget eller innleid IT-personell. Ved bruk av skytjenester derimot vil det ikke være behov for å bruke like mye ressurser på IT-personell, og det vil være behov for personell med en noe annerledes kompetanse (bestiller- og administrasjonskompetanse).

En annen hovedforskjell er organiseringen av data. Ved bruk av skytjenester kan data flyte rundt mellom ulike driftssentre mens for tradisjonelle IKT-tjenester er dataene lagret på dedikert(e) server(e). Det at dataene ikke ligger lagret på dedikerte servere, kan by på juridiske utfordringer, særlig fordi mange av de store skyleverandørene har datasentre plassert utenfor EU.

3.5 Ulike former for skyløsninger

Det nærmeste man kommer en offisiell definisjon på "skytjenester", er antakelig definisjonen fra den amerikanske offentlige etaten NIST (National Institute of Standards and Technology - underlagt det amerikanske Handelsdepartement)[1] hvor skytjenester beskrives slik:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Definisjonen fra NIST lister i tillegg opp 5 essensielle karakteristika for skytjenester:

- Selvbetjening etter eget behov («on-demand»)
- Bred anlagt nettverkstilgang for både tynne og tykke klientplattformer (mobiltelefoner, lesebrett, PC, mv.)
- Dynamisk ressurssamhandling (både mellom fysiske og virtuelle ressurser hver for seg og hverandre)
- Hurtig elastisitet, dvs rask behovsbasert utvidelse/innskrenkning av ytelser
- Målt og optimalisert tjenesteyting bl.a. som grunnlag for transparent kostnadsbilde for både kunde/forbruker og leverandør

Skytjenester kan videre deles opp i *tjenestemodeller*. De 3 vanligste er:

- "Software as a Service" (SaaS), som er en modell for leveranse av programvare over et nettverk hvor kunden benytter leverandørens applikasjon(er) på en nettsky-infrastruktur. Kunden har i utgangspunktet ikke kontroll over hverken applikasjoner, nettverk, servere, operativsystemer eller lagringsmuligheter.
- "Platform as a Service" (PaaS) hvor kunden innfører applikasjoner utviklet/kjøpt av kunden i leverandørens nettsky-infrastruktur gjennom å benytte programmeringsspråk og verktøy støttet av leverandøren. Kunden har kontroll over egne applikasjoner, men har ikke kontroll over nettverk, servere, operativsystemer eller lagringsmuligheter.
- "Infrastructure as a Service" (IaaS) som gjelder levering av datainfrastruktur som en tjeneste over et nettverk. Kunden har kontroll over relevante applikasjoner, servere, operativsystemer og lagringsmuligheter, samt i noen tilfeller visse elementer i nettverket (f.eks. på brannmur-siden).

Man kan også se for seg flere andre tjenestemodeller eller varianter av ovenstående, f.eks.:

- Lagring som tjeneste
- Databasehosting som tjeneste
- Informasjon som tjeneste
- Prosessering som tjeneste

[1] Siste versjon av NISTs definisjon er fra september 2011, og finnes i sin helhet på: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

- Integrasjon som tjeneste
- Sikkerhet som tjeneste
- Styring/ledelse som tjeneste
- Testing som tjeneste

Skytjenester kan i tillegg deles inn etter *leveransemodeller* («deployment models»), herunder:

- «Public cloud», hvor skytjenestene gjøres tilgjengelige av leverandøren for alle kunder.
- «Private cloud», hvor skytjenestene gjøres tilgjengelige kun for de virksomheter som skytjenestene skal gjelde for. Her vil miljøet/miljøene som skytjenesten leveres fra, typisk dedikeres til den enkelte kunde eller en definert kundegruppe. Dette opplegget åpner ofte for større grad av spesifikke kundetilpasninger enn tilfellet er med «public cloud»-modellen.
- Det kan også tenkes varianter av modellene over, for eksempel en blanding av «public cloud» og «private cloud» – såkalt «hybrid cloud».

Ofte er virksomheten (kunden) og leverandøren av skytjenester etablert i forskjellige land, slik at det mellom disse aktører skjer en overføring av informasjon over landegrenser. I mange tilfeller vil også leverandøren av skytjenester benytte seg av dataressurser i ulike fysiske og geografiske lokasjoner, både innenfor et enkelt land og på tvers av landegrenser. Dette gjøres ofte av praktiske årsaker nettopp som et ledd i å optimalisere den dynamiske samhandlingen mellom ressursene, og for å kunne tilby kundene et skalerbart og sammensatt sett av tjenester.

Prinsipielt er det imidlertid ingenting i veien for å avgrense leveransen av skytjenester rent geografisk. Her kan eksempelvis tenkes en «private cloud» satt opp med geografiske avgrensninger etter kundens spesifikasjoner. Teoretisk sett er det derfor mulig for en norsk virksomhet å bestille skytjenester fra en norsk leverandør basert i Norge, uten at noe av informasjonen forlater Norge. Ettersom det finnes en rekke særregler forbundet med overføring av ulike data over landegrenser, vil eventuell muligheter for geografisk avgrensning kunne ha stor betydning for valg av strategi ved virksomhetens anskaffelse av skytjenester. Flere norske leverandører bruker som salgsargument at de tilbyr skytjenester hvor dataene blir lagret på servere i Norge.

Generelt kan det tilføyes at begreper som «skytjenester», «nettskyløsninger» og «cloud» kan bli oppfattet som noe diffuse, og selve ordlyden kan skape inntrykk av å innebære en uoversiktlig situasjon for kunden.

En annen sak er at skytjenester har berøringspunkter med flere regelverk og kan reise flere komplekse juridiske problemstillinger. Dette diskuteres nærmere i det følgende.

3.6 Oppsummering

Som vi har sett i dette kapittelet finnes det en rekke ulike skytjenester, og begrepene som kan bli brukt om skytjenester kan bli oppfattet som diffuse. Spørreundersøkelsen i kommunene som er gjennomført viser også at det er usikkerhet rundt hva skytjenester er og hva som ligger i dette begrepet.

4 Oppsummering av spørreundersøkelsen og dybdeintervjuene

4.1 Innledning

I forbindelse med denne utredningen har det blitt sendt ut en spørreundersøkelse til 30 kommuner og enkelte fylkeskommuner. I tillegg har det blitt gjennomført dybdeintervju av 3 kommuner og av fire leverandører av skytjenester.

Spørreundersøkelsen og dybdeintervjuene har blitt gjennomført for å kartlegge kommunenes bruk av skytjenester, samt deres behov og vurderinger av kommunenes adgang til å benytte nettskytjenester. Spørreundersøkelsen og dybdeintervjuene danner noe av grunnlaget for de videre drøftelsene i denne utredningen.

4.2 Resultater

Oppsummeringsvis viser svarene på disse undersøkelsene at det er meget stor forskjell i kunnskapsnivå på både det juridiske rammeverket og på hva skytjenester er rent faktisk/teknisk.

Noen kommuner fremsetter en sterk skepsis mot at opplysningene er tilgjengelig i nettskyen fordi man vurderer at det åpner for at andre lands myndigheter kan skaffe seg tilgang til opplysninger.

Samtidig er det åpenbart at det eksisterer diametralt ulike oppfatninger om hvorvidt det er hensiktsmessig og ønskelig å benytte skytjenester. Det er også interessant at mange mener det nok er penger å spare på å bruke skytjenester, samtidig som det faktisk er sterkt divergerende oppfatninger om også dette.

Det er også verdt å merke seg at flere understreker at når man har tatt i bruk nettskytjenester, så har dette fungert bra, både teknisk og opplæringsmessig for brukerne.

Flere oppgir at de synes at myndighetene ikke veileder så godt som man skulle ønske på hvordan nettskytjenester kan brukes. De som har tatt tjenestene i bruk først, har brukt store beløp på konsulenttjenester, noe som antakelig neppe er like nødvendig for de som kommer etter.

En nærmere redegjørelse av funnene i spørreundersøkelsen og dybdeintervjuene fremgår av vedlegg 4 til denne utredningen.

5 Overordnede juridiske rammebetingelser som må tas i betraktning ved bruk av skytjenester

Felles for større anskaffelser innenfor både outsourcing av IT og skytjenester er at det er en rekke juridiske rammebetingelser som skal oppfylles. Spesielt skytjenester er for mange virksomheter «upløyd mark», og man vet ikke alltid hvilke forhold som skal vektlegges og dermed heller ikke hvor mye tid og innsats som må settes av til å gjøre de nødvendige vurderinger. I tillegg møter man ofte store leverandører med sterk markedsposisjon og ofte også en sterk overbevisningskraft.

Manglende etterlevelse av rettslige krav og pålegg fra myndigheter kan få alvorlige følger for de involverte virksomheter, eksempelvis:

- Eksponering av økonomisk risiko, for eksempel på grunn av forsinkelser i berørte prosjekter mv.
- Skade på virksomhetens rennommé
- Inngripen fra myndigheter
- Mulige erstatningssøksmål

På denne bakgrunn anbefales det på generelt grunnlag at den anskaffende virksomheten anlegger et helhetlig perspektiv fra planleggingen av anskaffelsen helt til tjenestenes opphør. Dette innebærer blant annet følgende:

- Nødvendige analyser i forkant som grunnlag for behov og kravstilling, herunder eksempelvis:
  - Risikovurderinger
  - Identifisere hvilke tjenester som er nødvendige/ønskelige
  - Identifisering av data som er i scope
  - Identifisere dataflyt
- Gjennomføring av anskaffelsesprosess i henhold til gjeldende regelverk (f.eks. lov og forskrift om offentlige anskaffelser), herunder eksempelvis:
  - Nærmere vurderinger av landrisiko for de aktuelle tilbydere
  - Valg av kontraktsmodell og –vilkår (avtalte tjenestenivåer (SLA), ansvarsfordeling mv.)
- Oppfølging i perioden for tjenesteytelser
- Etterlevelse av regulering om hva som skal skje ved opphør/exit

En spesiell utfordring er skytjeneste-leverandørenes ofte sterke markedsposisjon og teknologiske overtak, som bl.a. har bidratt til at de ofte tilbyr tjenester på basis av standardvilkår som ofte er ensidig og er utformet til deres egen fordel, og som de krever lagt til grunn uten at det gis noe realistisk rom for forhandlinger eller endringer.

Det finnes også flere eksempler på at leverandøren tilbyr kun standardiserte løsninger uten rom for individuelle tilpasninger eller variasjoner på applikasjonene eller driftsløsninger og avtalte tjenestenivåer. Tilsvarende ser man ofte standardiserte leveransevilkår der tjenestene leveres «as is», uten garantier eller rom for kompensasjon for sviktende leveranser. En ansvarsbevisst innkjøpsorganisasjon må være forberedt på den type motstand og ha strategien klar for hvordan man skal sikre sine interesser.

I punkt 6.2 vil nærmere bestemte områder som er spesielt relevante for skytjenester innenfor flere regelsett drøftes mer inngående.

Problemstillinger knyttet til sikkerhetsgradert informasjon i henhold til sikkerhetsloven med forskrifter er skilt ut i eget punkt 6.4 nedenfor.

6 Oversikt over relevant lovgivning og hovedutfordringer ved bruk av skytjenester

6.1 Innledning

I kapittelet over har vi sett at det er ulike rammebetingelser en kommune må ta hensyn til ved bruk av skytjenester.

Hensikten med denne utredningen er å undersøke hvilke lover som er til hinder, eller som oppleves som et hinder for bruk av skytjenester, og hvorvidt det er behov for endringer i lovgivningen.

Skytjenester har berøringspunkter med flere regelverk og reiser derfor flere komplekse juridiske problemstillinger. Dette vil det bli sett nærmere på i det følgende.

I dette kapittelet vil det bli gjort rede for følgende:

- Hvilken lovgivning som begrenser bruk av nettskyløsninger – og på hvilken måte
- På hvilken måte tillater lovgivningen bruk av nettskyløsninger, og på hvilke vilkår

I det følgende vil det bli redegjort nærmere for det relevante regelverket.

6.2 Utvalgt regelverk i kommunal sektor

6.2.1 Forvaltningsloven

Forvaltningsloven retter seg i først hånd mot saksbehandlingen i forvaltningen. Også leverandørene til norsk offentlig forvalting må i sine leveranser imidlertid etterleve forvaltningslovens (fvl.) bestemmelser om taushetsplikt, jf. fvl. §§ 13 flg.

Taushetspliktens omfang og unntak fra denne, gjelder dermed også for eventuelle leverandører av skytjenester til det offentlige, som etter dette blant annet må *«hindre at andre får adgang eller kjennskap til det han i forbindelse med tjenesten eller arbeidet får vite om […] noens personlige forhold, eller […] tekniske innretninger og fremgangsmåter samt drifts- eller forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde av hensyn til den som opplysningen angår.»*

Forvaltningsloven setter i utgangspunktet ingen begrensninger i adgangen til å benytte seg av skytjenester. Derimot innebærer reglene om taushetsplikt at kommunen ved anskaffelse av skytjenester, må sørge for å ilegge leverandørene en taushetsplikt både når det gjelder innholdet i avtalen samt informasjonen leverandørene får innsyn i.

6.2.2 Lov om offentlige anskaffelser og GPA-avtalen

Norske kommuner er bundet av anskaffelsesregelverket samt av GPA-regelverket. GPA-regelverket legger begrensninger på i hvilken grad man kan hindre medlemslandene i å tilby tjenester, altså slik at en norsk kommune vanskelig kan stille vilkår om at det ikke skal brukes ressurser fra enkelte GPA-land. GPA-regelverket er således ikke noen hinder for bruk av skytjenester.

Hva gjelder regelverket om offentlige anskaffelser, arbeider DIFI med hvordan skytjenester kan anskaffes og vi går derfor ikke nærmere inn på dette her. Forhold som blant annet må belyses nærmere er:

- Hvordan man skal vurdere anskaffelsesgrensene når man kjøper en tjeneste som er «pay per use».
- Hvordan man spesifiserer det man skal ha. Det er viktig at man spesifiserer på funksjon, slik at man ikke utelukker noen teknologiske plattformer fra starten av.
- Hvilke tildelingskriterier som bør legges til grunn. Dette kan være spesielt utfordrende dersom man skal kjøpe programvare, hvor enkelte tilbydere kan tilby dette som et produkt (lokal installasjon), mens andre skyleverandører vil tilby dette som en tjeneste.
- Valg av kontraktsform. Det kan være en utfordring av skytjenester som regels selges som hyllevare med standard kontraktsvilkår fra leverandøren.
- Eksempler på SLA-krav (tjenestenivå-avtale) til bruk i forbindelse med skyanskaffelser.
- Sikre at man ikke lager spesifikasjoner som utelukker standardløsninger eller løsninger levert for eksempel via skyen.
- Behov for standardisering/sertifisering. Myndighetene bør kommunisere tydelig hvilke standarder man anbefaler. Det er ønskelig med internasjonale standarder, minimum på EU-nivå.

6.2.3 Arkivloven

I følge arkivloven (LOV-1992-12-04-126) § 9 bokstav b er utgangspunktet at offentlig arkivmateriale ikke kan føres ut av landet uten etter særskilt samtykke fra Riksarkivaren. Offentlig arkivmateriale må her omfatte både gradert og ugradert informasjon som anses som arkivverdig. Unntak kan gjøres *«dersom dette ikkje representerer ein naudsynt del av den forvaltningsmessige eller rettslege bruken av dokumenta»*.

Denne bestemmelsen får stor betydning for kommunens adgang til å ta i bruk skytjenester. Som beskrevet nærmere i punkt 3.5 vil den fysiske lagringen ved bruk av skytjenester gjerne finne sted på opptil flere geografiske spredte servere, i motsetningen til at dataene lagres lokalt hos virksomheten. En skytjeneste kan derfor bestå av alt fra to servere plassert ett eller flere steder i Norge, til et utall servere fordelt over flere forskjellige land. I sistnevnte tilfellet vil data bli lagret i utlandet, og i et slikt tilfelle vil arkiv eller kopi av arkiv, i prinsippet bli ført ut av landet.

Det kan imidlertid stilles spørsmål ved i hvilken grad denne bestemmelsen - herunder unntakene – ut fra det opprinnelige formålet med bestemmelsen – passer på og får anvendelse på bruk av skytjenester levert fra utlandet. Denne regelen ble til for mer enn 20 år siden – det vil si i god tid før skytjenester i dagens form, eller databehandling og lagring i utlandet var en realitet.

Riksarkivet rettet i september 2014 en henvendelse til Kulturdepartementet vedrørende lagring av elektroniske arkiver på servere i utlandet.[2] I denne henvendelsen fremgår det at Riksarkivet mener at på bakgrunn av arkivloven § 9 bokstav b, kan arkiver ikke lagres på servere som befinner seg utenfor Norges grenser. Dette gjelder også kopier av arkiver. Begrunnelsen, i all enkelthet, er at dette i praksis vil innebære å føre arkiv ut av landet. Riksarkivet konkluderer med at arkivdatabasen skal være lagret og tilgjengelig på servere som er fysisk plassert i Norge. At arkivmaterialet er tilgjengelig fra Norge via internett finnes ikke å være tilstrekkelig. De hevder at en slik løsning ikke vil gi god nok kontroll, og mener at løsningen innebærer en rekke risikofaktorer. Riksarkivet fremhever i sin uttalelse at arkivlova

[2] http://www.media.allerinternett.no/km_fil/0/5180530.pdf

ble skrevet i 1992, og at den derfor ikke tar ikke direkte stilling til flere av de aktuelle spørsmålene knyttet til elektronisk arkivering. Riksarkivet utelukker imidlertid ikke at skylagring i utlandet kan bli en fremtidig løsning for offentlige organer i Norge, men mener at dette krever grundig utredning og eventuelt lovendring.

Slik regelverket er i dag, er det således, i følge Riksarkivets tolkning ikke mulig å bruke skytjenester for å lagre arkivverdig materiale. Riksarkivaren uttaler også at hverken loven eller forskriftene regulerer lagring av sikkerhetskopier i utlandet. Og siden sikkerhetskopien er ment å erstatte den originale databasen ved et eventuelt tap, mener Riksarkivaren at heller ikke sikkerhetskopier kan lagres i utlandet.

Denne uttalelsen fra Riksarkivet er etter vår oppfatning noe inkonsekvent, når de vurderer det slik at arkivmaterialet ikke kan føres ut av landet. I arkivloven § 9 som Riksarkivet viser til, fremgår det at Riksarkivaren kan gjøre unntak gjennom samtykke. Dette innebærer at Riksarkivaren faktisk kan samtykke til at arkiv føres ut av landet. At Riksarkivaren velger å ikke benytte denne muligheten vurderes å være lite heldig, særlig med tanke på at formålet med denne bestemmelsen i arkivloven var å sikre at dataene ikke går tapt for ettertiden.

