SENTER
FOR
IKT I
UTDANNINGEN

Bak skyene er himmelen alltid blå?

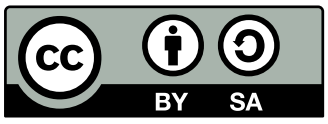
– en innføring i Cloud Computing for skoleeiere

Målgruppen for denne utredningen er IT-ledere, systemarkitekter og sikkerhetsansvarlige hos skoleeiere. Intensjonen er at dokumentet skal være til hjelp i skoleeiers egen vurdeing rundt bruk av skytjenester, personvern-spørsmål som dukker opp i forbindelse med dette, roller og ansvar og hvilke minimumskrav som må settes ved bruk av skytjenester.

Utredningen er skrevet på oppdrag fra Senter for IKT i utdanningen av Stian Danenbarger (Bouvet) i samarbeid med Senter for Rettsinformatikk.

Senter for IKT i utdanningen skal sikre bedre bruk av IKT for økt kvalitet, styrket læringsutbytte og bedre lærings-strategier i utdanningen. Barn i barnehagen, elver i grunnskolen og videregående opplæring og studenter i førskole-lærer- og lærerutdanningen er hovedmålgruppene for senterets arbeid. Senter for IKT i utdanningen er underlagt Kunnskapsdepartementet

post@iktsenteret.no
www.iktsenteret.no



Introduksjon

På 1950-tallet gikk ”databehandling” fra å være noe som tilhørte noen få store offentlige instanser til å bli tilgjengelig for bedrifter. Senere, på 70-tallet, dukket begrepet ”personlig databehandling” opp, sammen med de første PCene. Tjue år senere førte framveksten av ”World Wide Web” til store omveltninger på mange områder, ikke minst en enorm PC-vekst og desentralisering av prosessorkraften. Nå, etter ytterligere 20 år, er det mange anerkjente analytikere som hevder at vi i dag ser pendelen svinge tilbake mot industrialisert sentralisering i ”skyen” – nettbaserte tjenester levert fra store, strategisk lokaliserte datasentre.

Spekteret av tjenester i ”skyen” utvikles hurtig, men fokuset er inntil videre på horisontale, tverrsektorielle applikasjoner og tjenester. Denne veilederen reflekterer dette, og de tekniske og økonomiske betraktningene her er ikke sektorspesifikke. Det er grunn til å tro at leverandører gradvis og i økende grad vil oppfylle bransjespesifikke behov med hensyn til lovgiving, tjenestegarantier, m.v., for å oppnå utvidet aksept og mer gjennomgående anvendelse i virksomhetene. Omfanget av persondata som forvaltes innen utdanningssektoren, ikke minst data om mindreårige, stiller eksempelvis særlige krav til sektorens – og kanskje spesielt skoleeieres – bevissthet. I skyen har skoleeier begrenset kontroll over flyten og bruken av persondata. Skyen åpner mange nye forretningsmuligheter for leverandørene, og persondata har blitt en verdifull handelsvare[1]. Når sektoren vurderer å bruke tjenester i skyen i administrative eller pedagogiske sammenhenger framover, reiser dette derfor viktige utfordringer knyttet til hvordan elevenes eller lærernes persondata håndteres på måter som ikke krenker personvernet.

Før skoleeiere tar stilling til bruken av skytjenester, er det viktig at de har god informasjon om hva skytjenester er, hvilken nytte de kan ha av slike tjenester og hvilke personvernmessige utfordringer som bruken av tjenestene reiser. Denne rapporten vil derfor skissere hovedlinjene i utviklingen av skytjenester og løfte frem de viktigste personvernmessige aspektene som denne utviklingen bringer med seg.

Sammendrag

Hvorfor Cloud Computing?

- Endret koststruktur fra store engangsinvesteringer til variabel kost basert på ressursbruk gir fleksibilitet, og kan bety kostnadsbesparelser
- Betydelige tidsbesparelser ved endringer i IT-infrastruktur, spesielt mht skalering
- Mer veldefinert, handelsvare-liknende tilnærming til outsourcing

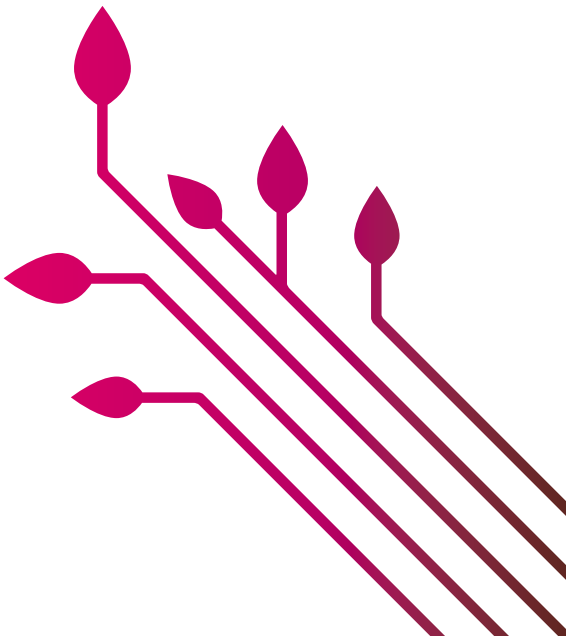
Hvorfor ikke Cloud Computing?

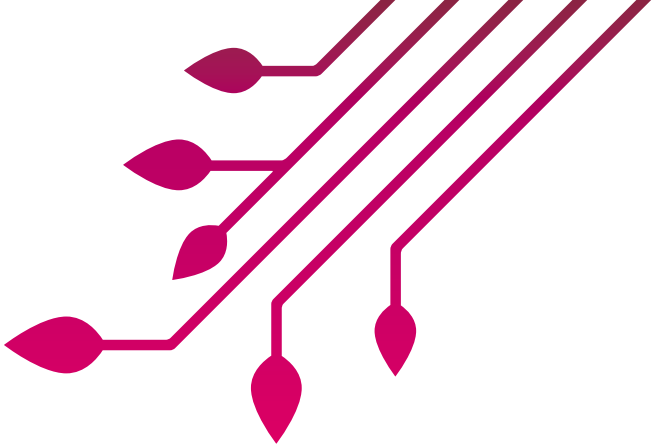
- Skolesektoren behandler persondata om mindreårige, dvs. personer som har selvstendig rett til personvern, men som ikke alltid kan forventes å ivareta sine personvernrettigheter på egen hånd
- Proprietært på mange områder, spesielt implementasjon og logikk (er tilbyderne motivert for interoperabilitet på tvers av plattformene...?)
- Ofte utilstrekkelige tjenestegarantier (SLA) og målemetoder for virksomhetskritiske anvendelser
- Prosesserings- og lagringskostnadene på sluttbrukersiden har lenge falt langt raskere enn båndbreddekostnadene, og gjør det fortsatt. Kostnadsbesparelsen ved å flytte prosesseringen til skyen er i mange tilfeller ikke stor nok i forhold til båndbreddekostnaden ved å flytte dataene, spesielt for dataintensive applikasjoner

