Oslo

Byrådsavdeling for finans

Veileder for sikker etablering av skytjenester

Versjon 1.0
November 2021

Foto: Roman Odintsov (Pexels

Om veilederen

Bakgrunn

Skytjenester blir stadig mer aktuelle ved etablering av IKT-tjenester. Virksomheter i Oslo kommune vil ha ulike behov og ulikt utgangspunkt for vurdering av skytjenester. Det store flertallet vil se til skyen for å kjøpe ferdige applikasjonstjenester som ansatte eller innbyggere kan benytte direkte. Andre vil kanskje ønske å flytte eksisterende applikasjoner til skyen, mens en tredje gruppe vil ønske å benytte skyen for utvikling av egne, helt nye, IKT-tjenester til ansatte eller innbyggere. Uavhengig av hvilken gruppe man faller inn under så er det en rekke vurderinger som må gjøres før etablering av tjenester i skyen for å sikre et akseptabelt risikonivå.

Formålet med veilederen

Formålet med veilederen er å bidra til å sikre at det ikke tas i bruk infrastruktur eller plattform i skyen som medfører uakseptabel risiko for kommunens virksomhet når det gjelder informasjonssikkerhet og personvern. Selv om man med skytjenester overlater mange oppgaver til en ekstern leverandør, så er det viktig å være klar over at ansvaret for sikkerhet og personvern aldri kan delegeres bort, ei heller ved bruk av skytjenester.

Etablering og bruk av infrastruktur og plattform i sky har mange fellestrekk med etablering og bruk av tradisjonelle IKT-løsninger. Fremgangsmåten for å vurdere skytjenester vil av den grunn ligne på fremgangsmåten for å vurdere tradisjonelle IKT-løsninger. Likevel vil det være særskilte vurderinger som må gjøres bare for skytjenester. Denne veilederen fokuserer på disse særskilte vurderingene som må gjøres for skytjenester, men tar med en del ikke-skyspesifikt stoff for å gjøre veilederen mer leservennlig.

I dette dokumentet får du en veiledning i oppgaver som bør eller må utføres i vurderingsprosessen rundt etablering av infrastruktur og plattform i sky. Dette inkluderer å sikre etterlevelse av lover, regelverk og kommunens styrende dokumenter, samt å gjennomføre nødvendig risikovurdering.

Målgruppe

Dokumentet skal gi veiledning til ledere og medarbeidere som er systemeiere eller er involvert i arbeidet med etablering, utvikling, forvaltning og drift av skytjenester. Erfaring fra noen av disse områdene vil være fordelaktig for å få best mulig utbytte av dokumentet.

Anvendelsesområdet

Veilederen vil videreutvikles, og omfanget av den er noe avgrenset i første versjon. Denne utgaven er rettet mot plattform som en tjeneste (PaaS) og infrastruktur som en tjeneste (IaaS), og etablering av kommunens egne tjenester basert på disse. Mye av innholdet kan imidlertid være nyttig også ved anskaffelse av programvare som en tjeneste (SaaS fra en

applikasjonsleverandør). Mer konkret veiledning rettet mot anskaffelse og bruk av applikasjoner basert på SaaS kan bli tatt med i en senere versjon av veilederen, evt. en separat veileder.

Veilederen tar utgangspunkt i at virksomhetene benytter kommunens eksisterende avtaler (se kapittel 7). Dersom det gjøres anskaffelser utover disse avtalene så vil veilederen også være relevant, men dette er ikke en veileder i hvordan man gjennomfører selve anskaffelsene.

Det jobbes kontinuerlig med forbedring av veilederen, og nye versjoner vil komme fortløpende. En liste over forbedringsforslag er opprettet og vurderes fortløpende for kommende versjoner. Har du innspill til forbedringer så ta kontakt med Seksjon for informasjonssikkerhet og IKT (ISI) i Byrådsavdeling for finans.

Veileder for sikker bruk av skytjenester

Innhold

1 Introduksjon til skytjenester

1.1 Hva er skytjenester?

Skytjenester er IKT-tjenester som leveres over internett. Datatilsynet beskriver skytjenester slik:

> «Skytjenester (*cloud computing*) er en samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett.»[1]

Skytjenester skiller seg fra tradisjonelle IKT-løsninger på den måten at skytjenestene er dynamisk skalerbare etter behov og betaling skjer etter forbruk av prosessorkraft, lagring, og datakommunikasjon. Kunden kan legge til og fjerne tjenester og kapasitet via selvbetjening, i motsetning til i et tradisjonelt leverandørforhold der man kanskje må endre på avtaler, godkjenne investeringer osv. for å få gjort tilsvarende endringer. En annen forskjell er at vedlikehold av en skytjeneste skjer sentralt og ikke ute på hver enkelt kundes lokale servere i egen infrastruktur.

Normalt gir skytjenester flere fordeler:

- Enkelt å tilpasse kapasitetsbehov, ved at prosesserings- og lagringskapasitet lett kan skaleres opp eller ned ettersom behovet endrer seg.
- Rask tilgang til den nyeste teknologien og ny funksjonalitet.
- Drift og vedlikehold av datarom, lagringssystemer, servernettverk og fysiske servere gjøres av leverandøren. Dette innebærer besparelser for kunden i form av arealbruk, maskinvareinvesteringer og behov for spesialistkompetanse.
- Store leverandører av skytjenester kan investere mer i sikre løsninger og kan tilby bedre sikkerhet i disse enn mange mindre virksomheter kan klare på egen hånd.

Samtidig er det knyttet noen ulemper til skytjenester:

- Skytjenesteleverandørenes avtalevilkår er i høy grad standardiserte, og i praksis ofte umulige å endre når det gjelder store utenlandske leverandører.
- Lover og regler kan legge begrensninger på hvor (geografisk) det er anledning til å behandle og lagre informasjon.
- Kunden er avhengig av en eller flere leverandører, og har selv mindre kontroll over tjenesten.
- Man er helt avhengig av tilgang til internett for å benytte tjenesten.
- Det kan være mer komplisert å ivareta sikkerhetskrav i en delt ansvarsmodell.

[1] https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/skytjenester/

- Kunden må på forhånd tenke gjennom ulike livssyklusbehov og sørge for at disse er ivaretatt i avtalen som inngås. For eksempel eierskap til data ved flytting til annen leverandør.

1.2 Typer av skytjenester

Det finnes flere typer skytjenester, og det er spesielt to akser de kategoriseres etter, nemlig tjenestemodell og leveransemodell. Følgende beskrivelser er laget av Digitaliseringsdirektoratet. Se deres nettsider for mer utfyllende beskrivelse av egenskaper ved skytjenester, og ulike tjeneste- og leveransemodeller[2].

1.2.1 Tjenestemodeller

Skytjenester leveres som løpende tjenester over nettet ("as a service"). Det er tre hovedtyper:

- **SaaS (Software as a Service)**. Kunden får tilgang over internett til applikasjoner som kjører i et datasenter i skyen. Eksempler på tjenester er kontorstøttetjenester som tekstbehandling og regneark, regnskapssystemer eller ulike saksbehandlingssystemer. Kunden kan ikke påvirke hvordan applikasjonen, nettverk, servere, operativsystemer eller lagring er satt opp.
- **PaaS (Platform as a Service)**. Levering av driftsmiljø (plattform) hvor kunden kan utvikle og levere applikasjoner selv. Plattformen kan inneholde database, utviklingsverktøy, testverktøy osv.
- **IaaS (Infrastructure as a Service)**. Omfatter alle dataressursene man tradisjonelt vil ha i sitt eget datasenter, dvs. servere, nettverk og lagring. Kunden kan selv sette opp virtuelle servere, velge mellom ulike typer lagring, og til en viss grad konfigurere hvordan nettverket mellom de virtuelle serverne settes opp.

De mest kjente plattformene for PaaS- og IaaS-tjenester er Microsoft Azure, Amazon Web Services (AWS) og Google Cloud.

1.2.2 Leveransemodeller

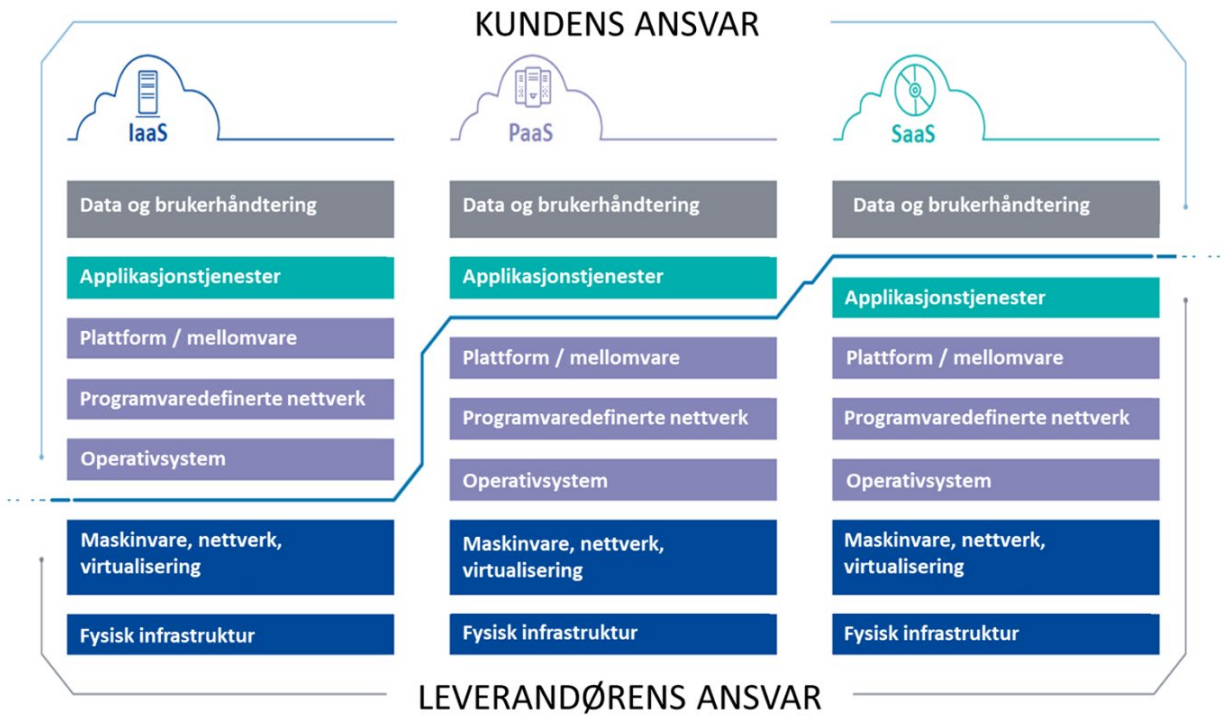
Skytjenester leveres på ulike måter:

- **Allmenn sky** (Public Cloud) er standardiserte tjenester som blir solgt på det åpne markedet. Tjenestene er stort sett like for alle kunder. Mange leverandører tilbyr programvare i den allmenne skyen. Eksempler på slike tjenester er saksbehandlingssystemer, økonomisystemer osv.
- **Privat sky** (Private Cloud) er en lukket skytjeneste som er avgrenset til en virksomhet. Leverandøren kan for eksempel sette opp et eget teknisk miljø for kunden.
- **Gruppesky** (Community Cloud) er en lukket skytjeneste som er avgrenset til en gruppe virksomheter, eksempelvis et samarbeid mellom flere kommuner. Leverandøren vil sette opp et eget teknisk miljø til gruppeskyen.
- **Hybridsky** (Hybrid Cloud) er en kombinasjon av de ulike skytjenestene over.