Det fremgår blant annet av forarbeidene til arkivloven at:

«Arkivvern er først av alt ein viktig del av det samla kulturvernet. Arkiv inneheld vitnemål om norsk kultur og samfunnsliv i fortid og notid. Vi må tryggje at slik dokumentasjonsmateriale står til rådvelde for forskning og andre studier i samtid og framtid».[3]

Videre fremgår det av forarbeidene at:

«…det er ei viktig kulturoppgåve å syte for at ettertida kan finna svar på flest mogleg av dei spørsmåla komande slektsledar vil koma til å stilla om vår tid, og at offentleg og privat arkivmateriale er ei av dei viktigaste kjeldene til auka innsikt i, og auka forståing for utviklinga av samfunnet.»[4]

I den skyteknologien som er tilgjengelig i 2015 er det ikke noe problem å sikre at dataene eksisterer og bevares, uavhengig av om de er lagret i Norge eller i et annet land. Det er helt klart at lovverket og praktiseringen av dette her ikke har holdt tritt med den teknologiske utviklingen. Lagring av arkivmaterialet ved bruk av skytjenester, hvor servere er plassert i utlandet, vil i aller høyeste grad ivareta formålet med loven om at arkivmaterialet skal være tilgjengelig for nåtiden og fremtiden.

Riksarkivarens begrunnelse for at heller ikke sikkerhetskopierer kan lagres på servere i utlandet, er etter vår oppfatning ikke uten videre holdbar. Arkivloven ble skrevet på et tidspunkt da det meste arkivmaterialet var papirbasert, og loven inneholder ingen bestemmelse om sikkerhetskopi av offentlig arkivmaterialet. Det kan således stilles spørsmål ved hvor sikkert det var tidligere da en kun hadde et sett med papirbasert arkivmaterialet, i motsetning til i dag hvor en har mulighet til å ha en sikkerhetskopi av dataene lagret lokalt, eller i nettskyen på en geografisk adskilt lokasjon i forhold til «originalen». Ved at det etableres en versjon av et arkiv i utlandet (i nettskyen). En slik ordning ville gi større sikkerhet for at *«..slik dokumentasjonsmateriale står til rådvelde for forskning og andre studier i samtid og framtid»*.[5]

[3] Ot.prp.nr.77 (1991-1992) Om lov om arkiv side 12
[4] Ot.prp.nr.77 (1991-1992) Om lov om arkiv side 7
[5] Ot.prp.nr.77 (1991-1992) Om lov om arkiv side 12

På bakgrunn av dette ville det etter vår oppfatning være fullt mulig for Riksarkivaren benytte seg av sin adgang til å gi samtykke til lagring av arkiv på utenlandske servere.

For å benytte seg av denne unntakshjemmelen kunne Riksarkivet legge til grunn en tilsvarende metodikk for vurdering av sikkerheten ved slik lagring og behandling som den som fremgår av personopplysningsloven § 13 for behandling av personopplysninger. Dette kunne gjøres slik at den behandlingsansvarlige (for arkivopplysninger) og databehandleren, gjennom planlagte og systematiske tiltak kunne sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av arkivopplysninger.

Videre kan den behandlingsansvarlige pålegges - for å oppnå tilfredsstillende informasjonssikkerhet - å dokumentere informasjonssystemet og sikkerhetstiltakene, og at dokumentasjonen skal være tilgjengelig for Riksarkivet.

Kommunal- og moderniseringsdepartementet ønsker at både offentlige og private virksomheter som ønsker å ta i bruk skytjenester skal kunne gjøre dette på en forsvarlig måte og de har derfor igangsatt et prosjekt for å kartlegge de juridiske mulighetene. Det er liten tvil om at mange myndigheter og brukere ønsker å bruke skytjenester og dette må være et relevant argument i tolkningen og praktiseringen av någjeldende regelverk. Dersom Riksarkivaren valgte å benytte det juridiske mulighetsrom de faktisk har, ville dette kunne åpne for bruk av skytjenester Riksarkivarens tilnærming står i sterk motsetning til hvordan denne moderne teknologien er håndtert av Datatilsynet. Datatilsynet var opprinnelig skeptisk til bruk av skytjenester, men har etter hvert gjort seg kjent med teknologien og har gått over til å sette fornuftige kriterier for hvordan teknologien skal brukes. Vi mener Riksarkivaren har et juridisk handlingsrom for å velge en tilsvarende tilnærming.

6.2.4 Bokføringslovgivningen

Forskrift om årsregnskap og årsberetning (for kommuner og fylkeskommuner) FOR-2000-12-15-1424 er hjemlet i Kommuneloven § 48, sjette ledd (Lov om kommuner og fylkeskommuner LOV-1992-09-25-107)

Forskriften inneholder i § 2, første ledd følgende om Bokføring i kommuner og fylkeskommuner:

«Bokføring, spesifikasjon, dokumentasjon og oppbevaring av regnskapsopplysninger skal foretas i tråd med lov 19. november 2004 nr. 73 om bokføring § 3 til § 14 og forskrift 1. desember 2004 nr. 1558 om bokføring kapittel 2 til 7».

Dette innebærer at bestemmelsene i Bokføringsloven om oppbevaring av regnskapsmateriale får anvendelse også på regnskapsmateriale i kommuner og fylkeskommuner.

I henhold til bokføringsloven § 13 annet ledd, skal som hovedregel regnskapsmaterialet oppbevares i Norge. Dette er med på å begrense muligheten til å bruke skytjenester, hvor leverandørene ikke har servere plassert i Norge.

Imidlertid finnes det noen unntak, for det første kan permanent oppbevaring skje i andre EØS stater, jf. bokføringsforskriften § 7-5. *Det fremgår der at «Bokføringspliktige kan 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.» I forskrift av 3. juni 2013 «Forskrift om oppbevaring av elektronisk regnskapsmaterialet i andre EØS-land» fremgår det at regnskapsmaterialet kan oppbevares i Danmark, Finland, Island og Sverige. Dette forutsetter imidlertid at det sendes en melding til Skattedirektoratet, hvor en informerer om slik oppbevaring.

Videre kan det også søkes om dispensasjon til permanent elektronisk oppbevaring i utlandet, jf. bokføringsloven § 13 siste ledd. Om dette heter det i Skattedirektoratets kunngjøring publisert den 30.6.2009, og senere oppdatert, om Dispensasjon fra enkelte bestemmelser i bokføringsloven og bokføringsforskriften følgende:

«Dersom den bokføringspliktige ikke kan benytte unntakene i bokføringsforskriften §§ 7-4 eller 7-5, men likevel ønsker å oppbevare regnskapsmateriale i utlandet, må det søkes Skattedirektoratet om dispensasjon etter bokføringsloven § 13 siste ledd.[6]

Skattedirektoratet har pr. 1. juli 2010 behandlet 777 søknader om å få oppbevare regnskapsmateriale permanent i utlandet. En stor andel av disse gjelder søknader om oppbevaring i Norden, og de er tilfeller som nå ville oppfylt vilkårene for unntak i den nye § 7-5 i bokføringsforskriften.

Bokføringsloven forutsetter at regnskapsmaterialet skal oppbevares i Norge. Skattedirektoratet anser det som en forutsetning for at dispensasjon skal innvilges at det medfører problemer for den bokføringspliktige å oppfylle lovens krav om at oppbevaringen skal skje i Norge. Skattedirektoratet finner i denne sammenheng ikke at 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 regnskapsmaterialet 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. Det presiseres at spesifikasjoner av pliktig regnskapsrapportering, jf. bokføringsloven § 5, og dokumentasjon av regnskapssystemet skal være på norsk, svensk, dansk eller engelsk også ved regnskapsføring og oppbevaring i utlandet, jf. bokføringsloven § 12.

Det er ikke gitt dispensasjon i tilfeller hvor regnskapsmateriale som søkes oppbevart i utlandet ikke kan skrives ut fra terminal i Norge. Dette betyr at regnskapsmateriale som kun forefinnes på papir normalt må oppbevares i Norge.

En søknad om dispensasjon bør inneholde følgende opplysninger:

- *Den bokføringspliktiges navn og organisasjonsnummer*
- *En begrunnelse for søknaden.*
- *Kort om hvilket regnskapsmateriale det søkes dispensasjon for.*
- *Opplysninger om eventuell konserntilknytning eller lignende til selskap som er involvert i oppbevaringen av regnskapsmaterialet i utlandet.*
- *Selskapsnavn og adresse til det stedet regnskapsmaterialet skal lagres i utlandet (serverplassering).*

6 http://www.skatteetaten.no/no/Radgiver/Rettskilder/Kunngjoringer/Dispensasjon-fra-enkelte-bestemmelser-i-bokforingsloven-og-bokforingsforskriften/

- *Bekreftelse på at alt materiale som lagres i utlandet kan leses og skrives ut på papir fra terminal i Norge, samt opplysninger om navn og adresse til dette stedet.*
- *Opplysning om hvilket språk som benyttes i spesifikasjoner av pliktig regnskapsrapportering og dokumentasjon av regnskapssystemet.»*

Til tross for unntakene, vil bokføringsloven fort være til hinder for bruk av enkelte typer skytjenester. Noe av grunnen til dette er at de store leverandørene ofte ikke tilbyr mulighet for å oppbevare opplysningene i de ovennevnte EØS landene, men på servere andre steder i verden. I tillegg er Skattedirektoratet restriktive med å gi dispensasjon og har blant gitt uttrykk for at de *«..anser det som en forutsetning for at dispensasjon skal innvilges at det medfører problemer for den bokføringspliktige til å oppfylle lovens krav om at oppbevaringen skal skje i Norge. Skattedirektoratet finner i denne sammenhengen ikke at kostnadsbesparelser ved utenlandsk oppbevaring gir noen selvstendig grunnlag for dispensasjon.»*[7]

6.3 Regler om vern av personopplysninger

6.3.1 Generelle regler

Enhver behandling av personopplysninger må tilfredsstille de generelle krav i personopplysningsloven (pol.), se særlig pol. §§ 8 (Vilkår for å behandle personopplysninger) og 11 (Grunnkrav til behandling av personopplysninger). For eksempel kreves et hjemmelsgrunnlag for behandling (ofte hjemmel i lov eller samtykke) og at opplysningene ikke brukes senere til formål som er uforenlig med det opprinnelige formålet med innsamlingen, uten at den registrerte samtykker.

Disse regler vil gjelde også i situasjonen hvor en norsk «behandlingsansvarlig» - dvs. «*den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes*», jf. pol. § 2 (4) - benytter seg av eksterne skytjenester som et ledd i behandlingen av sine persondata. Leverandøren vil i så fall bli «databehandler», dvs. «*den som behandler personopplysninger på vegne av den behandlingsansvarlige*», jf. pol. § 2 (5).

Generelt skal forholdet mellom behandlingsansvarlig og databehandler reguleres av en databehandleravtale. Krav til databehandleravtale fremgår i utgangspunktet av pol. § 13, jf. § 15 og personopplysningsforskriftens kapittel 2. Typisk angir en databehandleravtale formålet ved databehandlingen, hvordan behandlingen skal foregå, krav til databehandlerens informasjonssikkerhet (se neste punkt), avtalens varighet, ansvarsfordelingen mellom partene mv.

Den nærmere utforming av databehandleravtaler må tilrettelegges i hvert enkelt tilfelle. Det finnes en egen veiledning og maler for databehandleravtaler på Datatilsynets hjemmesider.

6.3.2 Informasjonssikkerhet etter personopplysningsloven og forskriften

Virksomheten skal sørge for å ha organisatoriske, fysiske og tekniske foranstaltninger, som er nødvendig for å sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av virksomhetens personopplysninger, jf. pol. § 13 og personopplysningsforskriftens kapittel 2. Det skal beskyttes mot at uvedkommende får innsyn i personopplysninger registrert hos virksomheten, og mot utilsiktet endring av opplysningene, og sørges for at tilstrekkelige og

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

relevante opplysninger er tilgjengelig i virksomhetens behandlinger. Personopplysningsforskriften kapittel 2 stiller herunder detaljerte krav til risikovurdering, sikkerhetsrevisjon mv.

Ved bruk av ekstern databehandler, herunder f.eks. leverandører av skytjenester, må den behandlingsansvarlige virksomheten sørge for at kravene til informasjonssikkerhet etter personopplysningsloven og -forskriftene reguleres skriftlig i databehandleravtalen. Forskriftens § 2-15 stiller som krav at *«Den behandlingsansvarlige skal bare overføre personopplysninger elektronisk til den som tilfredsstiller kravene i forskriften her.»*

6.3.3 Behandling av sensitive personopplysninger i skyen

Behandling av sensitive personopplysninger krever et høyere beskyttelsesnivå enn andre personopplysninger. Å bruke denne type personopplysninger ses normalt på som mer inngripende og regelverket stiller derfor også strengere krav til behandlingen av sensitive personopplysninger. Misbruk eller urettmessig spredning av slike personopplysninger vil normalt få større konsekvenser for den enkelte.

I følge Datatilsynet skal sensitive data oppbevares eller lagres adskilt fra åpen informasjon. For å ivareta sikkerheten, anbefaler Datatilsynet å plassere informasjon i egne soner med tilgangskontroll.

At det kreves et høyere beskyttelsesnivå, innebærer ikke at en ikke kan behandle personopplysninger i nettskyen. Imidlertid er det viktig å foreta en tilstrekkelig risiko-vurdering som nærmere beskrevet i punkt 11. Det skal også fremheves at Datatilsynet, så langt i ett tilfelle vi kjenner til, har akseptert at sensitive personopplysninger innenfor helsesektoren behandles i nettskyen.

6.3.4 Skytjenester i Norge og innenfor EU/EØS

I det følgende vil vi se nærmere på hvilke krav som stilles etter personvernreglene som følge av selve overføringen av persondata fra den behandlingsansvarlige virksomheten til databehandler som f.eks. er en leverandør av skytjenester. Det er imidlertid viktig å merke seg at overføringen kun kan finne sted dersom de generelle kravene, jf. over, er oppfylt. Regler om overføring kommer altså i tillegg til de generelle krav.

Det følger av personopplysningsloven (pol.) § 29 at *"Personopplysninger kan bare overføres til stater som sikrer en forsvarlig behandling av opplysningene. Stater som har gjennomført direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, oppfyller kravet til forsvarlig behandling."*

Alle land innenfor EØS/EU anses således for å ha et adekvat beskyttelsesnivå for behandling av personopplysninger. I den grad en norsk behandlingsansvarlig virksomhet overfører personopplysninger til for eksempel en tysk databehandler/leverandør av skytjenester, behøves derfor ikke et særskilt hjemmelsgrunnlag for selve overføringen til utlandet som sådan. Det er tilstrekkelig at behandlingen reguleres av en tilfredsstillende Databehandleravtale (jf ovenfor under pkt 3.3.1), eller eventuelt dekkende klausuler om databehandling som innbakes i vedkommende tjenesteavtale. Dette gjelder på samme måte som det kreves av en eventuell norsk leverandør av skytjenester som skal behandle personopplysninger på vegne av den behandlingsansvarlig.

Et spesielt viktig punkt i databehandleravtaler om skytjenester, er reguleringen av hvordan eventuelle underleverandører skal benyttes. Leverandører av skytjenester vil som nevnt i visse tilfelle ønske å trekke veksler på flere lokasjoner, blant annet for å kunne tilby sammensatte sett av tjenester, og ofte vil disse lokasjonene tilhøre underleverandører.

De er å anse som underleverandører selv om de tilhører samme konsern når det det dreier seg om selvstendige rettssubjekter.

Det vil derfor eksempelvis kunne oppstå situasjoner hvor en databehandler innenfor EU/EØS i tillegg benytter seg av underdatabehandler(e) både innenfor og utenfor EU/EØS. Særlig sistnevnte situasjon skaper komplikasjoner, se nærmere om dette i neste punkt. Databehandleravtalen mellom behandlingsansvarlig og databehandler må adressere dette på en tilfredsstillende måte.

Den nærmere utforming av databehandleravtaler må tilrettelegges i hvert enkelt tilfelle.

6.3.5 Skytjenester utenfor EU/EØS

Europakommisjonen anser at nærmere bestemte land utenfor EU/EØS oppfyller krav til å sikre forsvarlig behandling av personopplysningene. Eksempler på slike land er Australia, Canada og Sveits. For disse landene gjelder i utgangspunktet dermed de samme regler som for overføring innenfor EU/EØS som beskrevet i forrige punkt. En oversikt over hvilke land dette er, finnes på Europakommisjonen sin hjemmeside.[8]

Det samme gjelder ved overføring til amerikanske bedrifter som er tilsluttet Safe Harbor-avtalen[9], og det er altså enkelt å overføre personopplysninger til slike bedrifter. Safe Harbor-avtalen fra år 2000 er en egen avtale mellom EU og USA som utelukkende gjelder overføring av personopplysninger fra EU/EØS-området til amerikanske bedrifter. Safe Harbor er en selvsertifiseringsløsning der bedriftene selv erklærer at de oppfyller en rekke krav som er satt i reglene om Safe Harbor. Når denne utredningen skrives, er det nye forhandlinger mellom EU og USA om innholdet og forvaltningen av Safe Harbor fordi en intern undersøkelse i USA avdekket at det er til dels store mangler hos en del Safe Harbor-bedrifter hva gjelder forvaltning av personopplysninger. Det er likevel slik at det norske Datatilsynet ikke motsetter seg overføring til bedrifter innen Safe Harbor.

Det kreves særskilt hjemmelsgrunnlag for overføring av personopplysninger fra norsk behandlingsansvarlig til databehandler – f.eks. leverandør av skytjenester - etablert utenfor EU/EØS-området, og som ikke er etablert i de landene Europakommisjonen har godkjent eller er en amerikansk virksomhet tilsluttet Safe Harbor-avtalen.

Pol. 30 første ledd angir en rekke mulige grunnlag for slik overføring, for eksempel at den registrerte samtykker i overføringen. Det å benytte samtykke som grunnlag er imidlertid ikke særlig hensiktsmessig hverken for behandlingsansvarlig eller databehandler ettersom samtykket kan trekkes tilbake når som helst.

[8] Se liste over godkjente land på http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

[9] Se liste over amerikanske bedrifter som er tilsluttet Safe Harbor på følgende link: https://safeharbor.export.gov/list.aspx

I praksis ser vi i stedet ofte at unntaket i pol. § 30 annet ledd benyttes. Unntaksbestemmelsen angir at Datatilsynet kan tillate overføring til tredjeland dersom det gis «tilstrekkelige garantier for vern av den registrertes rettigheter».

Personopplysninger kan også overføres til tredjeland i henhold til personopplysningsforskriften § 6-3. Bestemmelsen gir et unntak fra personopplysningsloven § 30 andre ledd. Dersom en bruker EUs standardkontrakt[10] som grunnlag for overføringen til databehandler i tredjeland, er det tilstrekkelig å varsle Datatilsynet om overføringen, ved å sende inn en kopi av signert standardavtale.

En utfordring med standardvilkårene er at de ikke kan benyttes direkte på situasjonen hvor personopplysninger skal overføres fra EU/EØS-basert behandlingsansvarlig til EU/EØS-basert databehandler, og derfra til under-databehandler i tredjeland.

Denne begrensningen fremgår av vedtaket som standardvilkårene bygger på, samt av standardvilkårene selv. Uten å gå nærmere inn på det her, er begrensningen etter vårt syn tynt begrunnet og har vært gjenstand for kritikk bl.a. av den rådgivende Artikkel 29-gruppen.