Samlet anbefaling

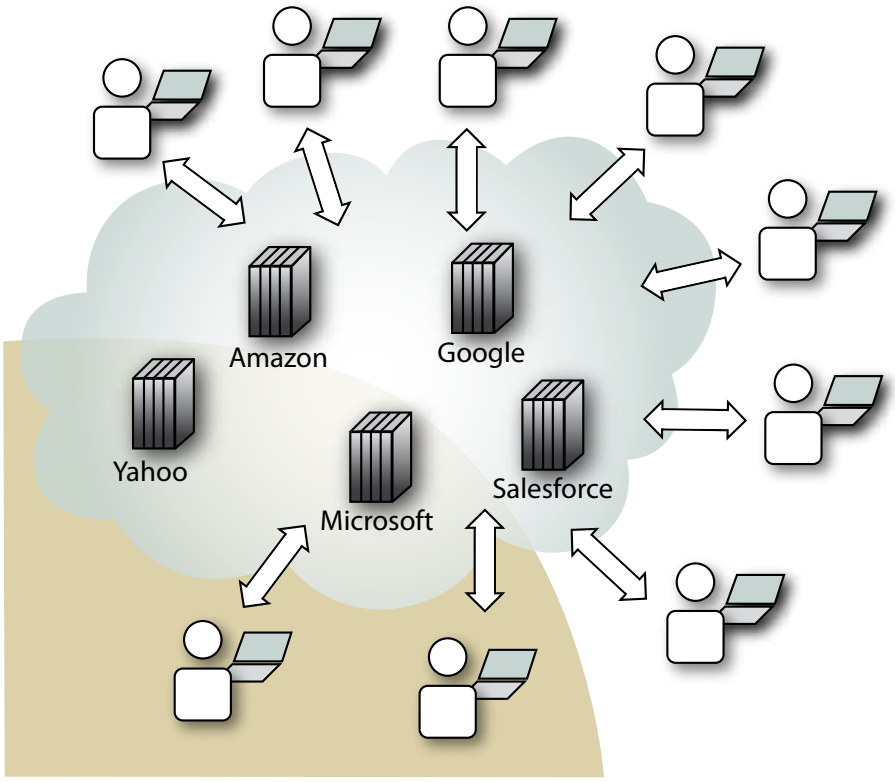
- Dersom det er nødvendig å lagre persondata i skyen, foretrekk leverandører som har tilrettelagt for datalagring innenfor grensene av EU, og som gjør det enkelt å kontrollere dette
- Forstå forretningsmodellen til tjenesteleverandøren. Mange leverandører i skyen har uklare tjenesteavtaler rundt formålet med å innhente persondata, og forretningsmodellen kan indikere om leverandøren kan ha et eget formål med håndteringen
- Prosessering bør skje nettverksmessig ”nær” dataene. Prosessering i ”skyen” lønner seg typisk bare for svært CPU-intensive applikasjoner[2]. Når data skal integreres fra flere kilder over nettverket, bør dataprosessering og -filtrering skje ved kilden
- Vær oppmerksom på svake tjenestegarantier, spesielt med hensyn til prosessorkraft
- Flere indikasjoner peker i retning av mer informasjonsintegrasjon på klientsiden, ikke minst personvernhensyn

Innhold





Hva er Cloud Computing?



Det finnes mange definisjoner, men ifølge det amerikanske standardi-seringsorganet NIST (National Institute of Standards and Technology) er ”Cloud Computing” en modell for nettbasert tilgang til mengder av konfigurerbare, delte dataressurser (f.eks. nettverk, servere, lagring, programmer og tjenester) som raskt kan allokeres og avgis etter behov, med minimal administrativ innsats eller involvering av tjenesteleverandør[3].

Begrepet ”cloud” (som regel direkte oversatt til ”sky” på norsk) brukes som en metafor for Internett, med utspring i den typiske framstillingen av Internett i nettverksdiagrammer[4]. Her er ”skyen” er en bevisst abstraksjon av den underliggende infrastrukturen, for å skjule kompleksitet. Begrepet antas å ha sin opprinnelse i telefoniverdenen, der langdistanse-operatørene på begynnelsen av 1990-tallet begynte å tilby garantert båndbredde over dynamisk rutede linjer for bedre utnyttelse av den totale båndbredden i nettverket[5]. Den dynamiske balanseringen gjorde det umulig å vite nøyaktig hvilken rute nettverkstrafikken tok, noe som kan minne om enkelte av kjennetegnene ved ”Cloud Computing”.

Typiske kjennetegn

Behovsbasert selvbetjening

Tjenestebrukere kan selv allokere prosesseringsressurser, for eksempel servertid og nettverkslagring, automatisk og etter behov, uten at det krever menneskelig interaksjon med de enkelte tjenesteleverandørene.

Bred nettilgang

Dataressursene er tilgjengelige over nettet, gjennom standardmekanismer som støtter bruk av heterogene tynne eller tykke klientplattformer (for eksempel mobiltelefoner, bærbare PCer og PDAer).

Ressursdeling

Leverandøren samkjører store dataressurser for å betjene svært mange tjenestebrukere ved hjelp av en leietakermodell med mange samtidige leietakere. Ulike fysiske og virtuelle ressurser tildeles dynamisk, avgis og tildeles igjen, i henhold til tjenestebrukernes etterspørsel. Det hele preges av stedsuavhengighet, ved at kunden vanligvis ikke vet, eller har kontroll over, den nøyaktige lokaliseringen av de tilgjengelige ressursene. Hvis mulig, kan lokaliseringen angis på et høyere abstraksjonsnivå

(f.eks. land, stat eller datasenter). Eksempler på ressurser er lagring, prosessering, hukommelse, båndbredde på nettverket, og virtuelle maskiner.