[2] https://www.anskaffelser.no/hva-skal-du-kjope/it/skytjenester-cloud

1.3 Skysikkerhet – omfang og ansvar

Det er viktig å være klar over at en virksomhet som setter ut tjenester til skyleverandører, kun setter ut oppgaver og ikke kan fraskrive seg ansvaret for IKT-tjenester som leveres til innbyggere, næringsliv eller ansatte. Det kan videre være en utfordring å forstå og håndtere oppgavefordelingen mellom skytjenesteleverandør og virksomheten (kunden), spesielt fordi denne varierer med tjenestemodell. Det er svært viktig å forstå nøyaktig hvem som er ansvarlig for hva i en skybasert tjeneste (se tegning under). Ved IaaS har kunden flest oppgaver, ved SaaS færrest. Jo nærmere man beveger seg SaaS hvor flere oppgaver faller på leverandøren, desto viktigere kan avtalen bli for kunden.



(Kilde: Information Security Forums rapport «Using Cloud Services Securely»)

Kunden har alltid ansvar for å sikre informasjonen som behandles, og for å styre brukertilganger. Ved PaaS, og spesielt IaaS, har kunden slik tegningen viser flere sikkerhetsoppgaver i totalløsningen enn ved SaaS. Mange feil og svakheter har oppstått som følge av at kunden ikke har forstått omfanget av ansvaret sitt ved bruk av de ulike tjenestemodellene (IaaS, PaaS og SaaS).

2 Virksomhets- og leverandørstyring

2.1 Ansvar ved bruk av skytjenester i kommunen

Kommunens styrende dokumenter innenfor IKT og informasjonssikkerhet/personvern[3] gjelder ved etablering og bruk av skytjenester på samme måte som for etablering og bruk av tradisjonell IKT.

Virksomheten som etablerer skytjenester, enten det gjelder etablering av en ny plattform eller en ny tjeneste på en eksisterende plattform, er ansvarlig for tjenestens informasjonssikkerhet og personvern både ved etablering og i hele tjenestens levetid. I dette inngår blant annet

- at ansvar og definerte oppgaver for systemeier ivaretas
- at eventuell delegering av oppgaver og myndighet til systemforvalter er basert på skriftlig forvaltningsavtale (anbefalt mal[4]) eller annen skriftlig avtale
- at behandling av informasjon i skytjenesten er innenfor virksomhetens definerte akseptable risiko, alternativt at risikovurderinger er forelagt og godkjent av virksomhetens ledelse. Behandlingen skal også være i henhold til føringer om akseptabel risiko fra respektiv byrådsavdeling dersom slike finnes. Tilstrekkelige sikkerhetstiltak, f. eks. tilgangskontroll, er iverksatt basert på risikovurdering.

Ledere har ansvar for informasjonssikkerhet og personvern innenfor sitt ansvarsområde. Ledere må akseptere risiko og godkjenne tiltak iht. risikovurderinger som ofte vil være gjennomført av medarbeidere.

2.2 Styring av forhold til leverandør

Som nevnt i kap. 1.3 «Skysikkerhet – omfang og ansvar» innebærer bruk av skytjenester ofte en annen ansvarsfordeling enn ved bruk av en tradisjonell driftsleverandør, hvor man ofte i større grad kan forhandle om innholdet i en kontrakt. Nedenfor går vi gjennom noe av det virksomheten bør se på når skytjenester skal tas i bruk.

2.2.1 Leverandørvurderinger

Virksomheten må før etablering av skytjenester gjennomføre nødvendige vurderinger av aktuelle leverandører basert på

- Tjenestetilbud
- Lokasjon, både for leverandør, datahaller og supportpersonell
- Tilgjengelige revisjonsrapporter
- Tekniske beskrivelser
- Informasjon om finansiell stilling.

---

[3] Reglement for informasjons- og kommunikasjonsteknologi og informasjonssikkerhet i Oslo kommune (IKT-reglementet), Instruks for informasjonssikkerhet, Instruks for virksomhetsstyring.

[4] Revideres 2022, denne lenken vil da antagelig ikke lenger fungere

- I hvilken grad leverandøren gir tilgang til logger, rapporter og eventuelt annet materiale som virksomheten kan trenge for å dokumentere eget samsvar med lover og regler som behandlingen blir underlagt.

2.2.2 Avtaler

Skytjenester er basert på fleksibel deling av ressurser for å oppnå stordriftsfordeler. Dette medfører at avtaler ofte er sterkt standardiserte og rigide. Det er viktig å forsikre seg om at vilkår og betingelser i avtalen gjør det mulig for virksomheten å sikre etterlevelse av lover, forskrifter og kommunens egne styrende dokumenter.

Dersom dette i utgangspunktet ikke er mulig, kan virksomheten:

- Prøve å få tilpasset betingelsene
- Iverksette kompenserende tiltak (hvis mulig)
- Eventuelt avstå fra å bruke tjenesten.

Virksomheten må ha oversikt over alle deler av vilkår og betingelser som inngår i avtalen – dette kan være utfordrende fordi standardvilkår og –betingelser kan referere mange ulike nettsteder og -sider som igjen refererer andre nettsider.

Avtalen er virksomhetens eneste garanti for et definert servicenivå og forpliktelser fra leverandøren, og hovedverktøyet for å ha kontroll på skytjenesten fra leverandøren. Se råd angående avtaler i kapittel 6, Skytjenesteavtaler.

2.2.3 Revisjoner gjennom livsløpet

Revisjoner er sentrale for å bevise eller motbevise samsvar med lover og regler og andre krav, og skal dokumentere dette. Informasjon fra revisjoner kan imidlertid også brukes for å støtte egne risikobeslutninger som ikke nødvendigvis er relatert til samsvar. Revisjoner er dermed viktige styringsverktøy for ledere og systemeiere gjennom hele perioden en virksomhet bruker en IKT-tjeneste.

Omfang av revisjoner kan variere. Det er viktig at man er bevisst på omfang når man planlegger en revisjon eller leser en revisjonsrapport. En revisjon kan omfatte en hel industribedrift - eller bare kantinen.

Hvordan påvirkes revisjoner ved bruk av skytjenester?

Skytjenester er vanligvis basert på deling av ressurser, og det kan være uoverkommelig for en leverandør å håndtere et stort antall kunder som ønsker å revidere selv. Virksomheter som etablerer skytjenester, vil derfor i større grad måtte basere seg på tredjeparts (dvs. uavhengige) revisjonsrapporter eller sertifikater fra leverandørene fremfor å utføre leverandørrevisjoner selv. Leverandørene tilbyr ofte slik dokumentasjon i forbindelse med anskaffelsen. Dette kan for eksempel være tredjeparts revisjonsrapporter som sannsynliggjør at leverandøren overholder

sine forpliktelser. Slike rapporter bør følge bransjestandarder som for eksempel ISAE 3402 og CSA STAR, ha et klart definert omfang og liste opp hvilke kontrolltiltak som er evaluert og implementert.

Virksomheten bør ha kartlagt hvilke eventuelle andre typer informasjon de kan ha behov for fra leverandøren i tillegg til revisjonsrapportene, f.eks. kopi av ulike logger som virksomheten behøver for å dokumentere egen etterlevelse av lover og regler.

2.3 Etterlevelse av forpliktelser

Samsvar (compliance) omfatter krav til at virksomheten er bevisst og etterlever sine forpliktelser, i henhold til for eksempel lover, regelverk, kontrakter og bransjekrav. Eksempler på kontrakter og bransjekrav kan være hhv. avtaler med leverandører, og tilknyttede kravsett som *Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten* (Normen).

Virksomhetens normale internkontroll skal omfatte prosesser og rutiner for å oppfylle disse forpliktelsene, samt rutiner for å oppdage om prosessene og rutinene ikke følges. Internkontrollen skal omfatte både oppfølging av skyleverandøren og egen virksomhet.

Hvordan endres krav til samsvar ved bruk av skytjenester?

Krav til samsvar med lover, forskrifter mm. ved anvendelse av skytjenester følger den delte ansvarsmodellen (ref. kapittel 1.3). Leverandør og kunde har ansvar for hver sine oppgaver knyttet til samsvar. Det presiseres igjen at en virksomhet i kommunen alltid har det fulle ansvaret for sin bruk av skytjenester – dette kan ikke delegeres til en leverandør.

Aktiviteter for å sikre etterlevelse av forpliktelser ved bruk av sky må ta høyde for den ensidige retten mange leverandører påberoper seg til å gjøre løpende endringer i vilkår, betingelser og funksjonalitet. I tillegg er det med skytjenester økt risiko for at medarbeidere kan gjøre uheldige valg mht. lagring av informasjon i ukjente tjenester i andre land, eller at de tar i bruk funksjoner som medfører betydelige kostnader. Dette siste som følge av at

- det er ikke fysiske servere og installasjoner involvert som må bestilles av en intern IT-avdeling,
- det er ikke nødvendigvis etablert gode endringshåndterings- og godkjenningsrutiner i nye team som bruker skytjenester,
- og det er enkelt for en medarbeider å utføre endringene selv – «med ett klikk».

Bruk av skytjenester kan derfor fordre en mer kontinuerlig prosess for oppfølging av forpliktelser. En revisjon mot sikkerhets- og personvernkrav én gang i året er ikke godt nok. Det må finnes kontrollrutiner med definerte og bemannede roller som har ansvar for overvåkning og varsling av endringer, både i vilkår og betingelser, og i funksjonalitet. Det er også viktig med gode endringskontrollrutiner som omfatter informasjonssikkerhet og personvern, der endringer som

medfører endring i risiko identifiseres og legges frem for godkjenning av aktuell leder. Det bør gjøres jevnlige stikkprøver av om kontrollrutiner og endringskontroll fungerer som de skal.