I ovennevnte situasjon identifiserer Artikkel 29-gruppen følgende alternative fremgangsmåter (jf. gruppens «Working paper 176»):

1. At det inngås direkte kontrakt mellom behandlingsansvarlig i EU/EØS og under-databehandler i tredjeland
2. At behandlingsansvarlig gir databehandleren i EU/EØS et klart mandat til å bruke EUs standardvilkår på vegne av behandlingsansvarlige og i den behandlingsansvarliges navn
3. «Ad-hoc»-kontrakter (dvs. ikke-standardvilkår som ivaretar prinsippene i standardvilkårene).

Som en oppsummering av dette temaet, kreves det ved grenseoverskridende bruk av databehandler(e) en grundig tilnærming for å kunne opprette et juridisk dekkende avtaleverk etter europeiske personvernregler. En av forutsetningene for å kunne gjøre dette er åpenhet fra databehandlers side når det gjelder hvilke underdatabehandlere som benyttes i forbindelse med leveransen, hvor disse befinner seg og hvilken rolle de har i forbindelse med databehandlingen.

6.3.6 Nærmere om risikovurdering og informasjonssikkerhet ved bruk av skytjenester

Personvernregelverket oppstiller i prinsippet ingen hindring for å ta i bruk skytjenester i kommunal sektor, imidlertid må en blant annet foreta en risikovurdering før en kan ta i bruk skytjenestene. Se nærmere om dette under pkt 11 under.

[10] EU sin standardavtale fra 2010 er tilgjengelig på: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087&from=EN

6.4 Eventuelle begrensninger som gjelder for nødvendig sikring av de informasjonskategorier som inngår (ut fra gradering)

6.4.1 Innledning

Skjermingsverdig informasjon eller sikkerhetsgradert informasjon betyr det samme, nemlig informasjon som skal merkes med BEGRENSET, KONFIDENSIELT, HEMMELIG, eller STRENGT HEMMELIG (jf. sikkerhetslovens §§ 3 og 11). Dersom løsningen for skytjenester vil involvere overføring av sikkerhetsgradert informasjon og gi leverandøren tilgang til slik informasjon, kommer sikkerhetsloven med forskrifter til anvendelse.

I praksis er det neppe denne type informasjon kommunene vil ønske å bruke skytjenester for, og som det følger av avsnittene under, vil det rent juridisk kunne være vanskelig å gjennomføre.

6.4.2 Sikkerhetsklarering og autorisasjon av personell

Sikkerhetslovens § 19 inneholder bestemmelser om når sikkerhetsklarering og autorisasjon av personell skal gjennomføres. Begrepene sikkerhetsklarering og autorisasjon må holdes fra hverandre:

- *Sikkerhetsklarering* er definert i sikkerhetslovens § 3 nr. 19 som en *«avgjørelse, foretatt av klareringsmyndighet og bygget på personkontroll, om en persons antatte sikkerhetsmessige skikkethet for angitt sikkerhetsgrad.»* Nasjonal Sikkerhetsmyndighet (NSM) beskriver dette på sin hjemmeside[11] ganske enkelt som «*en avgjørelse som er nødvendig for at en person kan gis tilgang til sikkerhetsgradert informasjon.»*

- *Autorisasjon* er definert i sikkerhetslovens § 3 nr. 20 som en *«avgjørelse, foretatt av autorisasjonsansvarlig, om at en person etter forutgående sikkerhetsklarering (med unntak for tilgang til informasjon sikkerhetsgradert BEGRENSET), bedømmelse av kunnskap om sikkerhetsbestemmelser, tjenstlig behov samt avlagt skriftlig taushetsløfte, gis tilgang til informasjon med angitt sikkerhetsgrad.»* NSM presiserer dette som en «*godkjennelse som enkeltpersoner må ha av sin leder (autorisasjonsansvarlig) for å få tilgang til sikkerhetsgradert informasjon. Autorisasjon kommer i tillegg til sikkerhetsklarering.»*

Hovedregelen etter sikkerhetslovens § 19 er at alt personell som skal ha tilgang til sikkerhetsgradert informasjon, skal sikkerhetsklareres på forhånd. Når man først er sikkerhetsklarert, må man autoriseres for å få tilgang til informasjonen. For å bli autorisert, gjennomføres en såkalt autorisasjonssamtale med en autorisasjonsansvarlig. Den autorisasjonsansvarlige er i utgangspunktet virksomhetens leder, som på nærmere vilkår kan delegere myndigheten til å autorisere (jf. forskrift om personellsikkerhet § 5-1).

Hovedregelen om sikkerhetsklarering for alt personell, kan gjøre det komplisert for en kunde å inngå samarbeid med utenlandsk leverandør. Noe av grunnen til dette er at det kan være vanskelig og/eller tidkrevende å få gjennomført en dekkende personkontroll av leverandørens personell i samsvar med sikkerhetslovens § 20, samt at personellets tilknytning til andre stater kan tillegges betydning i godkjennelsesprosessen (jf.

[11] Se https://www.nsm.stat.no/Arbeidsomrader/Personellsikkerhet/Ord-og-uttrykk/

sikkerhetslovens § 21 (k). Det må også antas at antall avslag vil være høyere på grunn av manglende nødvendig informasjon for å kunne autorisere, og dette kan skape en uforutsigbar situasjon for både kunde og leverandør.

Hovedregelen om sikkerhetsklarering for alt personell gjelder imidlertid kun for tilgang til skjermingsverdig informasjon gradert KONFIDENSIELT eller høyere. For tilgang til informasjon sikkerhetsgradert BEGRENSET er det - som fremgår av definisjonen over - gjort et unntak fra hovedregelen. Om dette nivået skriver NSM følgende: *«[BEGRENSET er] laveste sikkerhetsgradering av informasjon. Det er ikke behov for klarering på dette nivået, men man må autoriseres og underskrive på taushetserklæring for å få tilgang til BEGRENSET».*

Det tilføyes at for alle nivåer gjelder uansett en særregel om taushetsplikt i medhold av sikkerhetslovens § 12, som bestemmer at «*Enhver som får tilgang til sikkerhetsgradert informasjon som ledd i arbeid, oppdrag eller verv for en virksomhet, 3 plikter å hindre at uvedkommende får kjennskap til informasjonen»*.

Det er nærliggende å anta at vil være mindre vanskelig og tidkrevende å gi personell tilgang til BEGRENSET informasjon, ettersom selve sikkerhetsklareringsprosessen kan sløyfes. Dette vil i så fall være en relevant faktor å hensynta ved vurderingen av eventuell bruk av skytjenester.

6.4.3 Krav til sikkerhetsgodkjenning av informasjonssystemer mv.

Sikkerhetslovens § 13 sier at alle virksomheter som behandler sikkerhetsgradert informasjon elektronisk skal ha sikkerhetsgodkjente informasjonssystemer for håndtering av denne type informasjon. Sikkerhetsgodkjenning skal foretas før informasjonssystemet benyttes til håndtering av sikkerhetsgradert informasjon, jf. forskrift om informasjonssikkerhet § 5-15. Det vil være anskaffende myndighet eller NSM som foretar sikkerhetsgodkjenningen av sikkerhetsgradert informasjonssystem.

Etter forskrift om informasjonssikkerhet § 5-15 skal «*sikkerhetsgodkjenning av informasjonssystemet gjennomføres på grunnlag av sikkerhetskonseptet, valgt operasjonsmåte, sikkerhetsdokumentasjonen og verifikasjon av sikkerhetstiltak»*.
Eksempler på momenter som tillegges betydning for godkjenning, er blant annet:

- bruksområde for systemet
- informasjonens sikkerhetsgrad
- klarering og autorisasjon for personell med tilgang
- geografisk og fysisk plassering,
- inndeling i fysiske områder
- forbindelser utenfor eget kontrollert område
- sammenkobling med andre systemer
- valgt operasjonsmåte,
- sikkerhetsdokumentasjonen
- verifikasjon av sikkerhetstiltak.

Videre bestemmer sikkerhetslovens § 10 at NSM skal gis uhindret adgang til ethvert område hvor (blant annet) skjermingsverdig informasjon befinner seg, så langt det er nødvendig for at NSM skal kunne settes i stand til å utføre sine kontrolloppgaver i medhold av lov og forskrifter.

Eksempelvis kan NSM – eller den NSM bemyndiger – foreta tekniske sikkerhetsundersøkelser av lokaler, bygninger osv. som «eies, brukes eller på annen måte kontrolleres av» virksomheten, jf. sikkerhetslovens § 16. Poenget med slike undersøkelser er *«å fastslå hvorvidt uvedkommende med eller uten tekniske hjelpemidler kan skaffe seg tilgang til skjermingsverdig informasjon gjennom avtitting, avlytting av tale eller avlesing av elektroniske signaler.»*

For skytjenester kan denne kontrolladgangen skape praktiske utfordringer både for NSM og leverandøren og eventuelle underleverandører dersom tjenestene medfører tilgang til gradert informasjon. Det må også antas at det vil variere fra leverandør til leverandør i hvor stor grad de er villige til å akseptere at NSM skal ha slik adgangsrett. Mange leverandører vil åpenbart motsette seg slik adgang.

Sikkerhetslovens § 14 («Kryptosikkerhet») bestemmer at *«Sikkerhetsgradert informasjon skal sikres mot endring og mot at falsk informasjon kan innføres under overføring.»* I henhold til forskrift om informasjonssikkerhet § 5-5 om datakommunikasjon og kryptering, skal det benyttes kryptering og dekryptering ved kommunikasjon av sikkerhetsgradert informasjon utenfor eget kontrollert område. Etter sikkerhetslovens § 14 gjelder at «*Bare kryptosystemer som er godkjent av Nasjonal sikkerhetsmyndighet, tillates brukt for beskyttelse av skjermingsverdig informasjon.»* Detaljerte bestemmelser om administrativ kryptosikkerhet fremgår av samme forskrifts kapittel 7.

6.4.4 Sikkerhetsavtale

Sikkerhetsloven § 2 andre ledd gjelder for leverandører som leverer varer eller tjenester til et forvaltningsorgan i forbindelse med sikkerhetsgraderte anskaffelser. Kunden er i disse tilfellene pålagt å inngå en sikkerhetsavtale med leverandøren som formaliserer sikkerhetsmessige aspekter i forbindelse med anskaffelsen, jf. sikkerhetsloven § 27. Sikkerhetsavtale med utenlandske leverandører kan bare inngås etter godkjenning av NSM.

Merk for øvrig at en egen leverandørklarering – som kommer i tillegg til sikkerhetsavtale i avsnittet over - ikke er nødvendig for leverandører som kun skal ha tilgang til skjermingsverdig informasjon BEGRENSET, jf. sikkerhetsloven § 28.

6.4.5 Andre staters rolle og eventuelle myndighetstilganger

Forskrift om informasjonssikkerhet § 3-2 om fremmede staters tilgang til norsk sikkerhetsgradert informasjon, bestemmer at det bare kan gis slik tilgang *«dersom det er i samsvar med norske interesser og ikke er i strid med taushetsplikt»*. Videre forutsettes det at det foreligger *«en sikkerhetsavtale med den aktuelle stat eller organisasjon om utveksling av informasjonen og sikkerhetsmessige forhold»*.

Spørsmålet her er imidlertid i hvilken grad andre stater kan ha hjemmel for å få tilgang til norsk informasjon som lagres i utlandet, herunder norsk sikkerhetsgradert informasjon samt norske personopplysninger, *uten at slik tilgang «gis»* av norsk myndighet.

Et eksempel er hvorvidt amerikanske myndigheter med grunnlag i US Patriot Act i visse tilfelle kan kreve utlevering av opplysninger om norske borgere, eller graderte opplysninger som inngår i en IKT-løsning som eventuelt driftes for kommunene.

Det må i denne sammenheng påpekes US Patriot Act har et avgrenset formål, som innebærer at krav om innsyn i data om bestemte personer bare kan fremsettes knyttet til at

det foreligger konkret mistanke om aktiviteter knyttet til terrorisme mot amerikanske mål, eller hemmelig etterretningsvirksomhet rettet mot USA. Lovgivningen gir ikke amerikanske myndigheter fri tilgang til å kreve opplysninger, selv noen hevder at det kan være slik at myndighetene tillates mer i amerikanske domstoler enn hva en norsk domstol ville tillatt norske myndigheter.

Et like viktig element i denne vurderingen er «hvem som eier selskapet som eier serveren» - uavhengig av hvor serveren står rent geografisk. Noen land har krav i forhold til selskaper i sitt land når det gjelder rett til å få tilgang til data i selskapets systemer, også data fra selskap som bare er "leietakere" og uavhengig av hvor serveren står. USA har rett til innsyn i data som lagres hos amerikanske selskap, selv om serveren ikke står i USA. Dette er delvis bakgrunnen for den sak som Microsoft nå har mot amerikanske myndigheter der myndighetene har krevet at Microsoft Irland utleverer av data fra en epostserver i Irland – uten å gå via det polisiære rammeverket. Saken er pt ikke avgjort og er derfor ikke drøftet nærmere her. Samtidig er det klart at Microsoft finner myndighetenes praksis uønsket og at de vil beskytte sine brukere mot utlevering til myndighetene. En annen sak er at polisiære avtaler nok ville hjemlet den aktuelle utleveringen, men dette ville tatt lenger tid og var derfor ikke den fremgangsmåte myndighetene valgte.

Uansett er imidlertid problemstillinger knyttet til slik myndighetstilgang til opplysninger som behandles i land utenfor Norge en særlig problemstilling, som må vurderes konkret ut fra en risikovurdering i forhold til det enkelte aktuelle land og dets lovgivning.

6.5 Relevant lovgivning i EU

EU-direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, regulerer i utgangspunktet all elektronisk behandling av personopplysninger (definert i artikkel 2) og behandling av opplysninger som inngår i et personregister. Medlemsstatene må sikre at behandlingen av personopplysninger skjer med det beskyttelsesnivået direktivet angir. Direktivet er i Norge gjennomført i norsk rett ved personopplysningsloven med forskrift. I tillegg er EU-direktivet 2002/58/EF om beskyttelse av personopplysninger og elektronisk kommunikasjon implementert i lov om elektronisk kommunikasjon.

I 2012 kom EU-kommisjonen med forslag til en ny personvernreform for unionen. Forslaget fra kommisjonen består av en forordning om vern av personopplysninger, samt et direktiv som skal regulere myndighetenes behandling av personopplysninger i straffesaker. Som medlem av EØS og deltaker i Schengen-samarbeidet er kommisjonens forslag til ny personvernregulering relevant for Norge. Det skal bemerkes at kommisjonens forslag er en forordning og ikke et direktiv slik vi har i dag. Et direktiv åpner for tolkning og for visse nasjonale tilpasninger, mens en forordning derimot gjelder i sin originale tekst. Dette innebærer at forordningen per definisjon blir vedtatt som en lov av alle medlemsstatene, i det den blir vedtatt av EU. EU parlamentet traff vedtak om personvernforordningen i mars 2014, forslaget er vesentlig likt som innstillingen til kommisjonen. Det er foreløpig ikke avklart når denne forordningen vil bli endelig godkjent. Forslaget til ny forordning er teknologinøytral og sier ikke noe spesifikt om bruk av skytjenester.

6.6 Eksisterende veiledninger vedrørende bruk av skytjenester

Det er laget mange veiledere som skrittvis gir en gjennomgang av hvilke vurderinger som må foretas før man skal ta i bruk skytjenester. Under er det angitt noen sentrale veiledninger. For kommunenes videre bruk av nettskytjenester, anbefaler vi de retningslinjer denne utredning har utarbeidet, se rapportens punkt 10 og 11 om risikovurderinger.

- Cloud Computing en veiledning i bruk av nettskytjenester utarbeidet av datatilsynet i 2014[12].

- Opinion 05/2012 on Cloud Computing utarbeidet av artikkel 29 gruppen[13].

- Berlin-gruppens uttalelse om Cloud Computing utarbeidet i 2012[14]

- Cloud Computing – best practice (norden.org) Nordisk Råds offisielle nettsted. Her kan en blant annet lese eksempler på mønsterpraksis i nordiske offentlige myndigheters bruk av skytjenester.

7 Er det behov for endringer i regelverket?

Rent praktisk er det mange situasjoner der det kan være ønskelig å bruke nettskytjenester, men hvor dette er problematisk i lys av dagens regelverk.

I hovedsak gjelder dette når ulik form for lagring eller bruk av personopplysninger skjer i land som er utenfor EU/EØS, typisk India, asiatiske land og Ukraina. Den bruk av data som er aktuell, kan f eks være:

- Call senter tjenester
- Utviklingstjenester
- Supporttjenester
- Applikasjonsforvaltning

Som det fremkommer av det som er utredet foran, vil det være klart at det er arkivloven og bokføringsloven som danner de største juridiske hindre for bruk av nettskytjenester for slike tjenester. Av disse to regelsettene, er det ventelig arkivloven som har størst praktisk betydning fordi den har så vidt stort nedslagsfelt.

Hva gjelder arkivloven, mener vi det allerede i dag foreligger et tilstrekkelig juridisk grunnlag til at Riksarkivaren kan endre sin praksis. Muligens trenger Riksarkivaren støtte på datafaglige vurderinger for å ha trygghet for en omlegging av sin praksis.

Hva gjelder regnskapslovgivningen, vil Skattedirektoratets konservative praksis vedrørende tillatelse til lagring utenlands være et hinder og dersom også regnskapsdata som omfattes av regelverket skal behandles i nettskyen, så må denne praksisen endres. Imidlertid tror vi som nevnt ikke at det er dette som er det mest sentrale hinderet for en videre bruk av nettskytjenester i kommunene.

8 Oppsummering

Det er klart at det er et betydelig mulighetsrom for å ta i bruk nettskytjenester i kommunal sektor, men dette kan gjøres enda større ved noen endringer i forvaltningspraksis, særlig hos Riksarkivaren. Når man skal vurdere å ta i bruk nettskytjenester, så er det en rekke vurderinger som må gjennomføres.

[12] Veiledning om bruk av skytjenester er tilgjengelig på: http://www.datatilsynet.no/Teknologi/Skytjenester---Cloud-Computing/
[13] Artikkel 29-gruppens «working paper 196» er tilgjengelig på: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf
[14] http://www.datenschutz-berlin.de/attachments/875/Sopot_Memorandum.12.6.12.pdf?1339501499

Det første man må gjøre, er å kartlegge hvilke regelsett som er relevant for de opplysningene som skal legges ut. Slik arkivloven og bokføringsloven tolkes i dag, er det lettest å legge ut opplysninger som ikke omfattes av disse regelverkene. Dersom disse myndighetene endrer praksis, vil omfanget av opplysninger som kan legges i skyen, øke.

I punkt 10 og 11 under, har vi fremsatt konkrete retningslinjer for andre vurderinger som må gjøres, dette dreier seg bla om personopplysningslovens krav til vurdering av dataene som skal legges ut og risikoanalyser, krav til sikkerhet, avveining av risiko tiltak vurdere landrisiko, osv. Under ser vi nærmere på hvilke typer informasjon som vanligvis kan være aktuelle å legge i en nettskytjeneste.

9 Nærmere om kravene i personopplysningsloven

9.1 Innledning

I kapittel 6, 7 og 8 har vi sett at det finnes en rekke lover som har betydning for kommunenes adgang til å bruke skytjenester. Det er imidlertid få lover som er et absolutt hinder for å benytte skytjenester. De største utfordringene er arkivloven og bokføringsloven. Imidlertid, til tross for at personopplysningslovginingen ikke er til hinder for å bruke skytjenester, stiller regelverket en rekke krav en må ta hensyn til ved behandling av personopplysninger i nettskyen. I dette kapittelet vil vi derfor se nærmere på ulike kategorier av personinformasjon som typisk behandles i en kommune og hvilke krav som stilles til behandlingen av personopplysninger.