Fleksibel og svært skalerbar kapasitet

Tjenestens kapasitet kan allokeres hurtig, i noen tilfeller helt automatisk, til raskt å skalere ut og raskt avgis for å skalere inn igjen (”elastisk”). For tjenestebrukeren kan den allokerbare kapasiteten ofte synes å være ubegrenset, og tilsynelatende mulig å kjøpe i hvilken som helst mengde når som helst.

Forbruksmålte tjenester

Systemer i skyen styrer og optimaliserer ressursbruken automatisk ved å måle kapasitet på et abstraksjonsnivå som passer til tjenestetypen (for eksempel lagring, behandling, båndbredde og aktive brukerkontoer). Ressursbruken kan overvåkes, styres og rapporteres på en måte som sikrer åpenhet både for tjenesteleverandør og -bruker.

Typiske tjenestemodeller

Software as a Service (SaaS)

Tjenestebrukeren tilbys å kjøre leverandørens applikasjoner på en infrastruktur i ”skyen”. Applikasjonene er tilgjengelige via ulike klienter over et tynt klientgrensesnitt, som en nettleser. Webbasert epost er et typisk eksempel. Tjenestebrukeren har ingen kontroll over den underliggende infrastrukturen, herunder nettverk, servere, operativsystemer, lagring, eller den enkelte applikasjonens funksjonalitet, med mulig unntak av begrensede, brukerspesifikke konfigurasjonsinnstillinger. Sikkerhetsansvaret hviler i høy grad på applikasjonsleverandøren.

Rundt årtusenskiftet ble SaaS gjerne omtalt som ”ASP” (fra eng.: *”Application Service Provider”*).

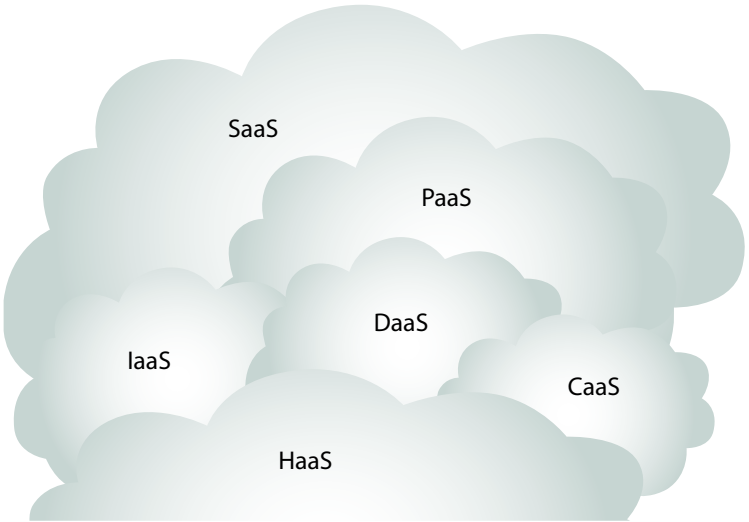
Platform as a Service (PaaS)

Tjenestebrukeren tilbys å distribuere egne eller andres applikasjoner på infrastruktur i skyen, gitt at de er utviklet i programmeringsspråk og verktøy som støttes av tjenesteleverandøren. Tjenestebrukeren har ingen kontroll over den underliggende infrastrukturen, herunder nettverk, servere, operativsystemer eller lagring, men har kontroll over applikasjonene, samt muligens konfigurasjonen av applikasjonenes driftsmiljø. Sikkerhetsansvaret deles mellom tjenestebruker og -leverandør, gitt at tjenestebruker har fulgt leverandørens policy.

Infrastructure as a Service (IaaS)

Tjenestebrukeren tilbys å allokere prosessering, lagring, nettverk og andre grunnleggende dataressurser der tjenestebrukeren kan distribuere og kjøre vilkårlig programvare, gjerne såvel operativsystemer som applikasjoner.

IaaS muliggjøres ved relativt nye fremskritt innen virtualisering, spesielt *paravirtualisering* og *hardware-assistert* virtualisering. Selv om begge disse virtualiseringsteknologiene skal ha hensyntatt behovet for ytelsesmessig isolasjon mellom virtuelle maskiner som konkurrerer om felles ressurser, har det vist seg vanskelig å unngå en viss gjensidig påvirkning. Fremveksten av multikjernearkitekturer har forverret problemet ytterligere. Dette har gjort det vanskelig for skytilbydere å tilby garantert ytelse. I stedet tilbyr de gjerne svakere tjenestegarantier (SLA) til en konkurransedyktig pris. Slike svake garantier lekker opp gjennom lagene, og påvirker tjenestegarantiene for hele systemer bygget over IaaS-plattformer.[6]



IaaS-brukeren har ingen kontroll over den underliggende infrastrukturen, men har kontroll over operativsystemer, lagring, distribuerte programmer, og muligens begrenset kontroll over utvalgte nettverkskomponenter (f.eks. brannmurer).

Sikkerhetsansvaret hviler i høy grad på tjenestebruker, men leverandøren kan tilby ulike sikkerhetsmekanismer i infrastrukturen som tjenestebrukeren kan anvende.

Datastorage as a Service (DaaS)

Data-Storage as a Service (DaaS) er nettbasert datalagring som lar brukere og applikasjoner lagre data på eksterne disker i "skyen". Datalagring i skyen må møte en rekke strenge krav for å ivareta brukernes behov, inkludert høy tilgjengelighet, pålitelighet, ytelse, replikering og datakonsistens. Disse kravenes motstridende natur gjør at ingen systemer fullt ut støtter alle. For eksempel kan tilgjengelighet, skalerbarhet og datakonsistens betraktes som motstridende mål. DaaS-tilbydere må derfor implementere systemer som favoriserer en av egenskapene, og dette gjenspeiles gjerne i tjenestegarantien. Relasjonsbaser prefererer for eksempel strengere konsistens på bekostning av tilgjengelighet, mens "*key-value*"-basert lagring legger mer vekt på tilgjengelighet, og mindre på konsistens.