3 Risikostyring

Når en virksomhet i Oslo kommune ønsker å ta i bruk skytjenester er det virksomhetens ansvar at skytjenesten har akseptabelt risikonivå. Det skal alltid gjøres en risikovurdering før nye IKT-løsninger tas i bruk. Dette gjelder også skytjenester. Omfanget av risikovurderingen kan variere, avhengig av verdien på informasjonen som skal behandles i løsningen og kritikalitet av tjenesten, dvs. hvor viktig den er for kommunen.

Risikostyring omfatter

- identifisering og verdivurdering av verdier
- kartlegging av trusler mot verdiene
- kartlegging av sårbarheter som kan føre til at truslene realiseres
- kartlegging av uønskede hendelser
- analyse av sannsynlighet og konsekvens av slike hendelser og vurdering mot akseptabel risiko
- håndtering av risikoer som ikke er akseptable, gjennom å henholdsvis redusere, overføre, akseptere eller unngå risiko,
- og deretter identifisere og iverksette nødvendige tiltak, samt følge opp at planlagte tiltak har blitt gjennomført
- overvåke risikobildet løpende og ta nødvendige grep ved endringer i risikobildet.

Hvordan påvirkes risikovurderinger ved bruk av skytjenester?

Informasjonen som behandles i en IKT-løsning vil være den samme uavhengig av om den behandles i egne applikasjoner i eget datarom eller hos en skytjenesteleverandør. Truslene, dvs. fra trusselaktører og -fenomener, er i utgangspunktet også de samme, men det kan være ulike sårbarheter med tilhørende risikoer og tiltak avhengig av hvor informasjonen behandles.

Det er også noen forskjeller i hvordan man innhenter data til selve risikovurderingen:

- En virksomhet kan bli mer avhengig av tilgang på dokumentasjon og ressurser fra leverandøren ved risikovurdering av en skytjeneste.
- Virksomhetens risikovurdering må i større grad basere seg på avtaletekst (leverandørens standardvilkår og betingelser), leverandørens sertifiseringer og rapporter fra uavhengige revisjoner enn ved driftsalternativer nærmere egen drift.

- Virksomheten har ikke fullt innsyn i skyleverandørens tekniske løsninger og drift, og har ikke nødvendigvis rett til sikkerhetstesting av leverandørens skyløsning.

De neste underkapitlene lister opp risikomomenter som er spesielt relevante ved bruk av skytjenester, delt opp i områder.

3.1 Risiko knyttet til styring og leverandørforhold

3.1.1 Kompleksitet

Stadig mer integrerte løsninger fører til økende kompleksitet, f.eks. hybride løsninger mellom eget og skybasert driftsmiljø med potensielt ulike sikkerhetsnivåer. Kompleksitet er mer tidkrevende, krever mer kompetanse og reduserer ofte evnen til å gjøre endringer på løsningen raskt og kontrollert. Kjeder av skytjenester og leverandørers bruk av skytjenester hvor man har begrenset innsyn i løsningene, kan føre til at det blir veldig vanskelig å holde oversikt over sikkerhetsnivå og ansvarsforhold.

3.1.2 Kompetanse

Det er begrenset tilgang i markedet på personell med erfaring og kunnskap om skytjenester. Spesielt er det mangel på folk med kompetanse på produkter fra mer enn én leverandør. Ulike leverandører har ulike konfigurasjonsmuligheter og administrasjonspaneler og det er ikke all kompetanse som kan gjenbrukes på tvers av leverandører. Manglende kompetanse i kommunens virksomheter kan føre til feil og sårbarheter i design, konfigurasjon, drift og forvaltning, som igjen kan føre til uønskede hendelser med tap og skader som resultat.

3.1.3 Skytjenesteavtaler og endringer i vilkår

Som nevnt i kapittel 1.3 og 2.2 blir leverandøren sittende med en rekke sikkerhetskritiske oppgaver i en skybasert leveransemodell, noe som gjør avtalen til et av de viktigste verktøyene kunden har for å håndtere risiko.

Ettersom de store skytjenesteleverandørene ofte kun vil forholde seg til sine egne standardavtaler som kunden normalt ikke kan endre, må man være trygg på at det som står i disse avtalene er akseptabelt og dekkende.

I mer tradisjonelle driftsmiljøer har kunden styring og kontroll på løsningen, eventuelt over en underleverandør på drift. For skytjenester kommer det vanligvis endringer innenfor avtalevilkår og betingelser uten at kunden styrer dette. Også de tekniske tjenestene fra leverandøren er stadig i endring uten at man kan påvirke eller stanse dette som kunde. Man kan ikke lenger la være å installere en ny versjon av et produkt, det gjøres automatisk. Funksjonalitet kan også forsvinne etter en viss periode uten at man kan gjøre noe med det annet enn å tilpasse seg.

Kap. 6 omtaler avtaler i detalj.

3.1.4 Avhengighet til leverandør

Utstrakt bruk av proprietær funksjonalitet fra skytjenesteleverandør (altså funksjoner eller API-er som er unike for en leverandør) i applikasjoner som utvikles av virksomheter i kommunen, kan gjøre det krevende å bytte leverandør ved behov. Dette kan medføre økonomisk risiko (leverandører skrur opp prisene når kundene har gjort seg avhengige av dem) men også risiko ifm. tilgjengelighet dersom leverandøren går konkurs eller ut av markedet på annen måte.

3.1.5 Kostnader

Skytjenester er basert på virtualisering og deling av ressurser. Dette kan gi lavere kostnader for virksomheter sammenliknet med andre tilnærminger. Kostnader ved bruk av PaaS- og IaaS-skytjenester kan i utgangspunktet se forutsigbare ut i og med at «satser» for konsumering av prosessorkraft, nettverkstrafikk, lagringsplass etc. er beskrevet i avtale som er inngått med leverandøren. Dog kan det være utfordrende for arkitekter, utviklere etc. i et slikt virtuelt miljø å ha oversikt over økonomiske konsekvenser av utprøving av funksjonalitet og av ulike designvalg. Opplæring av personell vil være et viktig tema for å begrense slik risiko, samt oppsett av varsling iht. grenser for forbruk der dette er mulig.

Dersom formålet med skytjenesten er å erstatte en eksisterende tradisjonell IT-løsning så er det viktig å være oppmerksom på at eventuell økonomisk besparelse ved dette er avhengig av at den gamle løsningen kan fases helt ut, hvis ikke ender det med doble kostnader i stedet. Dermed er det viktig å ha en plan for utfasing av gammel løsning.

3.1.6 Geopolitikk

Vi lever i en mer uforutsigbar verden enn for bare noen år tilbake, og det geopolitiske bildet kan potensielt endre seg i løpet av levetiden til en IT-løsning.

Virksomheter som ønsker å benytte skytjenester i utlandet, bør vurdere Norges forhold til landet og jurisdiksjon hvor leverandør er lokalisert og hvor virksomhetens informasjon prosesseres og/eller lagres. Slike vurderinger bør ta utgangspunkt i beskyttelsesbehovet (konfidensialitet) for informasjonen og kritikaliteten av tjenesten.

Normalt bør man velge leverandører som er lokalisert (hovedkontor, datahaller og personell) i land Norge har et sikkerhetspolitisk samarbeid med, men merk at de av disse som ligger utenfor EØS-området likevel kan ha personvernlovgivning som er mangelfull i forhold til EU/EØS (f.eks. USA).

Generelt bør høyere risiko i valg av land følges opp med en tilsvarende god exit-strategi.

3.2 Risiko knyttet til informasjonsbehandling

Virksomheter må beskytte informasjon iht. krav til konfidensialitet, integritet og tilgjengelighet. Dette gjelder like fullt ved bruk av skytjenester, der det spesielt er viktig å være oppmerksom på følgende forhold:

3.2.1 Leverandørers tilgang til data

Informasjonsbehandling i en skytjeneste skjer på fysisk og logisk infrastruktur som er kontrollert av skyleverandøren. Dette betyr at informasjon som behandles i skytjenesten vil kunne ses, kopieres ut eller manipuleres av leverandør eller underleverandør. Ulike leverandører har ulike tiltak som skal beskytte kundens informasjon mot dette. Effektiviteten av disse tiltakene kan måtte vurderes opp mot lover og regelverk samt nytten av løsningen og hvor attraktiv informasjonen som skal behandles kan være.

Man kan velge å kryptere dataene som benyttes i skytjenesten med en egen krypteringsnøkkel som man selv har kontroll på. Vær i så fall bevisst på at aktøren som kontrollerer maskinvaren der de virtuelle maskinene kjører («hypervisor»-laget), likevel vil kunne få tak i kundens eventuelle krypteringsnøkler hvis den virkelig vil, så lenge nøkkelen benyttes til å dekryptere data i minnet på de virtuelle maskinene[5]. Kryptering beskytter altså data under transport og data i ro, men ikke nødvendigvis data i bruk.

3.2.2 Lovpålagt utlevering av data til myndigheter

Ulike land har ulike regelverk mht. krav til utlevering av informasjon som behandles i skytjenester. Dette kan f.eks. gjelde i straffesaker og for etterretning. I noen tilfeller er skytjenesteleverandører pålagt hemmelig utlevering av kunders informasjon. Ved bruk av utenlandske tjenester og leverandører må virksomheten kartlegge lover og regelverk som kommer til anvendelse ved behandling av virksomhetens informasjon i de aktuelle land og jurisdiksjoner. Planlagt behandling vurderes opp mot etterlevelse av lover og regelverk samt risiko for uvedkommendes innsyn i virksomhetens informasjon. Spesielt kan nevnes behandling av personopplysninger og Schrems II-dommen, hvor det p.t. er uklart om det er mulig å oppnå tilsvarende sikkerhet for personopplysninger ved behandling hos selskaper med hovedsete i USA som ved behandling hos europeiske selskaper. Dette gjelder selv om de behandler kundens informasjon utelukkende i europeiske datasentre.

3.2.3 Tap av data

Digitale data kan gå tapt, for eksempel ved feil på lagringsmedia, cyberangrep eller menneskelige feil. Dette kan ha uønskede konsekvenser, både for tjenesteproduksjon og for lovetterlevelse. Et eksempel er at arkivloven med forskrifter stiller krav til hvor lenge offentlige virksomheter må ta vare på dokumentasjonen sin. Dersom dokumentasjonen skal langtidslagres (bevares) eller den obligatoriske oppbevaringstiden før sletting (kassasjon) ikke er utløpt, kan tap av data resultere i uhjemlet kassasjon av arkivmateriale og medføre brudd på arkivloven.