9.2 Kategorier av personinformasjon og andre typer av fortrolig informasjon som typisk behandles i kommunene

9.2.1 Generelt

I dette avsnittet vil vi kort gjennomgå noen viktige kategorier av informasjon som typisk behandles i en kommune. Felles for disse er at det ofte er informasjon som er underlagt taushetsplikt og med strenge krav til tilgangskontroll og sikkerhet.

Årsakene til at informasjon skal beskyttes kan være forskjellig. Tiltakene for å beskytte informasjonen er imidlertid langt på vei de samme – uavhengig av årsakene. Det er mer et spørsmål om viktighetsgraden – hva er risikoen for at informasjon kommer på avveie, og hvor store konsekvensene er av at den kommer på avveie.

Et hovedskille går mellom opplysninger av intern administrativ karakter i kommunen på den ene siden (Personopplysninger om ansatte og folkevalgte, informasjon om strategier, og andre fortrolige opplysninger om kommunens virksomhet mv.), og på den annen side personopplysninger eller bedrifts- og forretningshemmeligheter knyttet til kommunens samfunnsoppdrag, forvaltning og oppgaveløsning (Personopplysninger knyttet til innbyggere og brukere av kommunens tjenester, klientforhold, informasjon i saksdokumenter og annen informasjon som omfattes av taushetsplikt, og som for øvrig kan være underlagt avtalebaserte taushetsforpliktelser og konfidensialitetsavtaler mv.). Under ser vi nærmere på de enkelte informasjonstypene.

9.2.2 Opplysninger om ansatte

Personopplysningsforskriften § 7-16 om personalregistre mv. lyder som følger:

Arbeidsgivers behandling av ikke-sensitive personopplysninger om nåværende eller tidligere ansatte, personale, representanter, innleid arbeidskraft samt søkere til en stilling er unntatt meldeplikt etter personopplysningsloven § 31 første ledd.

Dersom det behandles sensitive personopplysninger, er behandlingen unntatt fra konsesjonsplikten etter personopplysningsloven § 33 første ledd, men underlagt meldeplikten etter § 31 første ledd. Unntak fra konsesjonsplikt gjelder under forutsetning av at:

a) den registrerte har samtykket i behandlingen eller behandlingen er fastsatt i lov,
b) opplysningene er knyttet til arbeidsforholdet, og
c) personopplysningene behandles som ledd i personaladministrasjonen.

Meldeplikt etter andre ledd gjelder likevel ikke behandling av

a) opplysninger om medlemskap i fagforeninger som nevnt i personopplysningsloven § 2 nr. 8 bokstav e,
b) nødvendige fraværsopplysninger og opplysninger som er registreringspliktige i henhold til arbeidsmiljøloven § 5-1,
c) opplysninger som er nødvendige for å tilrettelegge arbeidssituasjonen på grunn av helseforhold.

Selv om det foreligger unntak fra meldeplikt til Datatilsynet (for ikke-sensitive opplysninger) og fra konsesjonsplikt (for sensitive opplysninger - som således er underlagt meldeplikt), er likevel all behandling av personopplysninger underlagt alle de alminnelige reglene om behandling av personopplysninger i personopplysningsloven. Det er bare henholdsvis bestemmelsene om meldeplikt og om konsesjonsplikt som fravikes.

Dette innebærer at de alminnelige reglene om informasjon om behandling av personopplysninger og om overføring til utlandet gjelder fullt ut for behandling av opplysninger om kommunens ansatte. Dette er viktig fordi det gjelder svært mange personopplysninger.

9.2.3 Personopplysninger og andre opplysninger

Den sentrale bestemmelsen om taushetsplikt for ansatte og andre som utfører tjeneste eller arbeid for et forvaltningsorgan, fremgår av forvaltningsloven § 13, som lyder:

Enhver som utfører tjeneste eller arbeid for et forvaltningsorgan, plikter å hindre at andre får adgang eller kjennskap til det han i forbindelse med tjenesten eller arbeidet får vite om:

1) noens personlige forhold, eller

2) tekniske innretninger og fremgangsmåter samt drifts- eller forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde av hensyn til den som opplysningen angår.

Som personlige forhold regnes ikke fødested, fødselsdato og personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted, med mindre slike opplysninger røper et klientforhold eller andre forhold som må anses som personlige. Kongen kan ellers gi nærmere forskrifter om hvilke opplysninger som skal reknes som personlige, om hvilke

organer som kan gi privatpersoner opplysninger som nevnt i punktumet foran og opplysninger om den enkeltes personlige status for øvrig, samt om vilkårene for å gi slike opplysninger.

Taushetsplikten gjelder også etter at vedkommende har avsluttet tjenesten eller arbeidet. Han kan heller ikke utnytte opplysninger som nevnt i denne paragraf i egen virksomhet eller i tjeneste eller arbeid for andre.

Pliktsubjektet etter denne bestemmelsen *er «..enhver som utfører tjeneste eller arbeid for et forvaltningsorgan».*

Det som beskyttes ved denne bestemmelsen er det vedkommende *«..i forbindelse med tjenesten eller arbeidet får vite om:*

1) noens personlige forhold, eller

2) tekniske innretninger og fremgangsmåter samt drifts- eller forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde av hensyn til den som opplysningen angår.»

I tillegg til denne generelle bestemmelsen i forvaltningsloven, finnes det flere særlige bestemmelser om taushetsplikt i spesiallovgivning rettet mot spesielle profesjoner eller forvaltningsområder.

Vi går ikke her nærmere inn på rekkevidden av bestemmelser om taushetsplikt, men konstaterer at taushetsplikten og plikten til beskyttelse av informasjon som kommunale organer og virksomheter mottar i sin oppgaveløsning er klar og sterk. Den gjelder ikke bare personopplysninger, men *enhver* opplysning som er betrodd i forbindelse med oppgaveløsningen.

Dette medfører en plikt for vedkommende forvaltningsorgan til å treffe relevante og tilstrekkelige tiltak for å beskytte informasjonen, slik at den ikke blir tilgjengelig for uvedkommende. Denne plikten omfatter alle former for tilgjengeliggjøring av informasjonen for uvedkommende – enten dette skjer muntlig, på papir, elektronisk, eller ved tap av minnepinner eller mobiltelefoner eller andre elektroniske enheter. For å avgjøre hvilke tiltak som skal iverksettes for å beskytte informasjonen, må forvaltningsorganet foreta en risikovurdering, og iverksette tiltak for å begrense risikoen. Denne risikovurderingen og de tiltakene som iverksettes, vil være helt lik de vurderingene som gjøres i henhold til kravene til internkontrollrutiner i henhold til personopplysningsloven § 13. Se nærmere om dette nedenfor under pkt. 9.3.

Taushetsplikt kan i tillegg til taushetspliktbestemmelsene i forvaltningslovgivningen være avtalehjemlet i forholdet mellom vedkommende forvaltningsorgan og klienten, eller i forhold til øvrige parter i en sak. Dette gjøres gjerne gjennom forskjellige former for konfidensialitetsavtaler eller NDAer («Non Disclosure Agreements»). Slike avtaler inneholder ofte en konkretisering av krav til beskyttelse og ikke-spredning av konfidensiell informasjon, og mulige sanksjoner knyttet til mislighold av avtalen. Forvaltningsorganet må i hvert enkelt tilfelle foreta en konkret risikovurdering for å avgjøre om de generelle tiltak for å beskytte den relevante informasjonen er tilstrekkelig, eller om det er nødvendig å iverksette ytterligere tiltak.

I personopplysningsforskriften kapittel II og III er det gjort visse unntak fra konsesjon- og meldeplikt. Unntakene gjelder for en rekke av de behandlingene av personopplysninger som foretas i kommunale organer mv.

Det er i de aktuelle kapitlene bare gjort unntak fra bestemmelsene om henholdsvis konsesjonsplikt og meldeplikt. Alle de materielle reglene i loven om behandling av personopplysninger gjelder fullt ut. Dette innebærer at de alminnelige reglene i personopplysningsloven og om overføring til utlandet gjelder fullt ut for behandling av opplysninger om datasubjektene som det behandles opplysninger om

9.3 Kravene i personopplysningsloven til etablering og etterlevelse av et internkontrollsystem og sikkerhetsløsninger

9.3.1 Hvem har ansvar for fortrolig informasjon

Det overordnede ansvaret for å iverksette nødvendige og tilstrekkelige tiltak for å sikre og beskytte fortrolig informasjon i kommuner, fylkeskommuner og i kommunale virksomheter, (heretter kalt «virksomheten») ligger hos den øverste ledelse i virksomheten.

En del av dette ansvaret omfatter det å etablere et system for informasjonssikkerhet. Det må settes mål for informasjonssikkerheten, hvilket sikkerhetsnivå man skal ha og hvordan bedriften skal arbeide med risikohåndtering. Videre må det etableres styringsmidler. Det er også ledelsens ansvar å sørge for nødvendige dokumenter, som informasjons-sikkerhetsstrategi, og at instrukser lages og revideres.

Hvis virksomheten skal ta i bruk nettskyen for tjenester, må systemet for informasjonssikkerhet omfatte vurderinger og tiltak som også omfatter skytjenesteleverandøren med eventuelle underleverandører – slik at hele kjeden av leverandører og ikke minst underleverandører er dekket.

Behandling av personopplysninger eller andre beskyttelsesverdige opplysninger ved hjelp av skytjenester følger de samme regler som bruk av databehandlingsressurser for øvrig. Behandling av personopplysninger defineres i personopplysningsloven § 2 nr. 2. Den enkelte kommunale enheten er den behandlingsansvarlige i henhold til definisjonen i personopplysningsloven § 2 nr. 4, og skytjenesteleverandøren (med eventuelle underleverandører) er databehandler(e) som definert i personopplysningsloven § 2 nr. 5).

Ansvaret for behandling av personopplysninger i den enkelte kommunale enhet ligger som nevnt hos enhetens ledelse, og etablering av nødvendig og tilstrekkelig sikkerhet for behandlingen av opplysninger hos skytjenesteleverandøren må sikres gjennom databehandleravtale som angitt i personopplysningsloven § 15.

Hvis skytjenesten behandler personopplysninger (f. eks epost, tekstbehandling, kontakt og adresseopplysninger, regnskaps- og faktureringstjenester, kalenderoppføringer osv.) på vegne av den behandlingsansvarlige, er skyleverandøren (med eventuelle underleverandører) en *databehandler* i personopplysningslovens forstand uavhengig av hvilken tjeneste som leveres.

En databehandler kan ikke behandle personopplysninger på annen måte enn det som er avtalt med den behandlingsansvarlige, jf. personopplysningsloven § 15. Databehandleren plikter i tillegg å gjennomføre sikringstiltak som følger av personopplysningsloven § 13 og personopplysningsforskriftens kapittel 2.

Det må understrekes at en databehandleravtale ikke fritar behandlingsansvarlige for lovfestet juridisk ansvar. Derimot er det slik at den behandlingsansvarlige gjennom databehandleravtalen må pålegge databehandleren å gjennomføre de nødvendige sikringstiltak som den behandlingsansvarlige finner nødvendig som konsekvens av en analyse av type personopplysninger, behandling og risiko.

Datatilsynet har laget en veileder om og eksempel på avtaleskisser for en slik databehandleravtale. I avtaleskissen og veilederen finnes oversikt over minimumskravene som Datatilsynet forventer at en slik avtale inneholder. Det kan være andre punkter som tilkommer selve avtalen, men det er avhengig av internkontrollen til den behandlingsansvarlige som kjøper tjenesten. Noen slike punkter kan være sikkerhetskopiering, sletting, tilgangsstyring og segmentering av databaser. Med segmentering forstås i denne sammenheng at den behandlingsansvarliges personopplysninger ikke skal sammenblandes med personopplysninger fra en annen behandlingsansvarlig. Hva som nærmere ligger i forbudet mot sammenblanding beror på en konkret vurdering som det vil føre for langt å gå inn på her.

9.3.2 Risikovurdering og informasjonssikkerhet

En sentral plikt etter personopplysningsloven er at den behandlingsansvarlige skal etablere og holde vedlike et internkontrollsystem. Dette fremgår av personopplysningsloven § 14, som lyder:

«Den behandlingsansvarlige skal etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes kvalitet.

Den behandlingsansvarlige skal dokumentere tiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren.

Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda.
Kongen kan gi forskrift med nærmere regler om internkontroll.»

Det er viktig å understreke at internkontrollsystemet til enhver tid skal reflektere de vurderinger og retningslinjer som legges til grunn for å sikre at personopplysningsloven til enhver tid oppfylles av virksomheten. Internkontrollsystemet er helt sentralt i Datatilsynets kontroll med at loven etterleves i de virksomheter Datatilsynet kontrollerer.

Den behandlingsansvarlige skal gjennomføre en risikovurdering for sin behandling av personopplysninger. Risikovurderingen må ses i sammenheng med etablerte akseptkriterier for *risiko*, og den behandlingsansvarlige skal iverksette nødvendige tiltak for å oppnå en tilfredsstillende *informasjonssikkerhet*. En mal for risikovurdering er inntatt i punkt 11 i denne veilederen.

Det følger av personopplysningsforskriften § 2-4 at virksomheten selv skal fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger. Hva som defineres som akseptabel risiko vil variere fra virksomhet til virksomhet og hvilke typer personopplysninger som skal behandles. Begrepet akseptabel risiko kalles noen ganger for restrisiko. Uavhengig av begrep, handler det om å identifisere den risiko man ikke kan unngå uten urimelige ressurser, altså den risiko man aksepterer at skal eksistere. En konsekvens av dette er at en skytjeneste som anses å ha en tilfredsstillende sikkerhet for én behandlingsansvarlig ikke nødvendigvis har det for en annen. Dette altså til tross for at sikkerheten i tjenesten kan være nøyaktig den samme.

For å oppnå tilfredsstillende informasjonssikkerhet må den behandlingsansvarlige kunne forvisse seg om at skytjenesten møter de kravene som er fastlagt under arbeidet med akseptkriteriene og risikovurderingen. Virksomheten må tillegge vurderingen større vekt når den går fra egen drift til sky-baserte løsninger, ettersom personopplysningene vil ligge utenfor den behandlingsansvarliges direkte kontroll.

Spørsmålet blir da hvordan den behandlingsansvarlige skal kunne forvisse seg om at informasjonssikkerheten faktisk er tilfredsstillende.

Databehandleravtalen skal inneholde en del som omhandler informasjonssikkerhet, og det er viktig at den behandlingsansvarlige går grundig gjennom denne. Avtalen i seg selv er imidlertid ingen forsikring for at leverandøren har en tilfredsstillende informasjonssikkerhet.

Personopplysningsforskriftens kapittel 2 om informasjonssikkerhet har en bestemmelse om *sikkerhetsrevisjon*:

"Sikkerhetsrevisjon av bruk av informasjonssystemet skal gjennomføres jevnlig. Sikkerhetsrevisjon skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører. Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemet som ikke er forutsatt, skal dette behandles som avvik, jf. § 2-6. Resultatet fra sikkerhetsrevisjon skal dokumenteres."

Datatilsynet er derfor av den oppfatning at databehandleren må kunne legge frem dokumentasjon for informasjonssystemets utforming og sikkerhetsløsninger. Dette for at den behandlingsansvarlige kan forvisse seg om at løsningen har tilfredsstillende informasjonssikkerhet sett opp mot risikovurdering og akseptkriterier. ISO 27001 og tilsvarende standarder gir i seg selv ikke tilstrekkelig informasjon om valgt sikkerhetsnivå. Slike standarder gir først og fremst informasjon om måten skyleverandøren jobber med sikkerhet på (plan-do-check-act-rutiner), men altså ikke om valgt sikkerhetsnivå. For å få vite noe om de valgte sikkerhetsnivåene må man få innsyn i annen type sikkerhetsdokumentasjon. Kommunen må stille krav til skyleverandøren om slik konkret dokumentasjon. Det kan være et godt alternativ å få tilgang til revisjonsrapporter utarbeidet av eksterne revisjonsselskap som beskriver it-sikkerheten. Normalt gis kunden tilgang til disse mot at de forplikter seg til å signere konfidensialitetsavtale. Vi har sett at noen leverandører krever betaling for tilgang til slik dokumentasjon, noe vi mener at kunden ikke skal akseptere.

Databehandleren (skyleverandøren) skal ikke kunne endre informasjons-sikkerhetstiltak uten at den behandlingsansvarlige er blitt informert skriftlig og har godkjent endringen.

Den behandlingsansvarlige må sørge for å gjøre en fornyet vurdering av informasjonssikkerhetstiltakene når det skjer endringer i faktiske forhold. Dette kan f. eks være ny kunnskap om myndigheters praksis for tilsyn og tilgang til informasjon hos skyleverandøren el. Den behandlingsansvarlige bør også følge opp avtalene og revidere de på gitte tidspunkter, ut fra at leverandøren kan endre leveranser, eller ta i bruk nye løsninger, som gjør at tiltakene må vurderes på nytt.

9.3.3 Informasjonsplikt

Den behandlingsansvarlige har informasjonsplikt overfor den enkelte registrerte som følger av personopplysningsloven § 19.

Bestemmelsen går ut på at den behandlingsansvarlige har plikt til å gi *den registrerte* følgende informasjon:

- navn og adresse på den behandlingsansvarlige,
- formålet med behandlingen,
- om opplysningene vil bli utlevert, og eventuelt hvem som er mottaker,
- det er frivillig å gi fra seg opplysningene, og
- annet som gjør den registrerte i stand til å bruke sine rettigheter etter personopplysningsloven.

Når den behandlingsansvarlige benytter skyleverandør), kan innsynsretten gjøres gjeldende direkte mot skytjenesteleverandøren. Dette fremgår av personopplysningsloven § 24 «*Hvordan informasjonen skal gi*s», der det heter:

«Informasjonen kan kreves skriftlig hos den behandlingsansvarlige eller hos dennes databehandler som nevnt i § 15. Før det gis innsyn kan den behandlingsansvarlige kreve at den registrerte leverer en skriftlig og undertegnet begjæring».

Et slikt krav vil i mange tilfelle by på spesielle utfordringer ved bruk av skytjenesteleverandører som databehandlere. Databehandleravtalen mellom kommunen som den behandlingsansvarlige og skytjenesteleverandøren må regulere forholdet slik at det legges til rette for ivaretakelse av informasjonsplikten.

Kommunen må sikre at de har rutiner etc. for å oppfylle dette kravet i loven og dette må reflekteres i internkontrollsystemet som kommunen er pliktig til å ha.

9.3.4 Spesielle problemstillinger

Leverandører av skytjenester har i utgangspunktet noen fordeler i forhold til tradisjonelle leverandører av servertjenester. For eksempel kan skytjenestene gi mer fleksible og integrerte løsninger.