Communication as a Service (CaaS)

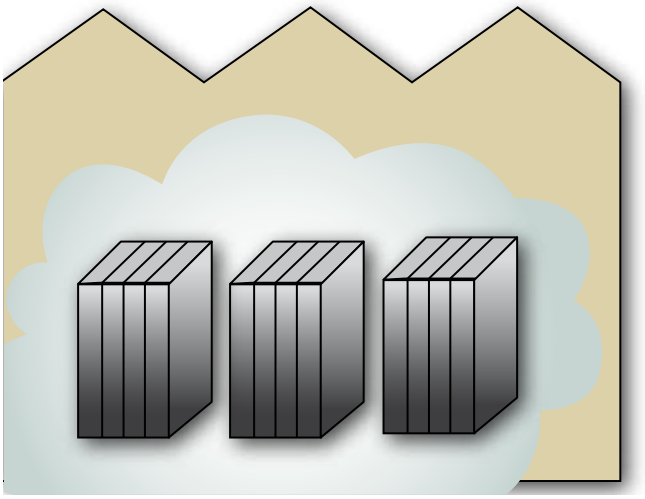
Kommunikasjon er en viktig del av skyens infrastruktur, og behovet for garantert tjenestekvalitet (*QoS*) for nettverkskommunikasjon vokser som en følge av dette. Flere sky-leverandører har derfor sett seg forpliktet til å tilby nettbaserte kommunikasjonstjenester som er tjenesteorienterte, konfigurerbare, tidsstyrte, forutsigbare og pålitelige. *Communication as a Service (CaaS)* er et "sky"-basert tjenesteområde som har vokst fram for å støtte slike krav, foruten nettverkssikkerhet, dynamisk tilbudte, virtuelle lag for trafikkisolasjon eller dedikert båndbredde, garantert meldingsforsinkelse, kommunikasjonskryptering, og nettverksovervåking. Selv om denne modellen inntil videre er den minst diskuterte og selvstendig benyttede kommersielle skytjenesten, har det vært mye forskning på området. VoIP-telefonsystemer, lyd-og videokonferanser samt chat kan bygge på CaaS, og i sin tur inngå i andre applikasjoner.

Hardware as a Service (HaaS)

Den nederste laget i skyen består av den faktiske fysiske maskinvaren og nettverksmessige infrastrukturen, og brukerne av dette laget er normalt store virksomheter med høye krav. Driftsleverandører opererer, styrer og oppgraderer maskinvaren på vegne av brukerne, slik at disse ikke trenger å investere i, bygge og håndtere datasentre. Leverandørene besitter den tekniske kompetansen og den kosteffektive infrastrukturen som kreves. Tjenestegarantiene i denne modellen er stringente, ettersom bedriftsbrukere gjerne har forhåndsdefinerte arbeidsbelastninger som stiller strenge krav. Leverandører av HaaS må håndtere en rekke tekniske utfordringer når det gjelder drift og administrasjon, ikke minst med hensyn til effektivitet, brukervennlighet og hurtig opp- og nedskalering etter behov.

Typiske distribusjonsmodeller

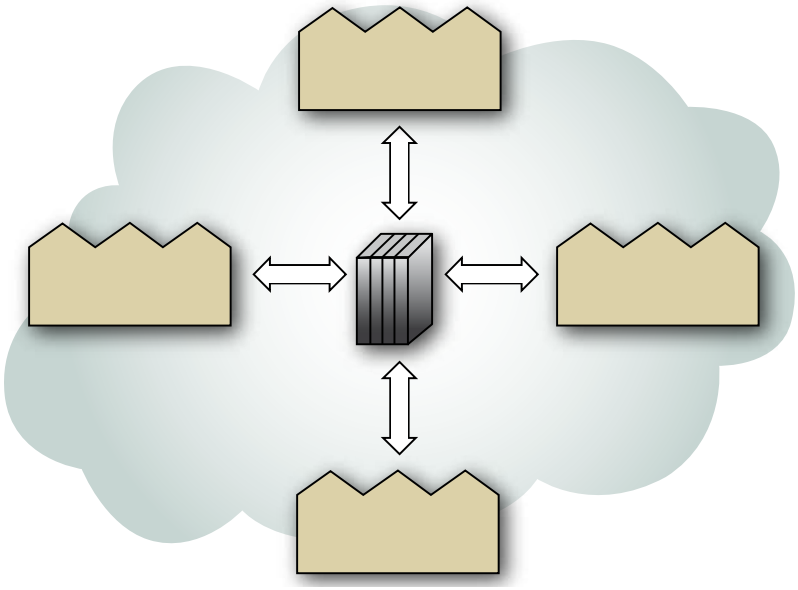
Privat sky



Privat sky
Infrastrukturen er administrert av virksomheten selv, og driftet innenfor brannmuren. Private skyer, av og til omtalt som "interne skyer", må virksomheter fortsatt kjøpe, bygge og administrere, og det har vært stilt spørsmål ved den økonomiske gevinsten ved dette[7].