Sikkerhetskopiering av data for å unngå datatap er like viktig for skytjenester som for tradisjonell IT, men hva slags regime som gjelder for sikkerhetskopiering kan variere fra tjeneste til tjeneste. Sørg alltid for at det er tilstrekkelig sikkerhetskopiering i tjenesten. Dersom det er svært kritiske data som man virkelig ikke kan miste, så kan det også være på sin plass å sikkerhetskopiere dem over til en annen leverandør enn den som drifter selve skytjenesten. Det

[5] Ifølge Nasjonal Sikkerhetsmyndighet (se spørsmål 7 her: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/ofte-stilte-sporsmal-om-sky-og-tjenesteutsetting/sporsmal-om-sky-og-tjenesteutsetting/)

er også viktig å sikre seg mot at ondsinnede aktører eller menneskelige feil kan medføre sletting av (alle kopier av) en sikkerhetskopi. Skytjenester kan være sårbare ettersom de, ofte inklusive tjenestens administrative grensesnitt, av natur er tilgjengelige fra internett. Det beste forsvaret mot alvorlig skade fra f.eks. løsepengevirus er å ha en separat sikkerhetskopi som ikke kan nås via normale nettverkskanaler, såkalt «offline backup».

3.2.4 Store informasjonsmengder utgjør et fristende mål

Konsentrasjonen av informasjon fra et stort antall kunder i en felles infrastruktur kan friste angripere mer enn lokale datalagre hos hver enkelt kunde, og dermed øke sannsynligheten for et angrep.

3.2.5 Tilgjengelighet fra internett

Skytjenester er av natur tilgjengelige via internett. Det er ikke mulig å isolere dem fysisk fra internett slik man kan med spesielt sikrede lokale nettverk internt i en virksomhet.
Et annet aspekt ved dette er at det er mulig å avlytte trafikkdata / metadata som sendes over internett, noe som kan forenkle eventuelle angriperes rekognosering av en virksomhet.

3.2.6 Innsyn fra andre kunder av leverandør

Siden de fleste skytjenester er basert på deling av fysisk infrastruktur mellom mange ulike kunder, er det en risiko knyttet til at noen av disse kan få tilgang til dine data. Dette kan skyldes f.eks. tekniske feil, konfigurasjonsfeil eller datainnbrudd.

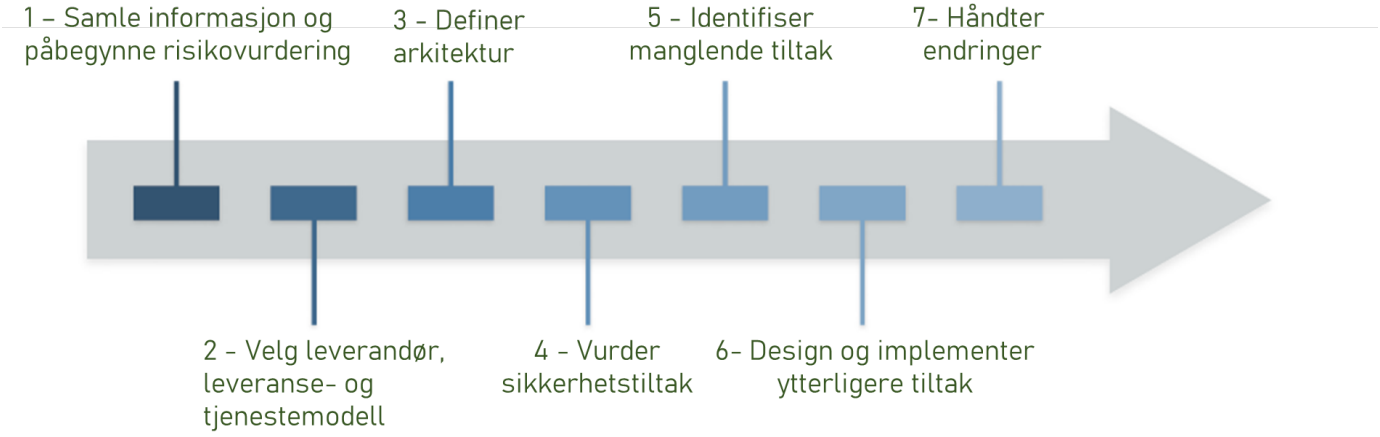
3.2.7 Informasjon aksesseres fra ukontrollerte enheter

Ansattes mulighet for å benytte skytjenesten fra enheter som ikke er underlagt arbeidsgivers kontroll kan gi utfordringer knyttet til mindre kontroll på informasjon. Informasjonen er da ikke lenger begrenset til å bli behandlet kun på kontrollerte enheter innenfor virksomhetens eget nettverk.

4 Fremgangsmåte for å etablere skytjeneste

4.1 Overordnet fremgangsmåte

Cloud Security Alliance (CSA) er en anerkjent industriallianse som fokuserer på sikkerhet ved bruk av skytjenester. CSA har en overordnet anbefalt prosessmodell for vurdering, etablering og idriftsettelse av en skytjeneste, inklusive steg for design og utvikling av sikkerhetsfunksjonalitet:



I alle etableringer av IT-tjenester skal det gjennomføres risikovurdering og personvernkonsekvensvurdering. Dette gjelder også for skytjenester, hvor risikovurderingen med fordel kan gjøres i faser som korresponderer med de tre første stegene vist i figuren ovenfor.

Hvert steg leder til oppdatering av risikooversikten med nye risikoscenarier. Risikoscenariene kan medføre nye krav for å kunne gå videre i prosessen og/eller kan legge føringer for tjenesten som skal utvikles.

I steg 4. «Vurder sikkerhetstiltak» til og med steg 6. «Design og implementer ytterligere tiltak» utføres risikohåndtering basert på gjennomført risikovurdering, og leverandørens og skyplattformens tekniske, prosessuelle og organisatoriske egenskaper og tiltak.

Ved endringer av tjenesten i driftsfasen, for eksempel av teknisk arkitektur eller typer informasjon som behandles, må risikovurdering av endringen gjennomføres, risikooversikt oppdateres og eventuelle endrede risikoer behandles.

Ansatte og innleide med ulike roller vil gi bidrag til risikovurdering og –behandling gjennom de ulike stegene i prosessen. Ledere og beslutningstakere er mer involvert i de tidligere stegene og teknisk personell mer i de senere stegene. Systemeier, eventuelt prosjekteier, er ansvarlig for at risikovurdering og –håndtering blir gjennomført. Prosjektleder, eventuelt prosessleder, vil planlegge og organisere aktiviteter, og sette av ressurser til gjennomføringen mens det faglige arbeidet kan ledes av en fasilitator gjennom prosjektet eller prosessen. I driftsfasen er det systemeier, eventuelt systemforvalter, som gjennomfører nødvendige risikohåndteringsoppgaver.

Kun de to første stegene er beskrevet i denne versjonen av veilederen. Steg 3. til 6. handler om tjenestedesignet, mens steg 7 er en forvaltningsprosess.

I alle stegene må det tas hensyn til personvern. Krav til innebygget personvern etter personopplysningsregelverket forutsetter at det må tas hensyn til personvern når det planlegges en behandling av personopplysninger og på tidspunktet for selve behandlingen av personopplysninger. I tillegg stiller personopplysningsregelverket krav til vurderinger som må være gjennomført og andre krav som må oppfylles før en behandling av personopplysninger kan starte. Dette innebærer at det må gjøres en vurdering av risikoer som behandlingen av personopplysninger i skyen vil medføre for den registrertes rettigheter og friheter, samt at det må fastlegges risikoreduserende tiltak. En slik personvernkonsekvensvurdering skal gjennomføres før behandling av personopplysninger i skyen. Den innledende personvernkonsekvensvurderingen kan gjøres uavhengig av risikovurderingen for tjenesten. Steg 2 av personvernkonsekvensvurderingen er imidlertid avhengig av tjenestens risikovurdering, og startes derfor normalt i steg 3 med fortløpende oppdateringer særlig i steg 6 og 7.

4.2 Steg 1 – Samle informasjon og påbegynne risikovurdering

Det første steget i etableringsprosessen er å kartlegge hvilke behov tjenesten skal dekke, hvilke rammer som gjelder, og hva som eventuelt skal til for at tjenesten skal kunne realiseres som en skytjeneste. Dette inkluderer å vurdere krav til både informasjonssikkerhet og personvern sett opp mot behovet – vil en skytjenesteløsning være egnet for å ivareta virksomhetens krav på disse områdene?

4.2.1 Administrativt

Det vil være en fordel for gjennomføring av prosjektet eller anskaffelsen at systemeier for skytjenesten utpekes tidlig i prosessen. Alternativt bør det utpekes en prosjekteier frem til systemeierrollen er bemannet.

4.2.2 Behov

Det første spørsmålet virksomheten må stille seg, er om IKT-tjenesten man ønsker å etablere eller endre for å dekke et brukerbehov, er egnet for leveranse ved hjelp av en skybasert infrastruktur eller plattform.

Virksomheten må avdekke om det finnes begrensninger ved skytjenester som vil ha betydning for oppfyllelsen av behovet. Videre bør det vurderes hvor stor grad av fleksibilitet skytjenesten tilbyr for å benytte dataene i løsningen på andre måter og i andre løsninger slik at tjenesten kan dekke endrede behov over tid.

4.2.3 Kartlegging av informasjon som skal behandles

Virksomheten må finne ut av og dokumentere hvilke virksomhetsprosess(er) skytjenesten skal støtte. I disse prosessene behandles det ulike former for informasjon. Hvilke kategorier av informasjon er det nødvendig å behandle, inklusive lagre og/eller overføre, for å oppfylle

formålet med tjenesten? Kategoriene må dokumenteres på et detaljeringsnivå som gir grunnlag for å vurdere kravene som gjelder for behandling av denne informasjonen.

4.2.4 Kartlegging av lover og regelverk som får anvendelse, og vurdering av etterlevelse

Det må kartlegges og dokumenteres hvilke lover, og eksternt og internt regelverk som får anvendelse med planlagt informasjonsbehandling, basert på informasjon kartlagt i forrige underkapittel. Det må vurderes om planlagt informasjonsbehandling i sky er innenfor lover og regelverk. Vurderingen må dokumenteres. Dersom behandling ikke er innenfor, vil virksomheten måtte sørge for tiltak som løser avvikene, eller la være å benytte skytjenester til dette formålet. Et sentral punkt i vurderingen er altså å kartlegge om det er noen «showstoppere» for tjenesten eller om man kan foreslå avgrensninger, sikkerhetstiltak eller andre forutsetninger som kan gjøre tjenesten lovlig. Flere av de viktige lovene som må undersøkes, er nevnt i veilederens kap. 5. Disse omfatter blant annet arkivlovgivning og regler om vern av personopplysninger.