Men slike fordeler fører også med seg noen spesielle problemstillinger som den behandlingsansvarlige må ta stilling til:

Sikkerhetskopiering/Speiling

- Hvordan fungerer dette?
- Overføres personopplysningene til et annet land for redundans, eksempelvis fra Irland til USA eller fra Tyskland til India?
- Er en slik redundans i henhold til de avtaler som er inngått?
- Hvordan behandles personopplysningene etter at de er overført?

Segmentering

- Datatilsynet har uttalt at den behandlingsansvarliges personopplysninger ikke skal sammenblandes med personopplysninger fra en annen behandlingsansvarlig. Hvordan håndterer leverandøren dette?

Tilgangsstyring

- Hvem hos leverandøren har tilgang til personopplysningene som behandles? Merk at om driftspersonell etc. som befinner seg i «tredjeland» (land utenfor EØS og som ikke er godkjent av EU for å ha etablert et «tilfredsstillende nivå av personvern») kan aksessere personopplysninger vil dette normalt også innebære at personopplysninger blir overført til landene hvor det aktuelle driftspersonellet etc. befinner seg.
- Er det tilgangsstyring (hvem har tilgang til hvilken informasjon – innmelding av nye brukere og utmelding av brukere som ikke lenger skal ha tilgang mv) og administrasjon av brukernavn, passord og tilganger i samsvar med lovpålagte krav og egen *internkontroll* (se avsnitt 9.3.2 over om risikovurdering og informasjonssikkerhet)?

Autorisert og uautorisert bruk

- Gir skytjenesten mulighet for registrering av autorisert og uautorisert bruk i henhold til personopplysningsforskriften § 2-14?

Dokumentasjon

- Er løsningen tilstrekkelig dokumentert med hensyn til kontroll fra offentlige myndigheter (jfr. personopplysningsloven § 14 om etablering og dokumentasjon av internkontrollsystem)?

Overføring til tredjeland

Personopplysninger kan som nevnt ikke uten videre overføres til utlandet. Personopplysningsloven § 29 og 30 fastsetter nærmere regler for når slik overføring kan skje og hvilke vilkår som gjelder for overføringen. Datatilsynet stiller videre krav om at man skal vite i hvilke land en databehandler og/eller dens underleverandører prosesserer personopplysninger. Det er derfor sentralt å stille dette spørsmålet til skyleverandøren og få dokumentert skriftlig i hvilke land personopplysninger behandles. Enkelte skyleverandører tilbyr kunden å kunne velge mellom land/regioner hvor dataen lagres innenfor.

Utgangspunktet er at opplysninger kan overføres innenfor EØS-området og til en del andre stater som *«..sikrer en forsvarlig behandling av opplysningene»* jfr. personopplysningsloven § 29. En liste overs like stater finnes på Artikkel 29-gruppens hjemmesider på følgende adresse: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm)

For øvrig kan opplysninger overføres til andre land enn de som der er angitt, hvis betingelsene i § 30 første ledd foreligger, eller etter 30 annet ledd med samtykke fra Datatilsynet. I henhold til ny § 6-3 i personopplysningsforskriften, er forhåndssamtykke fra Datatilsynet etter § 30, annet ledd ikke lenger nødvendig. Det kreves da at mottaker av opplysningene er en databehandler, og at grunnlaget for overføringen er EUs standardkontrakt inntatt i kommisjonsbeslutning 2010/87/EU datert 5. februar 2010. Den behandlingsansvarlige skal varsle Datatilsynet om overføringen ved innsending av utfylt og signert standardkontrakt. Overføringen kan finne sted når varsel er sendt.

9.4 Oppsummering

Vi har nå sett at personopplysningsloven stiller en rekke krav til behandling av personopplysninger, som også inkluderer behandling av personopplysninger i nettskyen. I kapittel 10 og 11 vil vi gi kommunene en mer praktisk tilnærming til bruk av skytjenester, blant annet en sjekkliste for hvilke vurderinger som må gjøres ved bruk av skytjenester, herunder; personopplysningslovens krav til vurdering av dataene som skal legges ut og risikoanalyser som må gjennomføres, krav til sikkerhet, avveining av risiko, vurdering av

landrisiko etc. Sjekklisten under gir ikke en fullstendig veiledning for anskaffelse av skytjenester, den tar blant annet ikke for seg kravene i anskaffelsesregelverket.

10 Sjekkliste for å sikre personvernregelverket og informasjonssikkerheten ved anskaffelse av skybaserte løsninger

Sjekklisten under er en ikke-uttømmende liste, men vil gi et godt utgangspunkt for å sikre at man tar i bruk nettskytjenester på en lovlig og forsvarlig måte i henhold til personvernlovgivningen. Sjekklisten er ikke ment å bli benyttet som det eneste verktøy ved anskaffelser av sky-baserte IT-løsninger. I tillegg til det som fremgår under er det viktig at kommunene følger anskaffelsesregelverket ved anskaffelse av skytjenester.

Sjekklisten bør legges til grunn når man skal planlegge en anskaffelse av skytjenester, og de forskjellige aktivitetene som anbefales under må inkorporeres der de hører hjemme i de ulike trinnene i anskaffelsesprosessen. Det forutsettes her at det enkelte foretak søker juridisk assistanse før avtale om sky-baserte IT-løsninger inngås, i den grad kunden ikke har tilstrekkelig kunnskap om dette selv.

10.1 Forberedelse

1. Identifiser hvilke typer opplysninger man ønsker å benytte skytjenester for.
2. Identifiser hvilke regelverk som gjelder for opplysningene – ta særlige hensyn hvis arkivloven eller bokføringsloven får anvendelse.
3. Skaff oversikt over hvordan flyten av opplysninger vil være (hvor blir dataene overført, direkte og indirekte).
4. Skaff oversikt over hvorfra opplysningene vil bli lest/aksessert/behandlet.
5. Skaff oversikt over hvordan IT-sikkerheten er ivaretatt i systemet som vurderes. Mye av dette kan typisk være beskrevet i whitepapers etc. som leverandøren publiserer på nettet, men innholdet der er ofte ikke tilstrekkelig. For å få nok informasjon til å kunne vurdere sikkerheten kan det være nødvendig med tilgang til annen dokumentasjon, slik som revisjonsrapporter fra uavhengige tredjeparter etc. Leverandøren vil normalt gå med på å dele slik informasjon med kunden, noen ganger mot at kunden signerer en konfidensialitetsavtale med leverandøren.
6. Forsikre deg om at IT-sikkerheten tilfredsstiller personopplysningsloven krav (evt. andre relevante rettsregler avhengig av hva slags type informasjon som prosesseres).
7. Forsikre deg om at det også ut fra et forretningsmessig ståsted og ut fra ditt eget foretaks risikoprofil og kriterier for aksept av risiko vil være ok å ta i bruk tjenesten.
8. Forsikre deg om at du som kunde fullt ut eier dataene som lagres og at leverandøren ikke kan utnytte de for andre formål enn det som spesifikt er avtalt med deg.
9. Forsikre deg om at dataene blir slettet når du gir beskjed om dette og/eller når avtalen med leverandøren avsluttes.
10. Gjennomfør en risikovurdering i samsvar med personopplysningslovens krav og eForvaltningsforskriften og sørg for at denne dokumenteres. En mal for slik risikovurdering står i rapportens punkt 11.
11. Ha klare kriterier for aksept av risiko/restrisiko.
12. Vurder om det er behov for melding til Datatilsynet, fordi data overføres til, eller er tilgjengelig og behandles fra land utenfor EU/EØS.

10.2 Inngåelse av avtale

1. Vær forberedt på at det er lite rom for forhandlinger, spesielt når avtalen inngås med store skytjenesteleverandører. Men stå samtidig fast på de krav som følger av norsk rett. De fleste leverandører vil ha et incitament til å levere tjenester som det er lovlig å

bruke, ettersom det motsatte vil kunne påvirke leverandørens muligheter for å selge tjenesten.
2. Forsøk å få en rett til å terminere avtalen om det skulle bli avdekket at leverandøren ikke opererer på en måte som tilfredsstiller kravene i norsk lovgivning, evt. slik disse kravene kommer til uttrykk i avtalen.
3. Vær på vakt etter bestemmelser som gir leverandøren en ensidig adgang til å endre (deler av) kontraktens innhold, typisk underliggende dokumentasjon uten å be om samtykke.
4. Sørg for at forhold som er viktige for å sørge for ivaretakelse av sikkerhet er på plass i avtalen. Eksempler på dette er krav til sikkerhet, sanksjoner ved brudd på slike, back-up/failover-løsninger etc.

10.3 Forhold å være spesielt oppmerksom på vedrørende personvern

1. Sørg for at du har oversikt over i hvilke land personopplysningene behandles.
2. Husk at «behandling» omfatter mer enn lagring – også utvikling, drift etc fra utland kan gjøre at reglene om overføring til tredjeland får anvendelse.
3. Sørg for at du leser leveranseavtalen grundig slik at du vet i hvilke land opplysninger vil bli lagret – og like viktig – i hvilke land leverandørens ansatte befinner seg når de utfører tjenester som omhandler behandling av personopplysninger. Det samme gjelder for avtalens formuleringer om hvor underleverandører befinner seg.
4. Skaff deg oversikt over hvor leverandørens representanter med potensiell tilgang til personopplysningene befinner seg. Om dette er i andre land enn det som er nevnt under punkt 1 i dette underkapittelet, må oversikten over land utvides tilsvarende.
5. Det er et krav etter norsk rett at det er mulighet for å gjennomføre sikkerhetsrevisjoner hos leverandøren. Datatilsynet har i sitt brev til Narvik kommune påpekt at kommunen jevnlig, for eksempel årlig, må sørge for at sikkerhetsrevisjonen blir gjennomført. [15]Undertiden kan det å få tilgang til leverandørens eksterne revisors rapporter vedr. sikkerhetsevalueringer være tilstrekkelig, men dette kan ikke tas som en generell regel og må derfor vurderes konkret jf. Datatilsynet sitt brev til Moss kommune[16]. Avgjørende er om man gjennom revisjonsrapporten får tilgang på informasjon som gjør det mulig å fastslå om lovens og avtalens krav overholdes eller ikke. Kommunen kan/bør eventuelt stille krav til skytjenesteleverandøren om at kommunen skal ha rett til å kreve at en tredjepart utfører revisjon av den aktuelle tjenesten.
6. Overføring av personopplysninger til utlandet må skje i samsvar med bestemmelsene i personopplysningsloven kapittel 5 og personopplysningsforskriften kapittel 6. Husk at overføring i visse tilfelle forutsetter at søkes om tillatelse fra Datatilsynet (personopplysningsloven § 30, annet ledd).
7. Påse at personopplysninger ikke overføres til land som ikke er forhåndsgodkjent av Datatilsynet, med mindre overføringen skjer i henhold til Safe Harbor-instituttet eller EUs mal for databehandleravtaler, BCR (Binding Corporate Rules) eller tilsvarende gyldig overføringsgrunnlag. Det understrekes at Safe Harbor-instituttet for tiden er under et visst press fra EU-parlamentet og at f. eks Tyskland stiller spesielle vilkår knyttet til bruk av Safe Harbor avtalene som grunnlag for en overføring til USA.
8. Merk at ikke alle amerikanske selskap er underlagt Safe Harbor. Du må få bekreftet at leverandøren du forhandler med er en såkalt «Safe Harbourite» og at leverandørens tilslutning til instituttet også omfatter de kategorier av data som det er aktuelt at denne behandler.

[15] Brev fra Datatilsynet til Narvik kommune av 21. september 2012 vedrørende Google Apps.
[16] Brev fra Datatilsynet til Moss kommune av 21. september 2012 vedrørende bruk av nettskyen Microsoft Office 365.

9. Påse at leverandøren har en plikt til å informere deg som kunde om brudd på sikkerheten som innebærer at personopplysninger har kommet eller kan komme på avveie. I gitte situasjoner vil du kunne ha en selvstendig plikt til å informere Datatilsynet (og de personene den kompromitterte dataen relaterer seg til) om dette.
10. Sørg for å ha en databehandleravtale på plass som ivaretar ovennevnte.

10.4 Øvrige forhold

1. Sett deg inn i hva avtalen sier om responstider ved feilmelding, oppetidsgarantier etc. og vurder om dette er tilfredsstillende for din virksomhet.
2. Sett deg inn i hvor enkelt/komplisert det vil være å migrere kundedataen til løsninger som tilbys av andre leverandører. Enkelte sky-baserte IT-tjenester er kjent for å kunne (bevisst eller ubevisst) skape en såkalt lock-in-effekt som innebærer at terskelen for å ta i bruk alternative tjenester blir høy.
3. Sjekk hvordan tap av data reguleres i kontrakten. Ofte tar ikke leverandøren ansvar for dette overhodet. Det må vurderes om dette er akseptabelt for din virksomhet. Verdt å merke seg for kommuner er at for dårlig sikring mot eventuelt tap av data vil kunne komme i konflikt med plikten til å oppbevare visse kategorier av data i en gitt periode.
4. Sjekk om avtalen gir leverandøren mulighet til leveransenekt ved manglende betaling (selv om betalingsmisligholdet ikke er vesentlig). Mange leverandører opererer med slike krav, noe som kan skape utfordringer om avtalen ikke endres på dette punkt.

11 Matrise for risikovurdering

11.1 Innledning

I dette kapittelet har vi utarbeidet et forslag til en metodikk for hvordan man forbereder faktagrunnlaget for en risikovurdering og hvordan man gjennomfører og dokumenterer denne. Dette er kun et forslag, og det er en rekke andre måter å gjennomføre en risikovurdering enn det som fremgår her. Det finnes en rekke tilgjengelige veiledninger for informasjonssikkerhet og internkontroll, herunder da også hvordan en kan gjennomføre en risikovurdering. Andre nyttige veiledninger er tilgjengelig på Datatilsynet og DIFI sine nettsider.

11.2 Verdivurdering

Informasjon er en stor del av virksomheters verdi. Ved bruk av skytjenester er det derfor viktig å forstå verdien av virksomhetens informasjon slik at riktige beskyttelsestiltak kan iverksettes. Det kan være mange forhold å vurdere i forhold til hvilken beskyttelse informasjonen må ha. Er beskyttelsen av informasjonen underlagt lovverk, virksomhetens retningslinjer eller andre former for beskyttelseskrav? Har kundene satt egne krav til beskyttelse? Alle disse momenter må vurderes i fastsettelsen av sikringstiltak.

Behovet for å beskytte informasjon springer ut av det forholdet at den har en verdi som kan gå tapt eller føre til et tap av verdier dersom den blir misbrukt, ødelagt eller endret.

Vi kan finne eksempler på slik type informasjon på alle nivåer i samfunnet.

Hvis man klassifiserer informasjonen etter hvor «verdifull» den er, vil det også bli lettere å iverksette riktige sikringstiltak. Som et ledd i en god informasjonshåndtering er verdivurdering en fremgangsmåte for å gi virksomheten et bilde på verdien av informasjon.

Det finnes på alle nivåer informasjon som det er et behov for å beskytte i ulik grad. Det er ikke alltid de som "eier" informasjon er bevisste om hvilken verdi informasjonen kan ha – dels ved at den går tapt eller kommer på avveie -men også med tanke på misbruk.

Informasjon kan ha krav til beskyttelse av både av hensyn til behovet for konfidensialitet, integritet og tilgjengelighet. Verdivurdering av informasjon dreier seg om å analysere informasjon med tanke på hvilke konsekvenser det kan få dersom denne informasjonen går tapt, endres eller kan bli misbrukt.

Det finnes noen enkle spørsmål som kan gi grunnlag for en nærmere vurdering av informasjonens verdi:

- Hvordan kan informasjonen misbrukes?
- Hvem kan misbruke informasjonen?
- Hva blir konsekvensen dersom informasjonen blir tilgjengelig for uvedkommende?
- Kan informasjonen påføre skade for andre?
- I hvilket tidsrom har informasjonen verdi?

Hvilken informasjon som til en hver tid har et beskyttelsesbehov, er ikke statisk over tid. Det vil alltid være et tilsig av ny informasjon som bør beskyttes, samtidig som behovet for beskyttelse av informasjon som tidligere ble ansett som ble ansett for verdifull, kan falle bort eller bli redusert. Det finnes informasjon som bare trenger beskyttelse "over natten", mens annen informasjon kanskje må beskyttes i mange tiår. Når informasjonen skal ut i en skytjeneste er det derfor svært viktig å ha gått igjennom og satt en klassifisering på informasjonen.

Det finnes flere forskjellige former for klassifisering. Et eksempel ved bruk av 4 klasser kan være:

- Offentlig informasjon
- Intern informasjon
- Sensitiv informasjon
- Kritisk informasjon

Det vil være behov for ulike sikkerhetstiltak, avhengig av hvilken klasse informasjonen settes i.

11.3 Risikovurdering

For å kunne vite noe om risikoen ved bruk av skytjenester sett opp mot verdien av informasjonen, er det krav om å gjennomføre risikovurderinger. En risikovurdering vil si noe om mulige trusler, sannsynligheten for at en sikkerhetshendelse vil inntreffe og konsekvensen om hendelsen inntreffer. Virksomheten må fastsette kriterier for hva som kan aksepteres av risiko. Tiltak for å begrense risiko må iverksettes overfor de truslene som ikke aksepteres. Ved å lage en risikomatrise får man et risikobilde, som på en enkel måte illustrerer hvilke trusler man ikke aksepterer.

I bruken av skytjenester er det mange forskjellige trusler man må vurdere. I denne veiledningen gis det ikke noen uttømmende liste over mulig trusler. Det gis imidlertid en kort innføring i hvordan man på en enkel måte kan sette opp en risikomatrise.

Eksempler på trusler kommunen kan se for seg er:

- Potensielle leverandører eller andre uautoriserte parter får tilgang til strategier, anbudsinformasjon og forretningshemmeligheter som er i kommunens varetekt
- Personopplysninger kommer på avveie
- Flere PC-er eller servere blir angrepet av virus, og flere ansatte blir dermed hindret i arbeidet
- En tjeneste som brukes har ikke tilstrekkelig sementering av data, slik at data fra flere brukere blandes eller gjøres tilgjengelig for brukere som ikke skulle ha tilgang
- En tjeneste har ikke tilstrekkelig sikring av data mot uautorisert tilgang, og media skriver om saken

Det må etableres skalaer for konsekvens, sannsynlighet og risiko:

Sannsynlighet kan deles inn i hvor ofte man tror hendelsen vil inntreffe:

- Sjelden
- Kan skje
- Svært vanlig

Videre, kan man tallfeste hendelser: 4 ganger pr år, 2 ganger pr måned, 2 ganger pr uke.

Konsekvens kan deles inn i:

- Liten
- Middels
- Stor

Evt. hvis man tallfester: Økonomisk tap på mer enn 50.000 tap på mer enn 500.000 eller tap på mer enn 1.000.000.

Skalaer må settes opp av noen som kjenner virksomheten.

I en tabell kan man, etter en vurdering, sette følgende risiko inn (det nedenstående er et eksempel, den konkrete vurderingen må skje i hver enkelt virksomhet):

- Med stor risiko menes hendelser som skjer mer en to ganger i uken, gir tap på over 1.000.000 kr eller betydelig tap av renommé. Rød farge er brukt, og er ikke akseptabelt.
- Med moderat risiko menes hendelser som skjer mer enn to ganger i måneden, gir tap på over 500.000 kr eller tap av renommé. Oransje/gul farge brukes, og må ha oppmerksomhet.
- Med lav risiko menes hendelser som ikke skjer mer enn to ganger i halvåret, medfører tap på over 50.000 kroner eller ubetydelig tap av renommé. Grønn farge benyttes, og risikoen aksepteres.