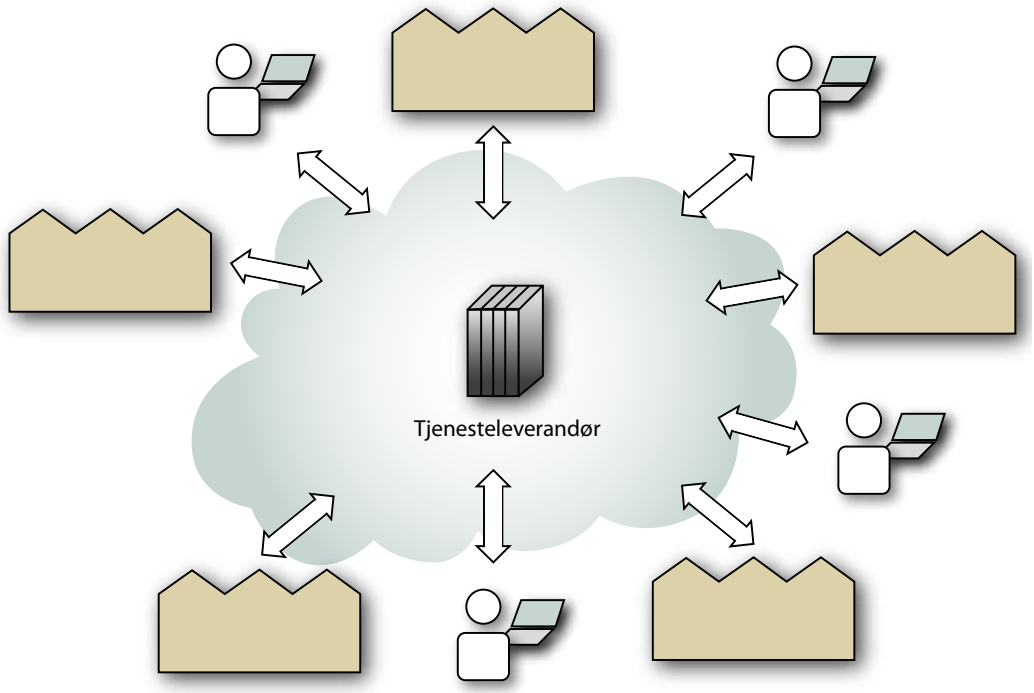
Virtuell privat sky
Infrastrukturen administreres av en tredjepart, og driftes fysisk utenfor brannmuren, men aksesseres over en kryptert linje og kan også i noen tilfeller innlemmes sømløst i virksomhetens sikkerhetskontekst. Begrepet "privat" må med andre ord forstås i *logisk* forstand, ikke fysisk, ihvertfall for PaaS-tjenester.

Delt sky



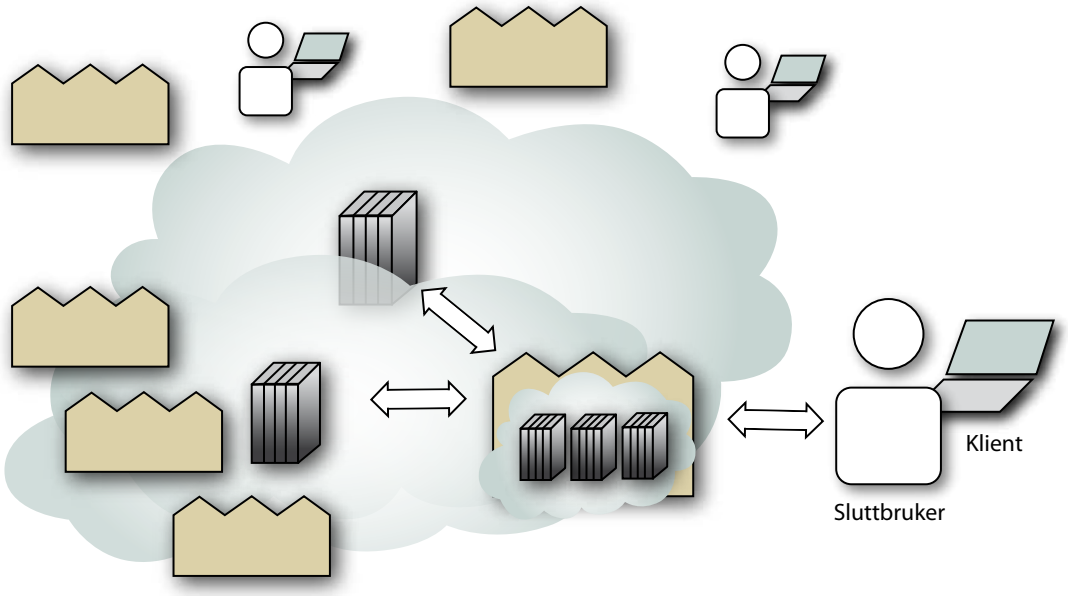
Skyens infrastruktur deles av flere virksomheter, og støtter et bestemt fellesskap som har delte hensyn å ta (f.eks. mht. misjon, sikkerhetskrav, personvern, og overholdelse av lov og direktiv). Infrastrukuren kan administreres av virksomhetene selv eller en tredjepart, og kan være lokalisert i virksomhetenes interne drifts-miljø eller utenfor.

Offentlig sky



Skyens infrastruktur gjøres tilgjengelig for allmennheten eller en større næringsgruppe, og eies av en virksomhet som selger skybaserte tjenester.

Hybridsky



Skyens infrastruktur er satt sammen av to eller flere skyer (private, delte eller offentlige) som forblir selvstendige enheter, men knyttes sammen gjennom standardisert eller proprietær teknologi som muliggjør data- og applikasjonsportabilitet (f.eks. såkalt ”Cloud Bursting” for lastbalansering mellom skyer).

Enkelte analytikere mener hybridsky-miljøer etterhvert vil være ”typisk for de fleste virksomheter”[8].

Skyer er flyktige fenomener...

Kritikere har pekt på de mange vage og vidtfavnende definisjonene av ”Cloud Computing”. *Larry Ellison*, CEO i *Oracle Corporation*, sa på *Oracle OpenWorld 2008*[9 10]: *”The interesting thing about cloud computing is that we’ve redefined cloud computing to include everything that we already do. I can’t think of anything that isn’t cloud computing with all of these announcements. The computer industry is the only industry that is more fashion-driven than women’s fashion. Maybe I’m an idiot, but I have no idea what anyone is talking about. What is it? It’s complete gibberish. It’s insane. When is this idiocy going to stop? We’ll make cloud computing announcements. I’m not going to fight this thing. But I don’t understand what we would do differently in the light of cloud.”*

Edge Computing

Som navnet antyder, skiller ”Edge Computing” seg fra den sentraliserte ”Cloud Computing”-modellen ved at applikasjoner, data og datakraft distribueres til de logiske ytterkantene av nettverket – nærmest mulig klienten. Wikipedia[11] beskriver modellen som en slags ”programvare-cache”, hvor hurtigbufferet er Internettet selv. I denne modellen replikeres fragmenter av informasjon på tvers av distribuerte nettverk av web-servere, som kan være stort og omfatte mange nettverk. Speiling av statiske nettsteder er ikke nytt, men Edge Computing viderefører prinsippet til transaksjonsbaserte og interaktive systemer, noe som er langt mer krevende. Modellen legger visse begrensninger på valg av teknologiplattform, applikasjoner og tjenester, som alle må være spesielt utviklet eller konfigurert for denne distribusjonsmodellen.