4.2.4.1 Spesielt om behandling av personopplysninger

All behandling av personopplysninger er lovregulert, dette gjelder naturligvis også ved bruk av skytjenester. Det må kartlegges hvilken behandling av personopplysninger som er nødvendig. Dette vil si at det må vurderes om den planlagte behandlingsaktiviteten er nødvendig og står i rimelig forhold til formålet med behandlingen. Typer av personopplysninger (om det er særlige kategorier av personopplysninger) og kilder til personopplysninger kan ha betydning for hvilken behandling av personopplysninger som er tillatt og hvilke tiltak som må iverksettes for å oppfylle kravene i regelverket om vern av personopplysninger. Det stilles strengere krav til behandlingen av særlige kategorier av personopplysninger, da behandling av disse opplysningene normalt anses som mer inngripende og derfor vil kreve et høyere beskyttelsesnivå enn andre personopplysninger.

Krav til dataminimering i personopplysningsregelverket forutsetter at det kun skal behandles personopplysninger som er nødvendig for å oppnå formålet med behandling av opplysningene. Det vil si at når personopplysninger skal behandles må det gjøres konkrete vurderinger av nødvendighet for bruk av enhver type av personopplysninger.

Hvilke kategorier av registrerte som behandles kan også ha betydning for hvilke tiltak som må iverksettes. Lover og regelverket setter begrensninger i bruken av personopplysninger for kategorier av sårbare registrerte, som for eksempel barn.

Hvem som utfører hvilke behandlinger av personopplysninger må også kartlegges. I tillegg må geografisk lokasjon til de som behandler personopplysningene identifiseres. Det naturlige kjennetegnet for skytjenester er at de tilbyr og aksesserer lagring og tilgang til dataene fra ulike land og steder i verden. Det må kartlegges om det er mulig å tillate lagring og tilgang fra de landene eller stedene skytjenesteleverandøren oppgir.

Kartlegging av behandling av personopplysninger bør omfatte all planlagt bruk av personopplysninger inkl. gjenbruk av personopplysninger dersom dette er mulig å kartlegge på forhånd. Bruk av skytjenester som basis for kommunens løsninger vil ofte medføre behandling av personopplysninger om ansatte i kommunen og hos drifts- og vedlikeholdsleverandører. Slik behandling må inngå i kartleggingen.

4.2.4.2 Spesielt om arkivverdig dokumentasjon

Arkivloven med forskrifter gir føringer for behandling av dokumentasjon i offentlige organer, blant annet for bevaring og kassasjon. Etter arkivloven plikter offentlige organer å holde arkiv, og å organisere og innrette disse slik at dokumentasjonen er sikret som informasjonskilder for samtid og ettertid.

All dokumentasjon som produseres av virksomheter i Oslo kommune skal undergå en vurdering som bestemmer om det skal tas vare på (bevares) eller om det kan destrueres (kasseres) etter en gitt tid. Det er innholdet, og konteksten som avgjør om dokumentasjonen er arkivverdig, uavhengig av format, plattform og system. Vurderingen skal gjøres for all dokumentasjon kommunen produserer eller mottar, uansett om det er i form av papirbaserte dokumenter, som data og metadata i ulike systemer, om det er publisert på intranett eller internett, er lydfiler eller videoer, og så videre. Dette gjelder også for data og metadata som lagres i skytjenester. Se mer om bestemmelser i kapittel 5.1.

Virksomheten må derfor kartlegge og ha oversikt over all dokumentasjon som lagres i skyen, og sikre at behandlingen etterlever krav i arkivregelverket, samt at dokumentasjonen er tilgjengelig for virksomheten helt til bevaring eller kassasjon er gjennomført. Benytt Oslo kommunes funksjonsbaserte klassifikasjon med tilhørende bevarings- og kassasjonsplan (OKA) for å kartlegge om materialet skal bevares eller kasseres. Arkivforskriften og riksarkivarens forskrift gir mer detaljerte føringer for behandling av arkivmateriale i offentlige organer.

Dersom dokumentasjonen skal bevares må det gjøres et uttrekk av data og relevante metadata fra skytjenesten eller systemet i skytjenesten, som etter avtale med Byarkivet avleveres dit for langtidsbevaring. Dersom dokumentasjonen skal kasseres, er det viktig at virksomheten er sikker på at all data og metadata kan slettes fra skytjenesten når oppbevaringstiden for denne typen dokumentasjon er utløpt. Muligheten for å ta uttrekk av og å kunne slette data og metadata fra skytjenesten bør være med som krav i en eventuell anskaffelsesprosess for å sikre at virksomheten har kontroll over egne data, og for å etterleve kravene til bevaring og kassasjon i arkivloven med forskrifter.

Virksomheten må sikre at data og metadata lagret i skyen er tilgjengelig til tidspunktet for overføring av uttrekk til Byarkivet for langtidsbevaring, eller til den obligatoriske oppbevaringstiden er utløpt og sletting av kassabelt materiale er gjennomført. Dersom skytjenesten ikke kan garantere fortsatt tilgjengelighet i løpet av hele tidsperioden må virksomheten vurdere tiltak som dataportabilitet for å redusere risikoen for tap av data og metadata lagret i skyen.

Spørsmål om bevaring og kassasjon, uttrekk og sletting, og generelle henvendelser om arkiv, kan rettes til Kulturetaten v/ Byarkivet, som er kommunens fagorgan for dokumentasjonsforvaltning og arkiv.

4.2.5 Klassifisering av konfidensialitet

Klassifisering av informasjonen som behandles i tjenesten, er et godt hjelpemiddel for styring av risiko knyttet til uautorisert innsyn og utlevering.

Konfidensialitetsnivå, eller «konfidensialitetsklassen», indikerer hvor alvorlig det vil være for kommunen og/eller en registrert person om informasjonen blir kjent av uvedkommende («taps- og skadepotensialet»). Høyt taps-/skadepotensial medfører høyt beskyttelsesbehov. Organisatorisk, prosessuell og teknisk beskyttelse av informasjon skal være i tråd med gjeldende lovverk og kommunens styrende dokumenter. Dette gjenspeiles i behandlingsregler som følger konfidensialitetsklassene. Det bør lages behandlingsregler for skytjenesten som setter rammer for hvilken informasjon som kan behandles på hvilken måte i tjenesten. Dersom ulike informasjonstyper med ulik konfidensialitetsklasse behandles i samme løsning, er det behandlingsreglene for den høyeste konfidensialitetsklassen som vil gjelde for løsningen.

En klassifiseringsmatrise kan være til hjelp både ved verdivurdering og risikovurdering av behandling av informasjon.

Klassifiser de ulike informasjonstypene som er planlagt benyttet i skyløsningen, iht. virksomhetens klassifiseringsmatrise, dersom slik finnes. Arbeid med felles klassifiseringsmatrise for hele kommunen pågår.

4.2.6 Klassifisering av integritet og tilgjengelighet

Krav til integritet og tilgjengelighet vil være avhengig av tjenesten man ønsker å realisere og virksomheten må kartlegge krav til integritet og tilgjengelighet for tjenesten.

Denne versjonen av skyveilederen beskriver ikke nærmere klassifisering av integritet og tilgjengelighet.

Når alle kartleggings- og klassifiseringsoppgavene nevnt i punktene ovenfor er gjennomført, så benyttes resultatene i aktivitetene som kommer i kapitlene «Personvern» og «Oppstart av risikovurdering» nedenfor.

4.2.7 Oppstart av risikovurdering

4.2.7.1 Intro

I kap. 4.1 anbefales det en prosess for de vurderingene som må gjøres før en skytjeneste etableres. De tre første stegene er:

- Samle informasjon og påbegynne risikovurdering
- Velge leverandør, leveranse- og tjenestemodell
- Definere arkitektur

Hvert av disse stegene i prosessen vil både fremskaffe ny informasjon og medføre valg mellom alternativer basert på til enhver tid tilgjengelig informasjon. Derfor er det naturlig å gjennomføre vurderinger av risiko knyttet til ny informasjon og valg i hvert steg. Det er viktig å presisere at dette ikke er noen fullstendig risikovurdering av tjenesten i hvert steg men kun en vurdering av det som er nytt. Kapittel 3 i denne veilederen gir innspill til noen risikoområder som kan tas inn i risikovurderingen.

Grovt sett vil risikovurdering i første steg kun omhandle krav fra vurdering av lover og regelverk som får anvendelse, og risiko knyttet til egenskaper ved skytjenester generelt. Dette ses opp mot informasjonen som skal behandles i tjenesten.

I steg nummer to vil det gjøres valg av tjenestemodell, leveransemodell og leverandør. Risikovurderingen skal oppdateres basert på ny informasjon og nyoppdaget eller endret risiko som følge av disse valgene.

Steg nummer tre vil ta for seg risikovurdering av arkitektur inklusive tekniske sårbarheter (en Risiko- Og Sårbarhetsanalyse, *ROS*). Dette steget er ikke dekket i denne versjonen av veilederen.

4.2.7.2 Risikovurdering – Steg 1

Målet med risikovurdering steg 1 er å fastslå om det er mulig å etablere IKT-tjenesten med bruk av skybasert infrastruktur eller plattform innenfor et akseptabelt risikonivå. Samtidig kan risikovurderingen resultere i krav til skytjenesteleverandøren som virksomheten vil avrope tjenester fra. Dersom man ender opp med å gjøre en egen anskaffelse kan disse føringene ende opp i vurderingskriterier eller i kravspesifikasjon.

Risikovurdering av en ny skybasert tjeneste tar utgangspunkt i at vurderingen av lovetterlevelse (kap. 4.2.4) er gjennomført med et resultat som tilsier at man kan gå videre med etablering av tjenesten («Ansatte med juridisk kompetanse må videre vurdere om planlagt informasjonsbehandling i sky er innenfor lover og regelverk, og dokumentere resultatet av dette.»).

Virksomheten kan ikke i en risikovurdering velge å akseptere manglende etterlevelse av lover og regelverk. Vurderingen av om planlagt informasjonsbehandling i sky er innenfor lover og regelverk eller ikke, gir imidlertid sjelden et ja- eller nei-svar. Mer vanlig er det at vurderingen lister opp forutsetninger for at en type behandling skal være innenfor lover og regelverk. Det er disse forutsetningene som er viktige, spesielt identifisering av «showstoppere» og eventuelle tiltak som kan oppheve dem.