Riskotabell

		Sannsynlighet		
		Sjelden	Kan skje	Svært vanlig
Konsekvens	Liten	*Lav*	*Lav*	*Moderat*
	Middels	*Lav*	*Moderat*	*Stor*
	Stor	*Moderat*	*Stor*	*Stor*

Konsekvenser
Dersom uvedkommende får tilgang til sensitiv informasjon kan det få store konsekvenser, alt etter hvilken informasjon som blir kjent og hvem som blir kjent med denne.

Risikovurdering

Eksempel på vurdering av risiko for virksomheten i tabellen nedenfor, viser aktuelle risiki og hvilke tiltak som kan iverksettes. Dette er ikke noen fullstendig gjennomgang, og den er ikke ferdigstilt. Den er generell, og ikke kun rettet mot trusler ifm. bruk av skytjenester.

Trussel: *Leverandører til kommunen som er konkurrenter, får tilgang til informasjon om hverandre.*

#	Årsaker	Risikovurdering			Mulige tiltak
		Konsekvens	Sannsynlighet	Risikonivå	
1	Egne ansatte kan ønske å spre sensitive opplysninger for egen vinnings skyld.	Stor	Sjelden	Moderat	Opplæring av ansatte
2	Uvedkommende kan få tilgang til informasjon som er lagret i en skytjeneste.	Stor	Kan skje	Stor	Opplæring av ansatte. Gode avtaler med skytjenesteleverandør. Test av skytjenesteleverandør.
3	Vi kan bli offer for generelle angrep (virus/ormer/trojanere, phishingangrep)	Stor	Kan skje	Stor	Opplæring av ansatte. Innstalleringer av sikkerhetsoppdateringer skal bli fast rutine. Beskyttelsen av selve nettverket skal bli bedre og mer helhetlig
4	Utenforstående kan stjele utstyr der sensitiv informasjon er lagret.	Stor	Kan skje	Stor	Opplæring av ansatte. Bedre fysisk sikring. Bedre rutiner for avhending av utstyr og makulering. Kryptering av lagringsmedier

12 Vedlegg

12.1 Oversikt

Under er en oversikt over dokumenter som er brukt i arbeidet med utredningen samt dokumenter som vil være nyttige for kommunene i arbeidet med å benytte skytjenester.

De spørreskjema som har vært sendt ut, er utformet i samråd med KS og med FAD.

Vedlegg 1 Mandat

Mandatet er vedlagt som vedlegg 1.

Vedlegg 2 Spørreskjema til kommuner

Dokumentet er vedlagt som Vedlegg 2.

Vedlegg 3 Spørreskjema til leverandører

Dokumentet er vedlagt som Vedlegg 3.

Vedlegg 4 Resultat av spørreundersøkelse og dybdeintervjuer

Vedlegg 5 - Sjekkliste ved anskaffelse av skybaserte løsninger

FØYEN TORKILDSEN ADVOKATFIRMA

Vedlegg 1 Tilbudsforespørsel

KOMMUNESEKTORENS ORGANISASJON
The Norwegian Association of Local and Regional Authorities

Føyen Advokatfirma DA
Postboks 7086 St.Olavsplass
0130 OSLO

Vår referanse:	14/00584-1
Arkivkode:	0
Saksbehandler:	Anne Mette Dørum
Deres referanse:	
Dato:	01.09.2014

Tilbudsforespørsel på KS FoU-prosjekt 144008 - Utredning av juridiske forhold ved bruk av nettsky i kommunal sektor – en mulighetsstudie

KS ønsker tilbud på løsning av et FoU-prosjekt som skal utrede juridiske aspekter ved bruk av nettsky som lagringsløsning i kommunal sektor. Utredningen skal være en mulighetsstudie.

Nettskyløsninger[17] er i ferd med å etablere seg i offentlig sektor, men det er uklare juridiske forhold ved anskaffelse og bruk. Fordi leverandører av skytjenester er store aktører som stort sett leverer standardiserte tjenester, vil enkeltkunder i hovedsak være henvist til å bruke leverandørenes standardavtaler. Dette kan komme i konflikt med krav i norsk regelverk, for eksempel kravene til informasjonssikkerhet i personopplysningsloven og kravet i arkivloven § 9 b om at arkiv ikke kan «førast ut or landet».

Vi skiller gjerne mellom ulike typer tjenester som leveres via skyen, for eksempel:

- applikasjoner; for eksempel tekstbehandling eller e-post levert via en nettleser
- utviklingsplattform; når en tilbyder benytter nettskyen for å utvikle egne applikasjoner som leveres til kundene via internett
- infrastruktur; når kunden bruker egne programmer, men kjøper lagringsplass og prosessorkraft hos en skyleverandør

Lagring i skyen betraktes som effektiv på grunn av at det er lett tilknytning, mobilitet, stor "skalerbarhet" for brukere og hos store leverandører garanteres god sikkerhetskopiering. Men det er ikke helt liketil å velge skytjenester. Ofte er det reservelagring i annet land/kontinent av sikkerhetsårsaker, og man kjenner ikke alltid til hvilke(t) land dette er. Leverandør disponerer hele skyen og "flytter data rundt" etter behov (transborder data flow), uten at oppdragsgiver vet hvor dataene befinner seg.

[17] Skytjenester (nettskyløsninger) er programvare og tjenester som leveres over internett, ofte fra en kommersiell leverandør. Det viktigste kjennetegnet på en skytjeneste er forretningsmodellen, som er basert på at man kun betaler for det man bruker

Selv om lagring i skyen selges inn som raskt, rimelig og trygt, kan det likevel være vanskelig å personopplysningsloven, sikkerhetsloven, arkivloven og annen lovgivning. Hvordan kan kommuner og fylkeskommuner velge riktig?

Det er viktig å vite hvor dataene faktisk er lagret, ettersom det i utgangspunktet er lovverket i det landet der serveren står, som gjelder for dataeiers tilgang til dataene. Det er ikke alltid at regler om innsyn, skjerming og personvern; deling eller salg av data; styresmaktenes rett til å vite; ansattes integritet og ærlighet eller dataeiers rett til tilgang til egne data er i tråd med de lover og regler som gjelder i Norge.

Et annet viktig element er hvem som eier selskapet som eier serveren. Noen land har krav i forhold til selskaper i sitt land når det gjelder rett til å få tilgang til data i selskapets systemer, også data fra selskap som bare er "leietakere" og uavhengig av hvor serveren står. Dette er hjemlet f. eks. i patriot act i USA etter 9/11. USA har rett til innsyn i data som lagres hos amerikanske selskap, selv om serveren ikke står i USA.

Fordi leverandører av skytjenester er store aktører som stort sett leverer standardiserte tjenester, vil enkeltkunder i hovedsak være henvist til å benytte disse leverandørenes standardavtaler. Dette kan komme i konflikt med krav i norsk regelverk, for eksempel kravene til informasjonssikkerhet i personopplysningsloven.

Personopplysningsloven stiller krav til lagring av personopplysninger. Dette innebærer at personopplysninger normalt kan lagres innenfor EU/EØS-området, hos virksomheter i USA som følger «Safe Harbour»-prinsippene eller andre land som EU-kommisjonen mener har et akseptabelt beskyttelsesnivå. «Safe Harbour»-prinsippene skal sikre at personopplysningene behandles i henhold til EUs personverndirektiv. Fordi kundene ved bruk av noen nettskyløsninger ikke vet nøyaktig hvor dataene befinner seg til enhver tid, kan det være juridisk vanskelig å bruke slike løsninger når man behandler personopplysninger. I Norge har Datatilsynet utviklet en veileder som ser spesifikt på personvernutfordringene ved skytjenester.

Datatilsynet har i 2012 vurdert bruken av nettskytjenester i to norske kommuner, Narvik og Moss. Basert på dette har tilsynet kommet med noen prinsipielle avklaringer rundt bruken av slike tjenester:

- Det må gjennomføres grundige risiko- og sårbarhetsanalyser i forkant. Virksomheten må spørre seg selv om hva som kan gå galt, og hvilke følger det i så fall kan få.

- Selskapene må ha en tilfredsstillende databehandleravtale som er i tråd med norsk regelverk. Det er den norske virksomheten som har ansvar for at lovens krav følges.

- Bruken av nettskytjenester må jevnlig revideres. Det vil si at en tredjepart gjennomfører en sikkerhetsrevisjon på vegne av virksomheten og sikrer at databehandleravtalen følges.

- Databehandleravtalen må være det som gjelder og leverandørens generelle personvernerklæring må ikke gå utover denne.

Problemstillinger:
Utredningen skal være en mulighetsstudie, som skal beskrive hva dagens lovverk faktisk tillater, hva kommunene faktisk kan ta i bruk av løsninger og hvordan de faktisk kan og bør rigge seg.
Utredningen skal også se på om det er behov for endringer i lov- og regelverket, og hvilke endringer dette i så fall bør være.

Utgangspunktet bør være hva det er som er spesielt ved bruk av nettsky sammenlignet med andre IKT-løsninger.

Overordnede problemstillinger som skal sjekkes ut er hvilke «lovlighetskrav» som gjelder innenfor ulike regelverk og ulike typer opplysninger, og hvordan disse faktisk kan praktiseres i dag.

- Hvilke lover begrenser bruk av nettskytjenester – og på hvilken måte?
- På hvilken måte tillater lovverket bruk av nettskyløsninger, og på hvilke vilkår?
- Hvilke bruksområder, muligheter og begrensninger finnes for ulike typer data, og på hvilke vilkår?
- Hvilke typer nettskyløsninger kan være aktuelle å bruke – og hvilke er uaktuelle for denne typen data?
- Hva skal kommunesektoren i særlig grad tenke på når de tar i bruk nettskyløsninger?
- Hva skal kommunesektoren være oppmerksom på ved avtaleinngåelse?

Tilbyder er velkommen til å supplere listen med problemstillinger.

Metodikk:
KS ønsker at tilbyder selv beskriver metodikken.

Vi ser likevel for oss at det er nødvendig at tilbyder både i tilbudet, sluttrapporten og andre dokumenter skiller mellom type skytjenester (løsninger) og hva kommunal sektor skal tenke på ved planlegging og anskaffelse av de ulike tjenestene.

Vi ser for oss at følgende aktiviteter skal gjennomføres, i tillegg til aktiviteter som tilbyder vurderer som relevant:

1. Dokumentstudie av veiledninger og utredninger som allerede finnes, inklusive arbeider som er gjort i Sverige og Danmark
2. Erfaringsinnhenting (Narvik, Alta og Moss kommuner)
3. Kartlegging av fylkeskommuner og kommuners ønsker og behov

Arbeidet skal blant annet baseres på det arbeidet som DIFI og IKT Norge allerede har gjort på dette feltet.

Prosjektet skal samarbeide med Kommunal- og moderniseringsdepartementet (KMD) i deres nettskyprosjekt som starter i september 2014. Metodikken for prosjektets kartlegging av fylkeskommuner og kommuners ønsker og behov skal utarbeides i samarbeid med KMDs prosjekt, ettersom KMD bare skal kartlegge statlig sektor og dette prosjektet kartlegger kommunal sektor.

Prosjektet skal ha felles referansegruppe med Kommunal- og moderniseringsdepartementets nettskyprosjekt.

Gjennomføring
Det er ønskelig at tilbyder synliggjør at løsningen av oppdraget vil bygge på oppdatert kunnskap på feltet, og at tilbyder redegjør for valg av datainnsamling og metode.

Vi ber om at tilbudet definerer relevante/naturlige milepæler i løpet av prosjektperioden, og at de ulike aktivitetene i prosjektet angis i en framdriftsplan. Totalkostnadene for prosjektet spesifiseres, inkludert mva.

KS' standardkontrakt for oppdragsforskning vil bli lagt til grunn for prosjektet. Det vil også bli oppnevnt en kommunal referansegruppe for prosjektet, som er et rådmannsutvalg i KS.

Leveranser/rapportering
I tillegg til sluttrapport og presentasjon skal prosjektet levere:

- Forslag til et internettbasert «veikart for bruk av nettskyløsninger» på ks.no. Se eksempel: http://www.ks.no/tema/Innovasjon-og-forskning1/Veikart-for-sosiale-medier/
- Sjekkliste som kommunesektoren kan bruke ved valg av leverandør og ved avtaleinngåelse med leverandør.

Resultatene skal presenteres på en leservennlig måte, med oversiktlige og tydelige fremstillinger. Prosjektet skal avsluttes med en sammenfattende sluttrapport og ferdigstilte verktøy.

Rammer for oppdraget
Økonomiske rammer for oppdraget vil være inntil kr 500 000,- inkl. mva. Tilbudet må inkludere alle kostnader som er nødvendige for å gjennomføre prosjektet. Tidspunkt for oppstart og avslutning avtales nærmere i forbindelse med avtaleinngåelsen.

Kontaktperson er Anne Mette Dørum, Anne.Mette.Dorum@ks.no .

Vedlegg 2 Kartlegging – skytjenester i kommunesektoren

1. Bakgrunn

KS-Kommunesektorens organisasjon (KS) har igangsatt et FoU-prosjekt som skal utrede juridiske aspekter ved bruk av nettsky i kommunal sektor. Utredningen er en mulighetsstudie, som skal beskrive hva dagens lovverk faktisk tillater, hva kommunene faktisk kan ta i bruk av løsninger og hvordan de faktisk kan og bør rigge seg.

FØYEN Advokatfirma DA er engasjert av KS for å gjennomføre utredningen.

Utredningen vil også vurdere om det er behov for endringer i lov- og regelverket, og hvilke endringer dette i så fall bør være.

Utgangspunktet for utredningen, er å se på hva som er spesielt ved bruk av nettsky sammenlignet med andre IKT-løsninger.

Nettskyløsninger[18] er i ferd med å etablere seg i offentlig sektor. Det er imidlertid uklare juridiske forhold ved anskaffelse og bruk. Leverandører av skytjenester er store aktører som stort sett leverer standardiserte tjenester. Enkeltkunder vil derfor i hovedsak være henvist til å bruke leverandørenes standardavtaler. Dette kan komme i konflikt med krav i norsk regelverk, for eksempel kravene til gjennomføring av offentlige anskaffelser i anskaffelsesregelverket, informasjonssikkerhet i personopplysningslovgivningen og kravet i arkivloven § 9 b om at arkiv ikke kan «førast ut or landet».

Vi skiller gjerne mellom ulike typer tjenester som leveres via skyen, for eksempel:

- applikasjoner; for eksempel tekstbehandling eller e-post levert via en nettleser
- utviklingsplattform; når en tilbyder benytter nettskyen for å utvikle egne applikasjoner som leveres til kundene via internett
- infrastruktur; når kunden bruker egne programmer, men kjøper lagringsplass og prosessorkraft hos en skyleverandør

Lagring i skyen betraktes som effektiv på grunn av at det er lett tilknytning, mobilitet og ”skalerbarhet” for brukere. Hos store og seriøse leverandører garanteres god sikkerhet.

Valg av skytjenester kan være komplisert. Ofte er det reservelagring i annet land/kontinent av sikkerhetsårsaker, og kunden kjenner ikke alltid til hvilke(t) land dette er. Selv om lagring i skyen selges inn som raskt, rimelig og trygt, kan det likevel være vanskelig å overholde personopplysningsloven, sikkerhetsloven, arkivloven og annen lovgivning.

[18] Skytjenester (nettskyløsninger) er programvare og tjenester som leveres over internett, ofte fra en kommersiell leverandør. Det viktigste kjennetegnet på en skytjeneste er forretningsmodellen, som er basert på at man kun betaler for det man bruker

2. Spørreundersøkelse

Ett ledd i utredningen er å foreta en spørreundersøkelse hos et utvalg av kommuner. Dette spørreskjemaet er sendt ut til et utvalg på 10 store, 10 mellomstore og 10 mindre kommuner, med sikte på å innhente opplysninger om bevissthet og status vedr bruk av skytjenester i kommunenes IKT satsninger.

Spørreundersøkelsen foretas i løpet av november måned, og resultatene vil bli brukt som underlagsmateriale i forbindelse med utredningen.

3. Problemstillinger som ønskes belyst

Spørsmål	Kommentarer
Hvor bevisst er kommunen i forhold til begrepet «Sky-tjenester»	
• Har kommunen en IT-strategi hvor bruk av skytjenester inngår	
• Hvis ja – er den en del av en mer helhetlig IT-strategi	
• Skilles det mellom hva som kan legges i Skytjeneste og hva som ikke kan	
• Skiller kommunen i sin strategi mellom forskjellige typer skytjenester	
○ Plattform som tjeneste	
○ Infrastruktur som tjeneste	
○ Software (applikasjoner) som tjeneste	
Har kommunen en sourcing strategi (en fremgangsmåte for anskaffelser av IKT varer og tjenester der anskaffelsesaktivitetene løpende evalueres og forbedres)	
• Hvis Ja - omfatter sourcing	

Spørsmål	Kommentarer
strategien bruk av skytjenester	
○ Direkte hos store utenlandske leverandører av skytjenester	
○ Bruk av lokale leverandører med skytjenestelevarandører som underleverandører	
Bruker kommunen skytjenester i dag	
• Hvis ja - Hvilke typer skytjenester bruker kommunen	
○ Infrastruktur-/lagringstjenester (f.eks. Dropbox, Box, Skydrive/Onedrive, Google Drive, ICloud,)	
○ Standardapplikasjoner (f.eks. Ms Office 365, Google apps, web-basert epost)	
○ Web-basert plattformer/fagsystemer (f.eks. Fronter, It's learning) ○ Annet …….	
Hvis kommunen bruker skytjenester, når ble hver enkelt tjeneste tatt i bruk (angi navn på den enkelte tjeneste)	
• Tjeneste 1 - tidspunkt	
• Tjeneste 2 – tidspunkt	

Spørsmål	Kommentarer
• Tjeneste 3 – tidspunkt	
• ---	
Er det gjennomført Risiko- og sårbarhetsanalyser for de skytjenester som er tatt i bruk	
Blir det behandlet sensitive personopplysninger i skytjenesten • Angi hvilke typer sensitive opplysninger (jf. Personopplysningsloven § 2 nr. 8)	
Vet kommunen hvor dataene fysisk er lagret?	
Blir kommunens data overført til andre land for redundans ved sikkerhetskopiering/speiling?	
Planlegger kommunen å ta i bruk nye skytjenester i nær fremtid	
• Hvor snart	
• For hvilke typer systemer og tjenester	
• Hvilke typer skytjenester	
• Når vil de enkelte tjenester bli tatt i bruk	
Har kommunen støtt på konkrete hindringer i lovverket for bruk av skytjenester	
• Hvilken lovgivning er identifisert som hindring	
• Er det identifisert hva som må/kan gjøres for å tilfredsstille den	

Spørsmål	Kommentarer
enkelte lov	
○ For bestemte typer systemer i kommunen	
○ I forhold til skytjenester generelt	
○ I forhold til bestemte typer skytjenester	
○ For hver type system og tjeneste - angi hindring	
○ Har kommunen analysert muligheten for avhjelpende tiltak i forhold til de angitte hindringene	
Har usikkerhet hindret kommunen i å ta i bruk skytjenester	
• Hva består usikkerheten i	
• Hva har kommunen gjort for å avklare usikkerhet	
• Har kommunen analysert muligheten for avhjelpende tiltak i forhold til usikkerheten Hvilke offentlige organer har skapt usikkerhet (Riksarkivet, Datatilsynet osv.)	
Hva er driverne for at kommunen har tatt i bruk eller ønsker å ta i bruk skytjentester	
• Økonomi	
• Standardisering	

Spørsmål	Kommentarer
• Ressursdeling	
• Skalerbarhet og fleksibilitet • Annet	
Internkontrollsystemer	
• Har kommunen etablert en internkontroll i overensstemmelse med kravene i Personopplysningsloven § 14 (etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes kvalitet).	
• Er tiltakene dokumentert og har kommunen et opplegg for å vedlikeholde internkontrollsystemet.	
• Har kommunen innlemmet andre typer opplysninger enn personopplysninger (f. eks bedrifts- og forretningshemmeligheter og andre opplysninger underlagt taushetsplikt mv) i opplysningene som omfattes av internkontrollsystemet.	
• Brukes internkontrollsystemet aktivt ved vurderinger og beslutninger om å ta i bruk skytjenester	
• Er det utarbeidet rutiner for å inngå databehandleravtaler med andre som behandler personopplysninger på vegne av kommunen (f. eks data-driftsleverandører, konsulenter	

Spørsmål	Kommentarer
som yter driftsbistand eller feilrettingstjenester)?	
Databehandleravtaler:	
Inneholder databehandleravtalen elementer som: • Tilgangsstyring (hvem har tilgang fra leverandør) • Lagring (hvor lagres dataene) • Sikkerhetsrevisjon • Evt. Underleverandører • Sletting (når slettes dataene etter at kommunen har initiert sletting)	
Sikker kommunikasjon:	
• Blir dataene kryptert? • Er kommunikasjonen kryptert mellom kommunen/leverandør, • Er kommunikasjonen kryptert mellom leverandør/underleverandør, • Er kommunikasjonen kryptert mellom datasentre?	
• Har kommunen en egen strategi for informasjonssikkerhet	
• Er det utarbeidet egne retningslinjer for informasjonssikkerhet? Angi ved innholdsfortegnelse hva retningslinjene inneholder	
• I hvilken grad er ledelse og ansatte kjent med kommunens retningslinjer for informasjonssikkerhet	
• Har ledelsen og de ansatte tilstrekkelig kunnskap om behandling av personopplysninger og andre taushetsbelagte	

Spørsmål	Kommentarer
opplysninger?	