Edge Computing hevdes å ha noen viktige fordeler i forhold til Cloud Computing:

- Nettverksbasert bufring nær brukeren kan medføre en betydelig nedgang i datavolumet som må flyttes, ikke minst i den påfølgende trafikken, og avstanden dataene må gå, og dermed redusere overføringskostnader og ventetid, og forbedre tjenestekvaliteten (QoS).
- Modellen eliminerer, eller i det minste reduserer, betydningen av et sentralisert servermiljø, og begrenser eller fjerner derved en potensiell flaskehals og et mulig feilpunkt.

For øvrig har Edge Computing mye til felles med Cloud Computing, som behovsbasert selvbetjening, bred nettilgang, ressursdeling basert på en leietakermodell, fleksibel og svært skalerbar kapasitet, og forbruksmålte tjenester.

Klientsky (”personlig sky”)

Carl Hewitt, forsker og emeritus ved MIT, definerer[12] en klientsky som en ”lokal sky” kontrollert av en klientenhet, for eksempel en mobiltelefon, en PC eller et hjemme-underholdningssenter.

Hewitt mener at informasjonsintegrasjon i større grad burde gjøres på klientsiden, og at skyenes datasentre tilsvarende burde lagre informasjon på en slik måte at den bare kan dekrypteres ved hjelp av en hemmelig nøkkel på klientenheten og sammenstilles der.

Av personlige data som best integreres på klientsiden nevner Hewitt kalendere og oppgavelister, epost, SMS- og Twitter-arkiver, tilstedeinformasjon, kart (inkludert firmaer, interessepunkter, trafikk, parkering og vær), hendelser (inkludert varsler og status), dokumenter (inkludert presentasjoner, regneark, forslag, jobbsøknader, helseinformasjon, bilder, videoer, gavelister, memoer, innkjøp, kontrakter, artikler), kontakter (inkludert sosiale grafer og autoritetsinformasjon) og søkeresultater (inkludert rangeringer og karakterer).

Integrasjon på klientsiden har noen viktige fordeler. Klienten opererer raskere når den ikke er avhengig av løpende kommunikasjon med tjenester i skyen, samtidig som tjenesteleverandørenes kapital-, drifts- og kommunikasjonskostnader kan holdes lavere fordi integrasjonen utføres på klientsiden i stedet for i leverandørenes datasentre. Hewitt hevder også at den rikere tilgangen på data på klientsiden gjør at leverandører kan levere mer adaptive eller personaliserte tjenester. Samtidig mener han at integrasjon på klientsiden vil redusere behovet for framtidig offentlig regulering, hvis det innebærer at informasjonen i datasentre kan holdes tilstrekkelig anonymisert og desentralisert.

Andre Internett-plattformer

Tidligere Netscape-gründer Marc Andreessen mener at en ”Internett-plattform” må kunne programmeres for å kunne kalles en plattform, og har karakterisert tre plattform-nivåer[13]:
Access API - applikasjonen eksekveres utenfor plattformen, typisk på en maskin som eies av tjenestebrukeren, og aksesserer data eller tjenester som tilbys av plattformen over Internett.
Plug-In API - som nivå 1, men applikasjonens funksjonalitet framstår som integrert i plattformens. *Facebook*-applikasjoner er et typisk eksempel. Applikasjoner for nivå 2 er betydelig mer krevende å utvikle enn for nivå 1.
Runtime Environment - applikasjonen lastes opp og eksekverer i selve *plattformen*, slik at tjenestebrukeren ikke trenger egen maskinvare, lagring, database, båndbredde, m.v. Plattformen tilbyr et komplett miljø for å eksekvere applikasjonen, slik at tjenestebrukeren i mange tilfeller bare trenger en nettleser. Applikasjoner for nivå 3 kan være betydelig enklere å utvikle enn for nivå 1 og 2, og flere størrelsesordener enklere å drifte. Til gjengjeld vil applikasjonene ikke fungere hvis plattformen forsvinner.

Sistnevnte nivå er på mange måter sammenfallende med *Platform as a Service (PaaS)*, som definert ovenfor. Andreessen legger i sin definisjon størst vekt på plattformer for bestemte anvendelser, som *Ning.com* for sosiale nettverkstjenester og *Salesforce.com* for virksomhetsrettede tjenester, som begge favner alle tre nivåene nevnt over.

Personopplysninger i skyen – rettslige utgangspunkter

Når persondata behandles innenfor rammen av "Cloud Computing", gjelder visse regler for personvern og behandling av personopplysninger[14]. Disse reglene bør både de som benytter seg av og tilbyr tjenester i skyen være oppmerksom på. Reglene finnes i første rekke i personopplysningsloven og personopplysningsforskriften (som trådte i kraft i 2001).

Formålet med reglene i personopplysningsloven og forskriften er å unngå krenkelser av grunnleggende personvernhensyn (spesielt privatlivets fred og den enkeltes personlig integritet) når behandlingen av persondata helt eller delvis skjer ved hjelp av elektroniske hjelpemidler (datamaskiner og programvare).

Slike krenkelser kan for eksempel oppstå hvis følsomme opplysninger om enkeltpersoner eksponeres i det offentlige rom, eller hvis opplysningene som samles inn er ufullstendige slik at de gir et misvisende bilde av den eller de som opplysningene gjelder.

Dagens regelverk for behandling av persondata er sektoruavhengig, det vil si at de samme reglene gjelder for virksomheter i alle bransjer eller sektorer hvor elektroniske hjelpemidler benyttes til håndtering av persondata. Samtidig baserer det norske regelverket seg på EUs direktiv om personopplysningsvern fra 1995. Det betyr at lovgivningen på området ikke er et særnorsk fenomen, men at vi finner tilsvarende regelverk (med tilsvarende regler) i de øvrige EU- og EØS-landene.

Både i Norge og i de andre EU/EØS-landene er det opprettet egne datatilsynsmyndigheter som har i oppgave å informere om regelverket, føre kontroll med at det overholdes og å sanksjonere eventuelle regelbrudd[15].

Nedenfor vil vi først gi en kort presentasjon av hvilke regler som gjelder for behandling av persondata. Deretter vil vi drøfte hvordan disse reglene kan tenkes å komme til anvendelse i "Cloud Computing".