I denne fasen ser vi kun på egenskaper ved skytjenester hvor disse avviker fra tradisjonell IKT. De viktigste egenskapene som grunnlag for risikovurdering kan være

- Tilgjengelighet av tjenesten inklusive admin-grensesnitt fra internett
- Informasjonsbehandling med ressurser delt med andre kunder
- Betaling etter forbruk
- Dynamisk skalering av kapasitet
- Test og utvikling av tjenester gjøres via selvbetjening, ikke alltid underlagt virksomhetens kontrollmekanismer
- Ekstern driftsleverandør – normalt med standardiserte vilkår og betingelser

I risikovurderingen identifiseres trusler, sårbarheter og risikoscenarier basert på informasjon som behandles, krav og andre forutsetninger fra lovlighetsvurdering, og egenskaper ved skytjenester. Vurdering av risikonivå gjøres og alt legges inn i valgt risikovurderingsverktøy. Malen på intranett kan brukes.

Konklusjonen fra steg 1 kan være at skysetting ikke er mulig, i så fall har man ved å følge prosessen klart å identifisere dette tidlig, og spart mye tid og krefter på det. En mer vanlig konklusjon er at skysetting er mulig gitt visse forbehold eller risikoreduserende tiltak. Resultatene fra steg 1 kan derfor legge en rekke føringer for beslutninger som kommer senere i prosessen, f.eks. valg av leveransemodell eller krav til arkitektur og sikkerhetstiltak.

4.3 Steg 2 - Valg av leverandør, tjeneste- og leveransemodell

4.3.1 Valg av tjenestemodell og leveransemodell

Virksomheten må gjøre valg av tjenestemodell, PaaS eller IaaS, basert på egen utviklingsstrategi samt en analyse av fordeler og ulemper/risikoer ved de to alternativene for angjeldende prosjekt. IaaS gir større fleksibilitet samt kontroll over komponenter som benyttes i plattform, samt drift, mens PaaS overlater flere oppgaver til leverandøren i bytte mot mindre fleksibilitet for virksomheten. Eventuelle virksomhetsspesifikke krav til komponenter og mikrotjenester kan påvirke både valget av PaaS vs. IaaS samt valg av leverandør (nedenfor).

Valg av leveransemodell bør være i henhold til virksomhetens «sourcingstrategi». Offentlig sky kan gi lavere kostnader, men medføre mindre fleksibilitet og rom for å forhandle om kontraktsbetingelser. Privat sky kan eies og/eller driftes av leverandør eller egen virksomhet. Spesielle beskyttelseskrav til informasjonen som skal behandles (krav til konfidensialitet, som identifisert tidligere) kan trekke i retning av privat sky.

Ved valg av tjenestemodell og leveransemodell skal krav knyttet til innebygd personvern hensyntas.

4.3.2 Leverandørvurderingsprosess

Når man har vurdert muligheten for å sette tjenesten i skyen og valgt tjeneste- og leveransemodeller med akseptabel risiko, er det neste steget å velge leverandør.. Dette gjelder enten man skal gjøre avrop på eksisterende avtaler eller om man skal gjøre en anskaffelse.

Ulike skytjenesteleverandører som for eksempel AWS, Google og Microsoft har ulike tjenester - med ulik funksjonalitet, sikkerhetstjenester og pris - og de krever ulik produktkompetanse hos medarbeidere som jobber med utvikling og drift. Dette siste poenget bidrar sterkt til at man blir låst til en leverandør, ettersom det for de fleste virksomheter ikke er ønskelig å vedlikeholde kompetanse på flere leverandørers produkter. Leverandørvurderingen man gjør første gang virksomheten etablerer infrastruktur eller plattform i sky, er derfor svært viktig.

Virksomheten må tidlig innhente, eventuelt forespørre, all dokumentasjon som skal inngå i vurderingene i denne prosessen. Dokumentasjonen er det primære verktøyet man har for å undersøke om leverandøren og dens løsning tilfredsstiller behov og krav som er identifisert i steg 1. Referanser kan også være nyttige. Leverandørens «verktøykasse» for oppnåelse av sikkerhets- og personvernkrav bør være en sentral del av leverandørvurderingsprosessen.

Dersom man ikke kan gjøre avrop på en samkjøps- eller rammeavtale og en anbudskonkurranse er nødvendig, må den endelige leverandørvurderingen gjøres i forbindelse med tilbudsevalueringen i konkurransen.

4.3.3 Exit-strategi

Tenk gjennom virksomhetens behov ved avslutning av avtalen basert på leverandørens standardvilkår og –betingelser, eventuelt med virksomhetens avtalte endringer. Dette gjelder både ved utløp av en tidsbegrenset avtale, oppsigelse av en løpende avtale og ved ikke-planlagt avslutning som følge av uønskede hendelser hos leverandøren, manglende etterlevelse av avtalen fra leverandørens side eller tilsvarende.

I etableringsprosjektet for skytjenesten må det lages en plan for avslutning av tjenesten. Planen må vedlikeholdes over tid ettersom vilkår, betingelser og andre forutsetninger kan endre seg.

Forslag til innhold i planen:

- Hvilke roller i egen virksomhet har ansvar for å utføre ulike oppgaver?
- Tidskrav virksomheten har satt seg ved avtaleavslutning?
    - Kan disse oppnås med teknisk kapasitet hos leverandør og virksomhet (eller hos leverandør man ønsker å flytte til)?
- Aktiviteter som må gjennomføres for å hente ut data i et strukturert og åpent format, sikre at leverandøren sletter data etc.?
- Aktiviteter som må gjennomføres for å hente ut evt. konfigurasjon (f.eks. «infrastruktur som kode») som kan gjenbrukes i den nye løsningen.

Virksomheten bør i størst mulig grad kunne hente ut konfigurasjon og data uten manuell bistand fra leverandøren. Dersom leverandøren skulle være i alvorlige problemer og det er årsaken til at virksomheten ønsker å skifte leverandør, kan det være mange kunder som er i ferd med å gjøre det samme! Avtalen bør også inneholde betingelser rundt ressursbistand fra leverandøren i forbindelse med avvikling, samt hvordan kostnader for dette skal dekkes.

4.3.4 Avtaleoppfølging

De store skyleverandørene krever at avtalene som inngås med dem er på deres premisser, med ensidig rett til å endre vilkår (se 3.1.3).

Virksomhetene må følge med på leverandørens endringer av avtalevilkår og betingelser, og ved behov tilpasse sin løsning og konfigurasjon til disse. Dersom nødvendig overvåkning av endringer i avtalevilkår og betingelser samt i funksjonalitet ikke samkjøres i kommunen, vil ulike virksomheter måtte gjøre det samme arbeidet i parallell. Ansvaret for slik koordinering er ikke plassert per i dag.

4.3.5 Risikovurdering – Steg 2

Målet med risikovurdering steg 2 er å vurdere om ønsket kombinasjon av tjenestemodell, leveransemodell og leverandør kan realiseres for tjenesten innenfor et akseptabelt risikonivå og hvilke tiltak som eventuelt må gjøres for å oppnå dette.

Risikovurdering i steg 2 bygger på alle resultatene av steg 1 (kap. 4.2.7.2), og ny informasjon samt valg av alternativer i steg 2. Det vil si at det gjøres utvidelse av risikovurderingen med risikoscenarier relatert til ønsket tjenestemodell, leveransemodell og leverandør. Dersom det har kommet til mer utfyllende informasjon, f.eks. om leverandør, bør risikoscenariene knyttet til informasjonsrisiko (ref. kap. 3.2), personvern (ref. kap. 4.2.4.1 og kap. 5.3) gjennomgås og eventuelt oppdateres.

I denne fasen ser vi altså på egenskapene ved tjenestemodell, leveransemodell og leverandør som grunnlag for risikovurderingen. Ref. kapittel 1.2, 2.2 og 3.1 kan de viktigste egenskapene være

For tjenestemodell:

- Leverandørens ansvar og omfang av oppgaver
- Virksomhetens krav til egen kompetanse
- Fleksibilitet til å utforme plattform

For leveransemodell:

- Grad av beskyttelse av informasjon/løsning

For leverandør:

- Avtalevilkår
- Tjenestetilbud mht. funksjonalitet
- Sikkerhetsnivå

- 3.partsrevisjoner – kvalitet på rapporter og hvor gamle er de

I risikovurderingen identifiseres trusler, sårbarheter og risikoscenarier basert på informasjon som behandles og egenskapene ved tjenestemodell, leveransemodell og leverandør. Alvorlighet av risikoer anslås gjennom estimering av sannsynlighet og konsekvens og alt legges inn i valgt risikovurderingsverktøy.

4.3.6 Eksisterende avtaler

Oslo kommune har tre avtaler med tre ulike leverandører som det kan avropes skytjenester på. Se vedlegg 1. For kommunen vil det være en fordel om alle virksomheter i kommunen benytter en av disse avtalene når de skal etablere skytjenester. Dette vil underlette administrasjon og standardisering, og potensielt redusere kostnader.

4.4 Videre prosess

Videre prosess omfatter stegene «Definer arkitektur» til «Håndter endringer». For IaaS- og PaaS tjenester er det virksomheten selv som bygger tjenestearkitekturen på toppen av leverandørens infrastruktur. Arkitektur for tjenesten som virksomheten ønsker å etablere utarbeides, og deretter oppdateres risikovurderingen fra steg 1 og 2 med risikovurdering av foreslått arkitektur for å vurdere om den oppfyller sikkerhetskrav. Eventuell uakseptabel risiko på grunn av mangelfulle sikkerhetstiltak hos leverandør eller i egen utarbeidet arkitektur, må reduseres gjennom tiltak.

Det er viktig å tilordne sikkerhetstiltak som må realiseres, enten til leverandør eller til navngitte personer i definerte roller eller stillinger i linjeorganisasjon. Dette vil ligge til grunn for oppfølging gjennom internkontroll for å sikre at nødvendige tiltak for å overholde akseptabel risiko blir etablert, samt vedlikeholdt over tid. Dersom nødvendige tiltak må gjennomføres i annen del av virksomheten eller i andre virksomheter i kommunen, må systemeier, eventuelt prosjekteier, avtale med ansvarlig leder for tiltaket, og dokumentere oppgaven, ansvarlig og tidsfrist.