Vedlegg 3 Intervju-guide - kommuner og leverandører

1. Bakgrunn

KS har igangsatt et FoU-prosjekt som skal utrede juridiske aspekter ved bruk av nettsky i kommunal sektor. Utredningen er en mulighetsstudie, som skal beskrive hva dagens lovverk faktisk tillater, hva kommunene faktisk kan ta i bruk av løsninger og hvordan de faktisk kan og bør rigge seg. v

Utredningen vil også vurdere om det er behov for endringer i lov- og regelverket, og hvilke endringer dette i så fall bør være.

Utgangspunktet for utredningen, er å se på hva som er spesielt ved bruk av nettsky sammenlignet med andre IKT-løsninger.

Nettskyløsninger er i ferd med å etablere seg i offentlig sektor. Det er imidlertid uklare juridiske forhold ved anskaffelse og bruk. Leverandører av skytjenester er store aktører som stort sett leverer standardiserte tjenester. Enkeltkunder vil derfor i hovedsak være henvist til å bruke leverandørenes standardavtaler. Dette kan komme i konflikt med krav i norsk regelverk, for eksempel kravene til gjennomføring av offentlige anskaffelser i anskaffelsesregelverket, informasjonssikkerhet i personopplysningslovgivningen og kravet i arkivloven § 9 b om at arkiv ikke kan «førast ut or landet».

Vi skiller gjerne mellom ulike typer tjenester som leveres via skyen, for eksempel:

- applikasjoner; for eksempel tekstbehandling eller e-post levert via en nettleser
- utviklingsplattform; når en tilbyder benytter nettskyen for å utvikle egne applikasjoner som leveres til kundene via internett
- infrastruktur; når kunden bruker egne programmer, men kjøper lagringsplass og prosessorkraft hos en skyleverandør

Lagring i skyen betraktes som effektiv på grunn av at det er lett tilknytning, mobilitet og ”skalerbarhet” for brukere. Hos store og seriøse leverandører garanteres god sikkerhet.

Valg av skytjenester kan være komplisert. Ofte er det reservelagring i annet land/kontinent av sikkerhetsårsaker, og kunden kjenner ikke alltid til hvilke(t) land dette er. Selv om lagring i skyen selges inn som raskt, rimelig og trygt, kan det likevel være vanskelig å overholde personopplysningsloven, sikkerhetsloven, arkivloven og annen lovgivning.

2. Intervju av Leverandører

Ett ledd i utredningen er å foreta Intervjuer hos et utvalg av Leverandører.

Dette notatet er et underlagsdokument for innhenting av opplysninger i form av intervjuer med fra noen få utvalgte leverandører om bevissthet og status vedr bruk av skytjenester i kommunenes IKT satsninger.

Intervjuene foretas i løpet av november måned, og resultatene vil bli brukt som underlagsmateriale i forbindelse med utredningen.

3. Problemstillinger som ønskes belyst

Nr	Spørsmål	Kommentarer

1	Hvor bevisste opplever er kommunen i forhold til begrepet «Sky-tjenester»?
	• Har kommuner en IT-strategi hvor bruk av skytjenester inngår
	• Hvis ja – er den en del av en mer helhetlig IT-strategi
	• Skilles det mellom hva kommunene kan legge i Skytjeneste og hva de ikke kan
	• Skiller kommunene i sin strategi mellom forskjellige typer skytjenester
	  ○ Plattform som tjeneste
	  ○ Infrastruktur som tjeneste
	  ○ Software (applikasjoner) som tjeneste
		Hvilke typer skytjenester leverer leverandøren
		  ○ Plattform som tjeneste
		  ○ Infrastruktur som tjeneste
		  ○ Software (applikasjoner) som tjeneste
		Hvor bevisste opplever leverandøren at kommuner er kommuner i forhold til begrepet «Sky-tjenester»?
		• Har kommuner en IT-strategi hvor bruk av skytjenester inngår
		• Hvis ja – er den en del av en mer helhetlig IT-strategi
		• Skilles det mellom hva kommunene kan legge i Skytjeneste og hva de ikke kan
		• Skiller kommunene i sin strategi mellom forskjellige typer skytjenester

2	Har kommunen en sourcing strategi
	• Omfatter sourcing strategien bruk av skytjenester
	  ○ Direkte hos store utenlandske leverandører av skytjenester
	  ○ Bruk av lokale leverandører med skytjenestelevarandører som underleverandører
		Hvordan håndterer kommuner anskaffelsesprosessen ved kjøp av skytjenester
		• Anbudsinnbydelse med fastlagte kontraktsvilkår
		• Kjøp etter forhandling
		• Direkte kjøp basert på leverandørens standard vilkår
		Legger leverandøren inn tilbud på anbudsutlysninger, der tilbud på sky-tjenester inngår som et element i en løsning som omfatter mer enn sky-løsningen?

Nr	Spørsmål	Kommentarer
3	Bruker kommunen skytjenester i dag	Har leverandøren kommuner eller fylkeskommuner som kunder på sky-løsninger
4	Hvilke typer skytjenester bruker kommunen • Infrastruktur-/lagringstjenester (f.eks Dropbox, Box, Skydrive/Onedrive, Google Drive, ICloud,) • Standardapplikasjoner (f.eks. Ms Office 365, Google apps, web-basert epost) • Web-basert plattformer/fagsystemer (f.eks Fronter, It's learning) • Annet …….	Hvilke typer skytjenester kjøper kommuner • Infrastruktur-/lagringstjenester (f.eks Dropbox, Box, Skydrive/Onedrive, Google Drive, ICloud,) • Standardapplikasjoner (f.eks. Ms Office 365, Google apps, web-basert epost) • Web-basert plattformer/fagsystemer (f.eks Fronter, It's learning) • Annet …….
5	Hvis kommunen bruker skytjenester, når ble hver enkelt tjeneste tatt i bruk (angi navn på den enkelte tjeneste) • Tjeneste 1 - tidspunkt • Tjeneste 2 – tidspunkt • Tjeneste 3 – tidspunkt • ---	Er kommunesektoren et satsningsområde for leverandøren • Tjeneste 1 - tidspunkt • Tjeneste 2 – tidspunkt • Tjeneste 3 – tidspunkt • ---
6	Er det gjennomført sikkerhets- og sårbarhetsanalyser for de skytjenester som er tatt i bruk	Stilles det krav fra kommunene til at leverandøren skal tilfredsstille norsk lovgivning? • Personopplysningslovgivningen • Arkivloven • Krav til datasikkerhet mv • Krav til ISO sertifisering e.l • Annet?
7	Blir det behandlet sensitive personopplysninger i skytjenesten?	Krever kommunene særskilte tiltak knyttet til behandling av sensitive opplysninger?

Nr	Spørsmål	Kommentarer
8	Planlegger kommunen å ta i bruk nye skytjenester i nær fremtid • Hvor snart • For hvilke typer systemer og tjenester • Hvilke typer skytjenester • Når vil de enkelte tjenester bli tatt i bruk	Har leverandøren totalt sett mange «leads» eller «prospects», eller tilbud til kommunale kunder
9	Har kommunen støtt på konkrete hindringer i lovverket for bruk av skytjenester • Hvilken lovgivning er identifisert som hindring • Er det identifisert hva som må/kan gjøres for å tilfredsstille den enkelte lov ○ For bestemte typer systemer i kommunen ○ I forhold til skytjenester generelt ○ I forhold til bestemte typer skytjenester ○ For hver type system og tjeneste - angi hindring ○ Har kommunen analysert muligheten for avhjelpende tiltak i forhold til de angitte hindringene	Har Leverandøren støtt på konkrete hindringer i lovverket for bruk av skytjenester • Hvilken lovgivning er identifisert som hindring • Er det identifisert hva som må/kan gjøres for å tilfredsstille den enkelte lov ○ For bestemte typer systemer ○ I forhold til skytjenester generelt ○ I forhold til bestemte typer skytjenester ○ For hver type system og tjeneste - angi hindring ○ Har leverandøren analysert muligheten for avhjelpende tiltak i forhold til de angitte hindringene
10	Har usikkerhet hindret kommunen i å ta i bruk skytjenester • Hva består usikkerheten i • Hva har kommunen gjort for å	Har usikkerhet hos kommunen ført til at leverandøren ikke har fått anledning til å levere skytjenester som en del av tjenesten som tilbys til kommunen • Hva består usikkerheten i

Nr	Spørsmål	Kommentarer
	avklare usikkerhet • Har kommunen analysert muligheten for avhjelpende tiltak i forhold til usikkerheten • Hvilke offentlige organer har skapt usikkerhet (Riksarkivet, Datatilsynet osv.)	• Hva har leverandøren gjort for å avklare usikkerhet • Har leverandøren analysert muligheten for avhjelpende tiltak i forhold til usikkerheten Hvilke offentlige organer har skapt usikkerhet (Riksarkivet, Datatilsynet osv.)
11	Hva er driverne for at kommunen har tatt i bruk eller ønsker å ta i bruk skytjentester • Økonomi • Standardisering • Ressursdeling • Skalerbarhet og fleksibilitet • Annet	Hva oppgis som driverne for at kommune-kunder har tatt i bruk eller ønsker å ta i bruk skytjentester • Økonomi • Standardisering • Ressursdeling • Skalerbarhet og fleksibilitet • Annet
		Er det leverandøren av eget tiltak som ønsker å tilby skytjenester som leveranseplattform – uten at kunden har noe forhold til bakenforliggende plattform?
12	Internkontrollsystemer • Har kommunen etablert en internkontroll i overensstemmelse med kravene i Personopplysningsloven § 13 (etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes kvalitet). • Er tiltakene dokumentert og har kommunen et opplegg for å vedlikeholde	Internkontrollsystemer – overholdelse av personopplysningsloven. Har leverandøren blitt bedt om å fremlegge dokumentasjon i tilknytning til • Kommunens internkontroll i overensstemmelse med kravene i Personopplysningsloven § 13 (etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes kvalitet). • Er leverandørens tiltak dokumentert og har kommunen krav til et opplegg for å vedlikeholde kommunens internkontrollsystem?

Nr	Spørsmål	Kommentarer
	internkontrollsystemet. • Har kommunen innlemmet andre typer opplysninger enn personopplysninger (f. eks bedrifts- og forretningshemmeligheter og andre opplysninger underlagt taushetsplikt mv) i opplysningene som omfattes av internkontrollsystemet. • Brukes internkontrollsystemet aktivt ved vurderinger og beslutninger om å ta i bruk skytjenester • Er det utarbeidet rutiner for å inngå databehandleravtaler med andre som behandler personopplysninger på vegne av kommunen (f. eks data-driftsleverandører, konsulenter som yter driftsbistand eller feilrettingstjenester)? • Har kommunen en egen strategi for informasjonssikkerhet • Er det utarbeidet egne retningslinjer for informasjonssikkerhet • I hvilken grad er ledelse og ansatte kjent med kommunens retningslinjer for informasjonssikkerhet • Har ledelsen og de ansatte tilstrekkelig kunnskap om behandling av personopplysninger og andre taushetsbelagte opplysninger?	• Har kommunen stilt krav knyttet til andre typer opplysninger enn personopplysninger (f. eks bedrifts- og forretningshemmeligheter og andre opplysninger underlagt taushetsplikt mv) i opplysningene som omfattes av internkontrollsystemet. • Oppfatter leverandøren at internkontrollsystemet brukes aktivt ved vurderinger og beslutninger om å ta i bruk skytjenester • Krever kommunene at det inngås databehandleravtaler når leverandøren behandler personopplysninger på vegne av kommunen, • Krever kommunene at det inngås underdatabehandleravtaler med underleverandører som leverandøren benytter (f. eks data-driftsleverandører, konsulenter som yter driftsbistand eller feilrettingstjenester)? • Har kommunen en egen strategi for informasjonssikkerhet, og fremlegges denne for leverandøren for • Er det utarbeidet egne retningslinjer for informasjonssikkerhet • I hvilken grad er ledelse og ansatte kjent med kommunens retningslinjer for informasjonssikkerhet • Har ledelsen og de ansatte tilstrekkelig kunnskap om behandling av personopplysninger og andre taushetsbelagte opplysninger?

Vedlegg 4 Resultat av spørreundersøkelse og dybdeintervjuer

1. Spørreundersøkelse – kommunene

I begynnelsen av denne mulighetsstudien ble det sendt ut en spørreundersøkelse til et utvalg av kommuner. Det ble sendt ut til et utvalg av 10 store, 10 mellomstore og 10 mindre kommuner, med sikte på å innhente opplysninger om bevissthet og status vedrørende bruk av skytjenester i kommunenes IKT satsninger. Spørreundersøkelsen har resultert i 16 svar.

Spørreundersøkelsen gikk i hovedsak ut på følgende:

- Hvorvidt skytjenester er en del av kommunens IT-strategi, og om det skilles mellom forskjellige typer skytjenester
- Hvorvidt kommunen bruker skytjenester i dag, og evt. hvilke
- Om det er gjennomført risiko- og sårbarhetsanalyse for de skytjenester som er tatt i bruk
- Hvorvidt sensitive personopplysninger blir behandlet i skytjenesten
- Vet kommunene hvor dataene fysisk er lagret
- Hvorvidt kommunene har støtt på konkrete hindringer i lovverket for bruk av skytjenester
- Hva som er driverne for at kommunene har tatt i bruk eller ønsker å ta i bruk skytjenester
- Hvorvidt kommunene har et internkontrollsystem
- Om kommunene har utarbeidet rutiner for å inngå databehandleravtaler med andre som behandler personopplysninger på vegne av kommunen
- Om kommunen har utarbeidet egne retningslinjer for informasjonssikkerhet etc.

Undersøkelsen viser at det finnes både kommuner som har tatt i bruk, kommuner som planlegger å ta i bruk og kommuner som ikke har tatt i bruk skytjenester. Hvor bevisst forhold kommunene har til begrepet skytjenester er varierende og det er svært få kommuner blant de spurte, som har skytjenester som en del av sin IT-strategi.

Det er flere kommuner som har tatt i bruk skytjenester, og det er særlig utbredt innenfor skolesektoren. Innenfor skolesektoren bruker kommunene blant annet Fronter, Google Drive, Google Classroom, Google Apps og Microsoft Office 365.

En viktig del av det å ta i bruk skytjenester er å foreta en risiko og sårbarhetsanalyse («ROS-analyse»), som nærmere beskrevet i punkt 9. De fleste av kommunene som har tatt i bruk skytjenester svarer at de har foretatt en risiko vurdering, og flere viser til at det har blitt gjennomført en ROS-analyse.

Videre har de fleste av kommunene som bruker skytjenester, svart at det ikke blir behandlet sensitive personopplysninger i skytjenesten. Spørreundersøkelsen viser også at det er usikkerhet i kommunene vedrørende i hvilket land dataene fysisk blir lagret. Noen viser blant annet til at de blir lagret hos Microsoft, men ikke i hvilket land. Det skal her fremheves at Microsoft har servere i ulike land over hele verden, noe som innebærer at dataene ikke nødvendigvis da kun blir lagret innenfor Europa. Det er også veldig få av kommunene som bruker skytjenester som er klar over i hvilke land dataene fysisk blir lagret.

Når det gjelder spørsmålet i undersøkelsen vedrørende hindring i lov, svarer flertallet at de ikke har støtt på slike hindringer. Mens noen svarer at de har støtt på hindringer i arkivloven og bokføringsloven. At ikke flere svarer det sistnevnte, men kun svarer at de ikke har støtt på hindringer kan skyldes at bruk av skytjenester på nåværende tidspunkt er lite utbredt i

kommunene. Samt at det i hovedsak er innenfor skolesektoren at skytjenester har blitt tatt i bruk av kommunene.

Det ovennevnte er nok også grunnen til at flere av kommunene hevder at usikkerheten rundt lovligheten av bruk av skytjenester, ikke har vært til hinder for å ta i bruk skytjenester. I tillegg skal det påpekes at det er svært få kommuner som har svart på akkurat dette spørsmålet.

Driverne i kommunene for at de har tatt i bruk eller ønsker å ta i bruk skytjenester er økonomiske faktorer, ønske om å i større grad å fokusere på tjenesteutvikling, skalerbarhet og fleksibilitet og økt tilgjengelighet til løsninger. Imidlertid er det også flere kommuner som hevder at det ikke vil være noe rimeligere å ta i bruk skytjenester, da skytjenester er høyt priset, samt at noen hevder det totalt sett koster like mye som å drifte selv. Bakgrunnen for det sistnevnte oppgis blant annet at man ikke kan si opp ansatte fordi, til tross for at man går over til en skyløsning, vil noe bli liggende igjen lokalt som man må ha ansatte til å drifte.