Persondata

I personopplysningsloven og forskriften defineres persondata som *all informasjon* som kan knyttes til *enkeltpersoner*. Persondata vil derfor være opplysninger om navn og adresse, telefon- og fødselsnummer, hobbyer og fritidssysler, skoleprestasjoner og helsedata. Det er ikke en forutsetning at persondata foreligger skriftlig – de kan også foreligge i form av bilder, video- eller audioopptak hvor enkeltpersoner kan gjenkjennes. Persondata vil i tillegg omfatte alt av opplysninger om oss selv eller andre som legges ut på internettet eller informasjon om hva vi bruker internettet til (for eksempel hvilke nettsteder vi har besøkt).

I skolesektoren vil mye av informasjonen som behandles i digitale læringsplattformer være å regne som persondata (enten om elever, lærere eller foresatte), mens mesteparten av den informasjonen som skolene legger ut på sine hjemmesider[16] ikke er persondata[17].

Lovverket i Norge og EU skiller mellom to hovedtyper persondata: *alminnelige* og *sensitive*. Sensitive persondata er bl.a. opplysninger om helsemessige forhold, rasemessig eller etnisk bakgrunn, politiske, religiøse eller filosofiske anskuelser, seksuell legning og informasjon om straffbare forhold. Andre typer persondata regnes som *alminnelige*. Det er strengere regler for behandling av sensitive enn alminnelige persondata, for eksempel ved at sensitive persondata er underlagt konsesjonsplikt, mens behandling av alminnelige persondata kun er underlagt meldeplikt[18]. I tillegg stilles det strengere vilkår for sikring av sensitive persondata[19].

Anonymiserte opplysninger kan ikke knyttes til identifiserbare enkeltpersoner - de er strippet for identifiserende elementer (for eksempel navn, adresse, fødselsnummer, osv.). Det betyr at de ikke regnes som persondata, og elektronisk behandling av denne typen opplysninger reguleres derfor ikke av reglene i personopplysningsloven og forskriften.

Reguleringsprinsipper og rettigheter

Prinsippet i dagens lovverk er at vi som enkeltpersoner skal ha en viss kontroll og medinnflytelse over hvordan andre behandler opplysninger som angår oss selv. En viktig regel i lovverket er derfor at de som behandler våre persondata ikke kan bruke opplysningene til andre enn eksplisitt definerte formål, og at de ikke samler inn flere data enn hva som strengt tatt er nødvendig[20]. Samtidig er det et krav at de opplysningene som innsamles er korrekte, fullstendige og oppdaterte.

En annen viktig regel er at de som benytter opplysninger om andre personer må skaffe seg lov til å behandle opplysningene før de kan sette i gang å bruke dem. Lovverket definerer tre mekanismer som gjør det lovlig å behandle opplysninger om andre. Dette kan skje ved at:

1. vi samtykker til at andre behandler opplysninger om oss,
2. lover og forskrifter (for eksempel opplæringsloven med forskrifter) gir andre (skolen/skoleeier) rett til å behandle opplysninger om oss, eller
3. andre har en "nødvendig grunn" til å behandle opplysninger om oss (for eksempel fordi de trenger opplysningene for å oppfylle en kontraktsmessig forpliktelse overfor oss).

Når de som behandler persondata har skaffet seg lov til å gjøre bruk av opplysningene, gir lovverket oss visse rettigheter:

- **Informasjon:** Vi skal bl.a. få informasjon om hva andre bruker opplysninger om oss til, hvem som gjør bruk av opplysningene, om opplysningene vil bli videreformidlet til andre og hvor lenge det er bruk for opplysningene.
- **Innsyn:** Vi kan kreve å få vite hvilke opplysninger som andre behandler om oss.
- **Retting/supplering:** Vi kan kreve at feilaktige eller misvisende opplysninger rettes og at ufullstendige opplysninger utfylles med nye.
- **Sletting:** Vi kan kreve sletting av opplysninger som andre ikke trenger å ha om oss eller som de ikke lenger har behov for å lagre.

Roller og ansvar

Det som til nå er sagt om (a) mekanismer for å skaffe seg lov til å behandle personopplysninger og (b) de viktigste rettighetene vi har i forhold til de som behandler våre persondata, innebærer at regelverket definerer visse roller som det knyttes rettigheter og plikter til. Vi vil nå gi en kort fremstilling av disse rollene (med tilhørende rettigheter og plikter) fordi de er relevante i forbindelse med "Cloud Computing":

- **Den registrerte:** vedkommende person som opplysningene gjelder. Rettighetene i regelverket knytter seg til den registrerte, bl.a. retten til å samtykke og retten til informasjon, innsyn, retting/supplering og sletting. Hensikten med rettighetene er at den registrerte skal sikres en viss råderett over bruken av egne persondata. I "Cloud Computing" vil sluttbrukeren være å regne som "den registrerte", for eksempel den enkelte elev.
- **Den behandlingsansvarlige:** vedkommende (virksomhet eller person) som (a) behandler opplysninger om andre personer og (b) bestemmer hva opplysningene skal brukes til og hvilke elektroniske hjelpemidler som benyttes. Pliktene i regelverket retter seg mot den behandlingsansvarlige, bl.a. plikten til å skaffe seg lov til å behandle persondata, plikten til å søke om konsesjon for behandling av sensitive persondata, plikten til å ha et tydelig formål med bruken av persondata, plikten til å gi den registrerte sine rettigheter og plikten til å sørge for tilfredsstillende informasjonssikkerhet. Dette omfatter også plikten til å holde god kontroll med behandlingen av persondata som er satt ut til andre virksomheter (såkalte databehandlere). I "Cloud Computing" vil det ofte være slik at den virksomheten som benytter seg av tjenestetilbydere i skyen, er å regne som "den behandlingsansvarlige", for eksempel skoleeier.
- **Databehandler:** en virksomhet eller person som behandler persondata etter oppdrag fra den behandlingsansvarlige (dette er spesielt relevant i forhold til out-sourcing av IT-systemer hvor persondata behandles). Databehandleren plikter å ikke bruke opplysningene på andre måter eller til andre formål enn det som er avtalt med den behandlingsansvarlige. Det betyr at databehandleren ikke har noen selvstendig råderett over opplysningene – det er den behandlingsansvarlige som forvalter denne råderetten. Den behandlingsansvarlige plikter derfor å lage en skriftlig kontrakt med databehandleren – en databehandleravtale. Her skal det fremgå hva databehandleren kan bruke opplysningene til og at opplysningene sikres mot brudd på informasjonssikkerheten. I "Cloud Computing" vil for eksempel aktører som tilbyr leietakertjenester være å regne som databehandlere.