5 Relevant lovgivning og typiske juridiske utfordringer

Bruk av skytjenester omfattes av flere regelverk, og reiser derfor flere komplekse juridiske problemstillinger. Nedenfor belyses et utvalg av sentralt regelverk gjeldende for kommunesektoren som gir rammer for hvordan kommunene kan ta i bruk skytjenester. Merk at det i tillegg kan finnes sektor- eller virksomhetsspesifikke lover eller regelverk som regulerer bruk av skytjenester. Dette må vurderes av den enkelte virksomhet.

5.1 Arkivlovgivning

Ved virksomhetens vurdering av bruk av skytjenester må virksomheten ta hensyn til forbudet mot å føre arkivmateriale ut av Norge. Offentlig arkivmateriale omfatter i denne sammenheng både gradert og ugradert informasjon som anses som arkivverdig.

I henhold til arkivloven § 9 b er det forbudt å «føre» offentlig arkivmateriale ut av Norge (utførsel) uten etter særskilt samtykke fra Riksarkivaren. Forbudet retter seg både mot utførsel av papirarkiv og lagring av digitalt arkivmateriale på servere i utlandet. Det finnes imidlertid noen unntak fra forbudet mot utførsel av offentlig arkivmateriale, slik at kopier kan lagres på servere i utlandet så lenge en komplett versjon av arkivet er lagret i Norge.

NB Det finnes et utkast til ny lovgivning på arkivområdet, men det er uvisst i skrivende stund (oktober 2021) når en ny lov vil tre i kraft.

5.2 Bokføringslovgivning

Bokføringsloven om oppbevaring av regnskapsmateriale får anvendelse på regnskapsmateriale i kommuner. I henhold til bokføringsloven § 13 annet ledd, skal regnskapsmaterialet oppbevares i Norge. Etter bestemmelsens femte ledd kan det i forskrift gjøres unntak fra kravet til oppbevaring i Norge. Hovedregelen for elektronisk regnskapsmateriale blir derfor at dataene må være tilgjengelig på en server i Norge, med mindre det finnes unntak.

Videre gir bokføringsforskriften § 7-4 enkelte unntak fra kravet om at regnskapsmaterialet skal oppbevares i Norge. Forskriften § 7-5 gir adgang til å oppbevare elektronisk regnskapsmateriale i andre EØS-stater på nærmere angitte vilkår. Det følger imidlertid av forskrift om oppbevaring av elektronisk regnskapsmateriale i andre EØS-land § 1 at det kun er de nordiske land som oppfyller disse kravene.

Merk at det finnes andre lover og regelverk som inneholder en rekke bestemmelser om oppbevaringsplikt utover bokføringsloven.

5.3 Personopplysningsregelverket

Personopplysningsregelverket kommer til anvendelse dersom behandlingen omfatter personopplysninger. Dette innebærer at virksomheten må etterleve personopplysningsregelverket ved planlegging av bruk, etablering, utvikling og forvaltning av skytjenester.

Personvernopplysningsregelverket stiller ingen direkte rettslige skranker for bruken av skytjenester, men gir rammer for behandling av personopplysninger i skyen. I det følgende gis det *noen eksempler* på utfordringer ved bruk av skytjenester for å behandle personopplysninger:

- Behandlingsansvar. Ansvarsplasseringen kan ofte være uklar, både mellom kommunen og leverandør, samt mellom leverandør og dens underdatabehandlere.

- Behandlingsoversikt. Alle virksomheter som behandler personopplysninger skal føre en protokoll over behandlingsaktivitetene de har ansvar for (GDPR artikkel 30). Det kan være utfordrende å få oversikt over all behandling av personopplysninger i skyen, og å sørge for at opplysningene bare behandles innenfor gitte formål og instruksjoner fra behandlingsansvarlig (f.eks. ikke bruke opplysningene til kommersielle formål).
- Databehandleravtaler. Etter GDPR art. 28 (3) har alle virksomheter som benytter seg av en underleverandør plikt til å ha en databehandleravtale. Det kan være utfordrende å inngå en databehandleravtale som understøtter og bidrar til etterlevelse av personopplysningsregelverket særlig fordi de fleste skyleverandører har egne standardavtaler. Dette vil kreve at kommunen evner å følge opp at vilkår i disse avtalene er dekkende for kravene som regelverket stiller.
- Bruk av underleverandør. I henhold til GDPR artikkel 28 (2) må databehandleren (hovedskytjenesteleverandør) innhente særlig eller generell skriftlig tillatelse fra den behandlingsansvarlige når databehandleren har til hensikt å overlate hele eller deler av oppgavene som er tildelt den til en underbehandler. Det kan være utfordrende for å få oversikt over alle underleverandører/underdatabehandlere som hovedskytjenesteleverandør/ databehandler benytter.
- Den registrertes rettigheter. GDPR gir en rekke rettigheter til den registrerte, blant annet rett til sletting. Hvordan den registrertes rettigheter ivaretas er særlig utfordret ved bruk av skytjenester fordi det er mange aktører som er involvert i behandlingen av personopplysninger.
- Overføring til tredjeland. Ved overføring til land utenfor EU/EØS (tredjeland) må virksomheten påse at kravene i GDPR kapittel V om overføring av personopplysninger til tredjestater eller internasjonale organisasjoner er oppfylt, i tillegg til øvrige krav. GDPR inneholder en rekke overføringsmekanismer som pålegger dataimportøren (skyleverandør) plikter for å sikre tilstrekkelig beskyttelsesnivå ved overføring til tredjeland.

5.4 Anskaffelsesregelverket

Anskaffelsesregelverket gir ikke i seg selv noen begrensninger for mulighet til å anskaffe eller bruke skytjenester. Regelverket setter rammer for tilrettelegning og eventuelt samordning av innkjøp av skytjenester. Det kan imidlertid være utfordringer ved selve gjennomføringen og ivaretakelsen av de angitte krav og prinsippene i anskaffelsesregelverket.

Anskaffelsesloven § 4 fastsetter de grunnleggende prinsippene som gjelder for alle anskaffelser omfattet av loven. Ved gjennomføringen av alle anskaffelser skal oppdragsgiver overholde prinsippene om konkurranse, likebehandling, forutberegnelighet, etterprøvbarhet og forholdsmessighet. Det kan være utfordrende å ivareta disse prinsippene ved selve gjennomføringen av offentlige skytjenester, selv om disse utfordringene ikke nødvendigvis er unike for skytjenester.

En utfordring som kan nevnes her er ivaretakelse av likebehandlingsprinsippet. Flere skyleverandører kan tilby mange ulike løsninger for å oppfylle et tjenestebehov der tilbudene er

vanskelige å sammenligne. Likebehandlingsprinsippet dekker også det EØS-rettslige prinsippet om ikke-diskriminering på grunnlag av nasjonalitet. Ved anskaffelse av skytjenester må virksomheten særlig være oppmerksom på at norske leverandører ikke blir favorisert på bekostning av utenlandske leverandører. Likebehandlingsprinsippet er likevel ikke til hinder for at oppdragsgiver unntaksvis kan behandle norske og utenlandske leverandører forskjellig dersom dette er saklig og objektivt begrunnet.

Videre setter anskaffelsesregelverket rammer og føringer for virksomhetens forhandlingsmuligheter, herunder hva som er beskrevet i konkurransegrunnlaget. Virksomheten bør, før man utarbeider konkurransegrunnlaget, identifisere områder i behovet som kan medføre at tredjeparts standardvilkår må justeres. Hvis slike justeringer er urealistiske, må det vurderes hvordan behovet kan dekkes.

Det er viktig å sikre at beskrivelsen av behovet bidrar til å skape god konkurranse i markedet. Det er ikke adgang til å beskrive sitt behov med den hensikt å legge til rette for at bare én leverandør kan velges, så her bør virksomhetene ha god oversikt over hva markedet kan tilby. Virksomheten bør i denne sammenheng være ekstra oppmerksom på å ikke la seg påvirke av det som fremkommer fra for eksempel enkelte leverandører ved markedsundersøkelse.

5.5 Forvaltningslovgivning og offentlighetslovgivning

Saksbehandlingen i kommunens forvaltning er regulert av blant annet forvaltningsloven og offentlighetsloven. Offentlighetslovens hovedregel er at saksdokumenter, journaler og liknende register for organet er åpne for innsyn dersom ikke annet følger av lov eller forskrift med hjemmel i lov. Alle kan kreve innsyn i saksdokument, journaler og liknende registre hos vedkommende organ.

I utgangspunktet setter forvaltningsloven og offentlighetsloven ingen begrensninger for bruk av skytjenester, men kommunen må sikre at bruk av skytjenester ivaretar innsynsretten og etterlever bestemmelser om taushetsplikt i forvaltningsloven §§ 13 flg. og offentlighetsloven § 13.

I henhold til offentlighetsloven § 13 er det ikke adgang til å gi innbyggerne innsyn i taushetsbelagt informasjon. Taushetsbelagt informasjon er definert og regulert i forvaltningsloven. Taushetsplikt i forvaltningsloven innebærer at enhver i virksomheten 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.»

Taushetspliktens og unntak fra denne gjelder derfor også for leverandører av skytjenester til norsk offentlig forvaltning.

6 Skytjenesteavtaler

6.1 Varianter av avtaler

Skytjenesteleverandørenes avtaler består ofte av flere avtaler, og de bør sees i sammenheng. Følgende avtaler er eksempler på avtaler man kan møte ved skytjenesteløsninger:

- Terms of Service (ToS)/Serviceavtaler: Omhandler forholdet mellom skytjenesteleverandør og kunde, herunder kommersielle forhold
- Service Level Agreement (SLA): tjenestenivå for tjenesten, herunder også eventuelle sanksjoner ved brudd på avtalt tjenestenivå.
- Acceptable Use Policy (AUP): tillatt bruk av skytjenesten, herunder hva er akseptert bruk/lagring av skytjenesten. Vilkårene vil kunne beskrive hvordan skytjenesteleverandøren kontrollerer akseptabel bruk fra kundens side.
- Privacy Policy: Skytjenesteleverandørens personvernerklæring.
- Databehandleravtale: se kap. 5.3. Her bør man også se hva de andre avtalene beskriver om personopplysninger.
- Statens standardavtaler for skytjenester (SSA-SKY): omfatter tjenester knyttet til etablering og forvaltning av komplekse skytjenester

6.2 Vilkår i avtalene

Ved alle typer skytjenester bør man vurdere, herunder også se på muligheten for å forhandle om, hva man som kunde kan akseptere. I det følgende gis det en ikke uttømmende liste over eksempler på problemstillinger man møter ved gjennomgang av skytjenesteavtalenes vilkår:

- **Lokasjon for lagring og tilgang:** Hvor lagres alle dataene fysisk? Finnes det flere typer av tilgang til dataene, for eksempel tilgang ved feilretting, kundehenvendelser o.l.? Hva kan den som gjennomfører feilretting faktisk se av dataene?