De fleste kommunene som har svart på spørreundersøkelsen hevder de har et internkontrollsystem på plass. Imidlertid hevder flere av kommunene at de er usikre på om internkontrollsystemene deres i tilstrekkelig grad tilfredsstiller kravene i personopplysningsloven § 14. i tillegg fremgår det at det er svært få av kommunene som bruker internkontrollsystemet aktivt ved vurderingene og beslutningene om å ta i bruk skytjenester.

Som nevnt tidligere, er det et krav etter personopplysningsloven at en behandlingsansvarlig (kommune) som benytter databehandler(e), må ha databehandleravtale på plass. Dette innebærer blant annet at kommunen må inngå databehandleravtale med en eventuell leverandør av skytjenester. De fleste av kommunene som har svart på dette spørsmålet, svarer at det er utarbeidet rutiner for å inngå databehandleravtaler med andre som behandler personopplysninger på vegne av kommunene. Imidlertid skal det påpekes at det er flere av kommunene som har deltatt i spørreundersøkelsen som ikke har svart på dette spørsmålet. Det er usikkert hvorfor dette spørsmålet ikke har blitt besvart og det kan ikke utelukkes at det faktisk mangler databehandleravtaler som skulle vært på plass.

Som tidligere nevnt er det et krav etter personopplysningsloven § 13 at den behandlingsansvarlige gjennom planlagte og systematiske tiltak skal sørge for tilfredsstillende informasjonssikkerhet. Dokumentasjonen av informasjonssikkerheten skal i tillegg være tilgjengelig for medarbeiderne hos den behandlingsansvarlige, samt for Datatilsynet. De fleste av kommunene som har besvart spørreundersøkelsen svarer at det er utarbeidet retningslinjer for informasjonssikkerhet for deres kommune.

Til tross for at flere av kommunene hevder at usikkerheten rundt lovligheten av bruk av skytjenester, ikke har vært til hinder for å ta i bruk skytjenester, er vårt inntrykk av svarene på spørreundersøkelsene at det er stor usikkerhet i kommunene rundt akkurat dette. De fleste kommunene synes heller ikke å være klar over at personopplysningsloven i utgangspunktet ikke er til hinder for bruk av skytjenester i kommunen. Selv sensitive personopplysninger kan legges ut i skytjenester – bare man har gjort de riktige grepene før dette gjennomføres.

2. Dybdeintervju – kommuner

2.1. Dybdeintervju 1 – Alta kommune

I forbindelse med denne mulighetsstudien har vi i tillegg til spørreundersøkelsen gjennomført tre dybdeintervjuer om bruk av skytjenester med utvalgte kommuner som allerede har tatt i bruk skytjenester. Under dybdeintervjuene ble det tatt utgangspunkt i de samme

spørsmålene som i spørreundersøkelsen som ble sendt ut til en rekke kommuner. Vårt inntrykk etter dybdeintervjuene er at kommunene har svært ulikt syn på bruk av skytjenester.

En av kommunene vi har intervjuet var Alta, de har tatt i bruk skytjenester i form av e-post tjenester til bruk for grunnskoleelever og lærere. I utgangspunktet begynte Alta kommune å ta i bruk skytjenester i et større omfang enn kun til bruk i skole. Imidlertid ble dette videre prosjektet stoppet da kommunen skiftet IT-leder. Planen var å ta i bruk Microsoft Office 365. Det var i utgangspunktet mailkontoer som skulle over til skyen, men disse er migrert tilbake til kommunen og ble ikke flyttet ut i skyen.

Noe av grunnen til at prosjektet ble stoppet, var manglende IT-strategi samt at kommunen ikke ønsket å gå over til bruk av skytjenester av økonomiske årsaker. Skytjenester ble vurdert som dyrt fordi alt ikke kunne flyttes ut i nettskyen og IT-avdelingen i kommunen ønsker å ha fokus på å få orden på egen drift og stabilitet av IT-systemene. For øvrig var det stor skepsis til bruk av skytjenester, blant annet på grunn av overføring av data til andre land og ikke minst skytjenesteleverandørens omfattende bruk av underleverandører.

Skytjenesten som faktisk blir brukt i dag, har vært i bruk i ca. 4 år. I følge kommunen, skal sensitive opplysninger i prinsippet ikke overføres via de skytjenester som den benytter. Det er en policy i kommunen som sier at sensitive personopplysninger ikke skal inngå i e-postkorrespondansen mellom elever og lærere.

For øvrig etterlyser Alta kommunen bedre råd og veiledning fra sentrale myndigheter med hensyn til hva som er akseptabel bruk av skytjenester.

2.2. Dybdeintervju 2 – Narvik kommune

Det andre dybdeintervjuet som ble foretatt var av Narvik kommune som i stor grad har tatt i bruk skytjenester. Narvik kommunen har tatt i bruk Google Apps, hvor de blant annet benytter seg av dokumenter, elektroniske skjemaer, regneark og e-post. Kommunen har tatt i bruk flere og flere av verktøyene som tilbys gjennom Google Apps. I hovedsak er det alle i administrasjonen, enhetsledere og alle organer innad i kommunen som har en administrativ funksjon som benytter seg av Google Apps.

Det er særlig verktøyet som heter «Dokumenter» som blir brukt i stor grad. Innad i kommunen er det strenge instrukser på at en ikke skal behandle personsensitiv informasjon i verktøyet Dokumenter. Blant annet får ikke lærere bruke skytjenestene til å behandle elevinformasjon, som f.eks. sykefravær. Dette behandles i egne systemer, kommunen benytter kun fagsystemer som driftes lokalt i egen lukket sone til behandling av sensitive personopplysninger.

Under intervjuet fremgikk det også at bruk av skytjenester er en del av kommunen sin strategi, hvor det blant annet fremgår at bruk av internettbaserte tjenester skal vurderes når dette er hensiktsmessig og kostnadsbesparende. Kommunen skiller også mellom hva som kan legges i skyen og ikke, sensitive personopplysninger skal ikke lagres i nettskyen.

Kommunen har foretatt en grundig risiko og sårbarhetsanalyse for bruk av Google Apps og har blant annet hatt jevnlig dialog med Datatilsynet. I tillegg fremgår det av databehandleravtalen at plasseringen av data skal være innenfor EU. Kommunen har også adgang til å få innsyn i Google sin revisjonsrapport utarbeidet av tredjepart, vedrørende IT-sikkerhet.

Kommunen har videre identifisert personvernlovgivningen og arkivloven som hindring for bruk av skytjenester, men har ikke vært i kontakt med riksarkivaren. Imidlertid har kommunen en rekke fagsystemer som benyttes av de ulike tjenestene og kommunen har foreløpig ikke identifisert noe behov for å lagre arkiv i skyen.

Driverne for at kommunen har tatt i bruk skytjenester er økonomi, standardisering, ressursdeling, skalerbarhet og fleksibilitet. De fremhevet blant annet at de gjennom skytjenester har god tilgang til samhandlingsverktøy, samt at det er enklere å forstå lisensieringen til skytjenestene. I tillegg har skytjenestene et veletablert brukergrensesnitt og er tilgjengelig både på jobb og hjemme.

Generelt har kommunen etter at de tok i bruk skytjenester blitt mer positive til skytjenester, og det har vært lite behov for å lære opp de ansatte fordi systemene oppfattes som enkle å bruke.

2.3. Dybdeintervju 3 – Moss kommune

I forbindelse med denne utredningen har vi også vært i en egen samtale med Moss kommune, som har tatt i bruk skytjenester. Moss har lagt store deler av sine systemer ut i nettskyen. Moss kommune mener at det på kort sikt ikke er rimeligere å gå over til nettsky, imidlertid på lang sikt vil dette lønne seg. Dette fordi det i en overgangsfase ofte vil være nødvendig med doble lisenser innenfor enkelte områder før alt er lagt ut i nettskyen. For å kunne gjennomføre prosjektet har kommunen hatt en tett dialog med Datatilsynet underveis. De mener at det største hinderet for å ta ut full gevinst ved bruk av skytjenester er arkivloven.

For å kunne gå over til nettskyen har det løpende blitt foretatt risikovurderinger av de enkelte elementer som flyttes, etter hvert som de i større og større grad har tatt i bruk nettskyløsninger. De har blant annet i samråd med DNV GL gjennomført en kvalitativ risikovurdering av nettskytjenesten Office 365 fra Microsoft.

3. Dybdeintervju - leverandører

I forbindelse med denne mulighetsstudien har det også blitt gjennomført dybdeintervju av fire leverandører av skytjenester; Evry, Microsoft, Visma og Google Norway.

Alle disse fire leverandørene selger skytjenester til kunder i Norge, og også til kommunesektoren. Leverandørene som ble intervjuet, fikk i forkant oversendt spørreundersøkelsen som har blitt sendt ut til kommunene. Hensikten med intervjuene var å få leverandørene sine synspunkt på kommunenes bevissthet og status vedrørende bruk av skytjenester i kommunenes IKT satsninger.

Leverandørenes hovedsynspunkt var at det var stor variasjon i kommunene i forhold til hvor bevisste kommunene er rundt bruk av skytjenester og at det er varierende forståelse av hva som ligger i begrepet skytjenester. Enkelte av leverandørene mener at det er mye usikkerhet og ubegrunnede oppfatninger i kommunene vedrørende lovligheten av bruk av skytjenester og at dette i hovedsak skyldes frykt, usikkerhet og tvil. Usikkerheten rundt bruk av skytjenester har ikke nødvendigvis grunnlag i hvorvidt lovgivningen tillater bruk av skytjenester eller ikke.

Flere av leverandørene er også av den oppfatningen at det i hovedsak er de største kommunene som har en IT-strategi hvor bruk av skytjenester inngår, og at kommunene i hovedsak ønsker å bruke skytjenester på det som ikke omfattes av kjerneoppgavene til

kommunen. Videre er kommunene mest opptatt av applikasjonene i seg selv og ikke den bakenforliggende plattformen. De er også opptatt av integrasjonsgrensesnitt.

Leverandørene ga også klart uttrykk for at de ønsker å levere skytjenester til kommunene, og at de i enda større grad kommer til å gå over til å levere tjenester basert på nettsky. I dag legges det ut veldig få offentlige anbud som tilrettelegger for at leverandørene kan tilby sine skytjenester. Slik konkurransegrunnlagene er utformet, vil det være umulig eller svært vanskelig for kunden å sammenligne prisene for skytjenester med IKT-tjenester basert på en mer tradisjonell plattform. Dette gjør det vanskelig for leverandørene å kunne tilby skytjenester ved offentlige anbud. Leverandørene ser imidlertid at det har begynt å skje en utvikling på dette området, særlig i de anbudene hvor kunden etterlyser funksjonalitet i stede for tekniske krav.

Videre påpeker leverandørene at ut i fra regelverket så er det i hovedsak arkivloven som er det største problemet, dette er blant annet en av grunnene til at et par av leverandørene satser på lagring i Norge i stede for i andre land. En annen utfordring oppgis å være behandling av sensitive personopplysninger i skytjenestene, men det største problemet her er at Datatilsynet har vært opptatt av at sensitive personopplysninger skal være lagret i separate fysiske kontainere for lagring av data.

En av leverandørene fortalte også at Norge er et av de landende i den vestlige verden som i minst grad tar i bruk skytjenester i kommunal og offentlig sektor.

Vedlegg 5 Sjekkliste ved anskaffelse av skybaserte løsninger

	SJEKKLISTE	KOMMENTAR
	Forberedelser	
1	Identifiser hvilke typer opplysninger man ønsker å benytte skytjenester for.	
2	Identifiser hvilke regelverk som gjelder for opplysningene – ta særlige hensyn hvis arkivloven eller bokføringsloven får anvendelse.	
3	Skaff oversikt over hvordan flyten av opplysninger vil være (hvor blir dataene overført, direkte og indirekte).	
4	Skaff oversikt over hvorfra opplysningene vil bli lest/aksessert/behandlet.	
5	Skaff oversikt over hvordan IT-sikkerheten er ivaretatt i systemet som vurderes. Mye av dette kan typisk være beskrevet i whitepapers etc. som leverandøren publiserer på nettet, men innholdet der er ofte ikke tilstrekkelig. For å få nok informasjon til å kunne vurdere sikkerheten kan det være nødvendig med tilgang til annen dokumentasjon, slik som revisjonsrapporter fra uavhengige tredjeparter etc. Leverandøren vil normalt gå med på å dele slik informasjon med kunden, noen ganger mot at kunden signerer en konfidensialitetsavtale med leverandøren.	
6	Forsikre deg om at IT-sikkerheten tilfredsstiller personopplysningsloven krav (evt. andre relevante rettsregler avhengig av hva slags type informasjon som prosesseres).	
7	Forsikre deg om at det også ut fra et forretningsmessig ståsted og ut fra ditt eget foretaks risikoprofil og kriterier for aksept av risiko vil være ok å ta i bruk tjenesten.	
8	Forsikre deg om at du som kunde fullt ut eier dataene som lagres og at leverandøren ikke kan utnytte de for andre formål enn det som spesifikt er avtalt med deg.	
9	Forsikre deg om at dataene blir slettet når du gir beskjed om dette og/eller når avtalen med leverandøren avsluttes.	
10	Gjennomfør en risikovurdering i samsvar med personopplysningslovens krav og eForvaltningsforskriften og sørg for at denne dokumenteres.	
11	Ha klare kriterier for aksept av risiko/restrisiko.	
12	Vurder om det er behov for melding til Datatilsynet, fordi data overføres til, eller er tilgjengelig og behandles fra land utenfor EU/EØS.	
	Inngåelse av avtale	
1	Vær forberedt på at det er lite rom for forhandlinger, spesielt når avtalen inngås med store skytjenesteleverandører. Men stå samtidig fast på de krav	

	SJEKKLISTE	KOMMENTAR
	som følger av norsk rett. De fleste leverandører vil ha et incitament til å levere tjenester som det er lovlig å bruke, ettersom det motsatte vil kunne påvirke leverandørens muligheter for å selge tjenesten.	
2	Forsøk å få en rett til å terminere avtalen om det skulle bli avdekket at leverandøren ikke opererer på en måte som tilfredsstiller kravene i norsk lovgivning, evt. slik disse kravene kommer til uttrykk i avtalen.	
3	Vær på vakt etter bestemmelser som gir leverandøren en ensidig adgang til å endre (deler av) kontraktens innhold, typisk underliggende dokumentasjon uten å be om samtykke.	
4	Sørg for at forhold som er viktige for å sørge for ivaretakelse av sikkerhet er på plass i avtalen. Eksempler på dette er krav til sikkerhet, sanksjoner ved brudd på slike, back-up/failover-løsninger etc.	
	Forhold å være spesielt oppmerksom på vedrørende personvern	
1	Sørg for at du har oversikt over i hvilke land personopplysningene behandles.	
2	Husk at «behandling» omfatter mer enn lagring – også utvikling, drift etc fra utland kan gjøre at reglene om overføring til tredjeland får anvendelse.	
3	Sørg for at du leser leveranseavtalen grundig slik at du vet i hvilke land opplysninger vil bli lagret – og like viktig – i hvilke land leverandørens ansatte befinner seg når de utfører tjenester som omhandler behandling av personopplysninger. Det samme gjelder for avtalens formuleringer om hvor underleverandører befinner seg.	
4	Skaff deg oversikt over hvor leverandørens representanter med potensiell tilgang til personopplysningene befinner seg. Om dette er i andre land enn det som er nevnt under punkt 1, må oversikten over land utvides tilsvarende.	
5	Det er et krav etter norsk rett at det er mulighet for å gjennomføre sikkerhetsrevisjoner hos leverandøren. Datatilsynet har i sitt brev til Narvik kommune påpekt at kommunen jevnlig, for eksempel årlig, må sørge for at sikkerhetsrevisjonen blir gjennomført. Undertiden kan det å få tilgang til leverandørens eksterne revisors rapporter vedr. sikkerhetsevalueringer være tilstrekkelig, men dette kan ikke tas som en generell regel og må derfor vurderes konkret jf. Datatilsynet sitt brev til Moss kommune. Avgjørende er om man gjennom revisjonsrapporten får tilgang på informasjon som gjør det mulig å fastslå om lovens og avtalens krav overholdes eller ikke. Kommunen	

	SJEKKLISTE	KOMMENTAR
	kan/bør eventuelt stille krav til skytjenesteleverandøren om at kommunen skal ha rett til å kreve at en tredjepart utfører revisjon av den aktuelle tjenesten.	
6	Overføring av personopplysninger til utlandet må skje i samsvar med bestemmelsene i personopplysningsloven kapittel 5 og personopplysningsforskriften kapittel 6. Husk at overføring i visse tilfelle forutsetter at søkes om tillatelse fra Datatilsynet (personopplysningsloven § 30, annet ledd).	
7	Påse at personopplysninger ikke overføres til land som ikke er forhåndsgodkjent av Datatilsynet, med mindre overføringen skjer i henhold til Safe Harbor-instituttet eller EUs mal for databehandleravtaler, BCR (Binding Corporate Rules) eller tilsvarende gyldig overføringsgrunnlag. Det understrekes at Safe Harbor-instituttet for tiden er under et visst press fra EU-parlamentet og at f. eks Tyskland stiller spesielle vilkår knyttet til bruk av Safe Harbor avtalene som grunnlag for en overføring til USA.	
8	Merk at ikke alle amerikanske selskap er underlagt Safe Harbor. Du må få bekreftet at leverandøren du forhandler med er en såkalt «Safe Harbourite» og at leverandørens tilslutning til instituttet også omfatter de kategorier av data som det er aktuelt at denne behandler.	
9	Påse at leverandøren har en plikt til å informere deg som kunde om brudd på sikkerheten som innebærer at personopplysninger har kommet eller kan komme på avveie. I gitte situasjoner vil du kunne ha en selvstendig plikt til å informere Datatilsynet (og de personene den kompromitterte dataen relaterer seg til) om dette.	
10	Sørg for å ha en databehandleravtale på plass som ivaretar ovennevnte.	
	Øvrige forhold	
1	Sett deg inn i hva avtalen sier om responstider ved feilmelding, oppetidsgarantier etc. og vurder om dette er tilfredsstillende for din virksomhet.	
2	Sett deg inn i hvor enkelt/komplisert det vil være å migrere kundedataen til løsninger som tilbys av andre leverandører. Enkelte sky-baserte IT-tjenester er kjent for å kunne (bevisst eller ubevisst) skape en såkalt lock-in-effekt som innebærer at terskelen for å ta i bruk alternative tjenester blir høy.	
3	Sjekk hvordan tap av data reguleres i kontrakten. Ofte tar ikke leverandøren ansvar for dette overhodet. Det må vurderes om dette er akseptabelt for din virksomhet. Verdt å merke seg for kommuner er at for dårlig sikring mot	

	SJEKKLISTE	KOMMENTAR
	eventuelt tap av data vil kunne komme i konflikt med plikten til å oppbevare visse kategorier av data i en gitt periode.	
4	Sjekk om avtalen gir leverandøren mulighet til leveransenekt ved manglende betaling (selv om betalingsmisligholdet ikke er vesentlig). Mange leverandører opererer med slike krav, noe som kan skape utfordringer om avtalen ikke endres på dette punkt.	