- **Immaterielle rettigheter:** Dersom man skal utvikle en tjeneste, hvem er det som faktisk besitter de immaterielle rettighetene?
  Der kunden selv ønsker å utvikle en IKT-tjeneste (applikasjon) på en skyløsning (typisk IaaS eller PaaS), bør man vurdere hvem som faktisk har rettigheter til / eier komponentene som inngår i applikasjonen, herunder de immaterielle rettighetene. Dette kan for eksempel være forretnings- og bedriftshemmeligheter, knowhow, patenter, varemerker, design, opphavsrettigheter, firma(navn), domenenavn, åpen kildekode-biblioteker samt kundens informasjon og programkode. Dette kan variere i leverandørenes standardvilkår, og kunden må derfor vurdere eierskapet til komponentene og selve applikasjonen grundig.
- **Sikkerhet:** Hvilket nivå av sikkerhet kan leverandøren tilby? Kan kunden konfigurere sikkerheten slik at eget behov blir imøtegått? Vil skytjenesten kunne tilby den sikkerheten kunden har behov for?

- **Databehandleravtale:** Er det behov for EU Model Clauses e.l.? Beskrives dette behovet i tredjepartsvilkårene? Tilrettelegger databehandleravtalene for at kunden kan oppfylle sine plikter i henhold til GDPR? Oppfyller tredjepartsvilkårene kravene etter GDPR for databehandlere/underdatabehandlere?
- **Tilgjengeligheten av data:** Hvordan kan kunden aksessere data, og er den tilgjengelig til enhver tid (se også SLA)? Hva beskrives i tredjepartsvilkårene om dette?
- **Gjenoppretting av data:** Hvordan skjer gjenoppretting av data? Finnes dataene på flere steder (redundans)? Hvem bærer kostnadene ved gjenoppretting?
- **Muligheten for overføring av data til en ny leverandør (portabilitet):** Hva beskrives i avtalen, kan kunden lett skifte skytjenesteleverandør ved avtalens opphør? Hvordan skal dette praktisk håndteres fra både skytjenesteleverandørens side og kundens side?
- **Back-up av data:** Er back-up inkludert eller ikke? I tilfelle back-up er inkludert hvor lagres dataene og hvordan lagres de? Kunden kan tenkes å ha en lagringsbegrensning i henhold til lovverk, hvordan håndteres dette i løsningen?
- **Tilgjengeliggjøring av data ved undersøkelse fra myndigheter:** Legges dette ansvaret til kunden eller skytjenesteleverandøren?
- **Garantier ved utførelsen av tjenesten**: Finnes det garantier i ToS eller andre avtaler?
- **Erstatningsansvar for tap av data o.l.** Hva er direkte tap og indirekte tap i henhold til ToS eller andre avtaler? Hvordan beregnes erstatningsansvar i henhold til kostnader for tjenesten?
- **Ansvarsbegrensninger:** Har skytjenesteleverandøren inntatt andre vilkår som begrenser eget ansvar?
- **Endring av avtalevilkår:** Hvordan og hvor ofte skjer endringer, og hva åpner tredjepartsvilkårene for? Hvordan skal informasjon om oppdatering av avtalevilkår skje? Hvordan gis det varsel, og hva slags endringer varsles det om? Hvordan vil endringer i funksjonalitet påvirke avtaleforholdet? Gis kunde rom og tid til å vurdere endringene og eventuelt kommer med innsigelser?
- **Avslutning av avtalen:** Hva skjer ved avslutning av avtalen, enten om det er ved oppsigelse som følger naturlig av varighet eller ved heving av avtalen? Er det avtalt sletting? Hva skjer dersom man skal overføre eller ta uttrekk av data til en ny tjenesteleverandør? Hva sier tredjepartsvilkårene om dette? Hvem bærer både kostnader og risikoen for at dataene faktisk blir overført?
- **Tvisteløsning:** Hvilket lands rett gjelder dersom det er tvist om avtalen? Hvor skal tvisteløsning skje?

7 Vedlegg 1: Avrop av skytjenester

Hvis virksomheten din har en idé til en ny IKT-basert tjeneste som kan baseres på en IaaS eller PaaS skytjeneste «i bunn», eller virksomheten ønsker å flytte en eksisterende IKT-basert tjeneste til (ny) skytjeneste, ta kontakt med kundekontakten din i Utviklings- og kompetanseetaten (UKE).

Oslo kommune har avtaler med tre ulike partnere som det kan avropes skytjenester på, henholdsvis Sopra Steria, Crayon og Atea. Kundekontakten i UKE kan hjelpe dere å vurdere behovet dere har, opp mot de ulike avtalene og tjenestene som tilbys samt mot en eventuell egen anskaffelse. UKE vil også, avhengig av kapasitet, kunne bistå dere med rådgivings-, prosjektleder- og utviklingskompetanse etter avtale.

7.1 Systemdriftsavtalen med Sopra Steria

Systemdriftsavtalen med Sopra Steria omfatter en opsjon på avrop av IaaS og PaaS skytjenester fra AWS, Google og Microsoft som virksomhetene i kommunen kan benytte. Ved å avrope skytjenester gjennom Systemdriftsavtalen vil man også få «Cloud integration og drift». Denne tjenesten omfatter bistand, faste vedlikeholdsoppgaver og noen timer rådgiving inkludert i prisen.

Det presiseres at ved avrop av skytjenester i Systemdriftsavtalen (RightCloud) er virksomheten selv ansvarlig for konfigurasjon, kostkontroll, styring, sikkerhet og integrasjon av applikasjoner og data, mens driftsleverandør er ansvarlig for å følge opp funksjonalitet, oppetid og sikkerhet i plattformtjenestene.

Virksomhetene anbefales å ta kontakt med kundekontakten i UKE for mer informasjon om denne avtalen og forutsetninger for avrop på den.

7.2 Samkjøpsavtalen «Lisenser Bredde» med Crayon

Samkjøpsavtalen omfatter forvaltning av Oslo kommunes avtaler med rettighetshaverne om kjøp av lisenser og programvarevedlikehold, rådgivning i forhold til riktig lisensiering, bistand ved revisjoner og lisensregnskap på all programvare som Oslo kommune har, herunder, men ikke begrenset til:

- AWS skytjenester
- Google skytjenester

Avtalen finnes her: https://felles.intranett.oslo.kommune.no/anskaffelser/samkjopsavtaler/ikt-hardware-og-software/lisenser-bredde/

Det presiseres at ved avrop av skytjenester i samkjøpsavtalen er virksomheten selv ansvarlig for konfigurasjon, kostkontroll, styring, sikkerhet og integrasjon av applikasjoner og data, og også

ansvarlig for å følge opp funksjonalitet, oppetid og sikkerhet i plattformtjenestene.

Avtalen har en begrenset ramme. Virksomhetene anbefales å ta kontakt med sin kundekontakt i UKE for mer informasjon om denne avtalen og forutsetninger for avrop på den.

7.3 Samkjøpsavtalen «Lisenser Microsoft» med Atea

Avtalen omfatter blant annet

- følgende tjenester uten ekstra kostnad:
  - Mulighet for direkte kjøp og leie av lisenser og tjenester fra Microsoft, for eksempel for Azure skytjenester
- flere valgfrie opsjoner som i hovedsak faktureres pr. time:
  - Administrasjon av lisenser knyttet til skytjenester
  - Mulighet til å benytte leverandøren som Cloud Solution Provider (CSP), denne opsjonen er priset i prisskjema som ligger vedlagt.

Avtalen finnes her: https://felles.intranett.oslo.kommune.no/anskaffelser/samkjopsavtaler/ikt-hardware-og-software/lisenser-microsoft/

Det presiseres at ved avrop av skytjenester i samkjøpsavtalen er virksomheten selv ansvarlig for konfigurasjon, kostkontroll, styring, sikkerhet og integrasjon av applikasjoner og data, og også ansvarlig for å følge opp funksjonalitet, oppetid og sikkerhet i plattformtjenestene.

Virksomhetene anbefales å ta kontakt med sin kundekontakt i UKE for mer informasjon om denne avtalen og forutsetninger for avrop på den.

7.4 Virksomhetens egen anskaffelse av skytjenester

Dersom avrop av skytjenester på en av de tre ovenstående avtalene ikke møter virksomhetens behov og/eller krav, kan virksomhetene vurdere egen anskaffelse.

Virksomhetene anbefales først å ta kontakt med sin kundekontakt i UKE for mer informasjon om de tre ovenstående avtalene og forutsetninger for avrop på dem, og deretter vurdere om egen anskaffelse er nødvendig.

8 Vedlegg 2: Eksternt veiledningsmateriale om skytjenester

Denne veilederen for Oslo kommune er delvis basert på Cloud Security Alliances (CSAs) veileder «Security Guidance For Critical Areas of Focus In Cloud Computing v4.0».

Lesere som ønsker mer detaljer innenfor de ulike kapitlene, oppfordres til å oppsøke CSAs veileder, på https://cloudsecurityalliance.org/research/working-groups/security-guidance/ .

Det finnes også ulike sikkerhetsmodeller og referansearkitekturer for skytjenester, blant annet hos CSA.

Oslo kommune er medlem av Information Security Forum - ISF. Dette er en internasjonal forening som ikke har noen forbindelse med Norsk informasjonssikkerhetsforum - ISF, som forøvrig Oslo kommune også er medlem av.

For å lære mer om god praksis for bruk av skytjenester på sikker måte (omfatter styring av sikkerhet i skytjenester samt etablering av kjernetiltak for skysikkerhet), se ISFs Standard of Good Practice , kapittel Supply Chain 2 (SC2).

ISF-rapport om sikker bruk av skytjenester, se ISF_Using Cloud Services Securely_Report

Hvis du ikke har tilgang til ISF Live hvor disse dokumentene ligger, se felles intranett om hvordan registrere seg på ISF Live.

Fra NSMs rapport «Risiko 2021»: Virksomheter som har behov for skyløsninger og tjenester fra datasenter, må sette seg godt inn i hvordan dette påvirker deres digitale sikkerhet. NSM anbefaler å legge rådene i temaheftet «Sikkerhetsfaglige anbefalinger ved tjenesteutsetting» til grunn for slike vurderinger. Se https://nsm.no/regelverk-og-hjelp/rapporter/sikkerhetsfaglige-anbefalinger-ved-tjenesteutsetting/om-temarapporten/