Det er i utgangspunktet ikke tillatt for behandlingsansvarlige som befinner seg innenfor EU/EØS-området å overføre persondata til virksomheter i land som ikke gir tilsvarende beskyttelse mot krenkelser av personvernet som EUs personopplysningsdirektivet og den norske personopplysningsloven (med forskrift) legger opp til.

Personvernutfordringer i skyen

"Cloud Computing" reiser en rekke utfordringer i forhold til de reglene for behandling av persondata som er beskrevet ovenfor. Vi vil ikke drøfte alle utfordringene her, men de viktigste og mest prinsippielle kan skisseres i følgende hovedpunkter:

- **Skyens "utstrekning":** Hvis skyen strekker seg utenfor EU/EØS-området – og persondata overføres til virksomheter og tjenestetilbydere som ligger utenfor dette området – kan slik overføring være ulovlig i henhold til dagens regelverk i Norge og EU/EØS. Det er bare noen få land utenfor EU/EØS-området som i dag vurderes å ha tilstrekkelig gode personvernregelverk på plass til at overføring av persondata aksepteres. Med bakgrunn i generell personvernstenkning kan det samtidig være en fordel om de behandlingsansvarlige i skyen er lokalisert i den registrertes (sluttbrukerens) geografiske nærhet: det kan være enklere å for den registrerte å ivareta sine rettigheter hvis den behandlingsansvarlige befinner seg i nærheten enn hvis han befinner seg langt unna.
- **Skyens "gjennomsiktighet":** Hvis skyen er lite gjennomsiktig, slik at det blir vanskelig å vite hvem som gjør bruk av våre persondata, hva persondataene brukes til og om de utleveres/utveksles mellom ulike aktører i skyen, kan det bli problematisk for den

registrerte å vite hvem han eller hun skal henvende seg til for å få sine rettigheter ivaretatt. Samtidig kan det være problematisk for den behandlingsansvarlige å vite hvem som er databehandler, det vil si hvilke andre aktører i skyen som håndterer persondata som vedkommende er rettslig ansvarlig for. Dermed kan det også bli vanskelig å oppfylle kravet om at databehandlere (for eksempel tilbydere av leietakertjenester) bare kan benytte persondataene etter vilkår som fremgår av skriftlig avtale med den behandlingsansvarlige.

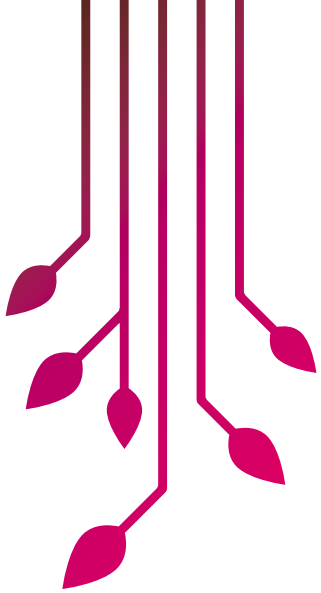
- **Skyens struktur:** Hvis nettbaserte tjenester leveres av noen få, store og strategisk lokaliserte tjenesteleverandører i skyen, kan dette føre til større gjennomsiktighet og oversikt over hvem som er ansvarlig for hvilke opplysninger. Dermed kan det også bli enklere for den registrerte (tjenestebrukeren) å vite hvem han/hun skal henvende seg til for å få sine rettigheter ivaretatt. Men samtidig reiser sentralisering i skyen viktige personvernutfordringer fordi noen relativt få virksomheter forvalter store mengder persondata om veldig mange registrerte. På denne måten kan risikoen for misbruk av opplysningene (og muligheten for krenkelser av personvernet) øke. Spredning av personopplysninger på flere uavhengige virksomheter kan redusere denne personvernrisikoen, men det forutsettes at spredningen skjer på en slik måte at den registrerte får god informasjon om og innsikt i hvor opplysningene til enhver tid befinner seg og hva som skjer med dem.
- **Type persondata:** Generelt sett vurderes det å være mindre personvernrisiko knyttet til behandlingen av alminnelige enn til behandlingen av sensitive persondata. Når sensitive persondata overlates til behandlingsansvarlige eller databehandlere i skyen, er derfor regelen at det stilles særlig strenge krav til informasjon om og innsikt i hvem som er ansvarlig for hvilke opplysninger. Her kan det være nødvendig med konsesjon fra Datatilsynet, og det stilles ekstra strenge krav til de behandlingsansvarlige om å forsikre seg om at eventuelle databehandlere i skyen ivaretar informasjonssikkerheten på en god måte.
- **Informasjonssikkerhet:** I følge personopplysningsloven og forskriften skal den behandlingsansvarlige sørge for tilfredsstillende sikring av persondata. Arbeidet med informasjonssikkerhet skal skje med utgangspunkt i risikoanalyser, hvor lokale sikringstiltak baseres på vurderinger av sannsynligheten for og konsekvensene (for den registrertes personvern) av ulike typer sikkerhetsbrudd. Slike analyser kan bli vanskelige å gjennomføre hvis forhold som har betydning for informasjonssikkerheten skjules i skyen. I lite ”gjennomsiktige” skyer vil den behandlingsansvarlige trolig mangle informasjon som gjør det (a) mulig å vurdere risikoen for at den registrertes personvern krenkes og (b) iverksette målrettede sikringstiltak som reduserer denne risikoen.

Denne skissemessige fremstillingen av noen av de viktigste personvernutfordringer som ”Cloud Computing” reiser, viser to ting:

For det første at prinsippet som ”Cloud Computing” hviler på – persondata kan behandles av hvem som helst, hvor som helst og når som helst uten at den registrerte (og kanskje heller ikke de behandlingsansvarlige) trenger å vite noe om disse forholdene – ikke harmonerer godt med forutsetningene som ligger til grunn for norsk og europeisk lovgivning på personvernområdet. Her er utgangspunktet at vi som registrerte skal utøve en viss råderett (kontroll og medinnflytelse) både over hvordan andre behandler våre persondata, hvilke persondata de behandler og hva de bruker opplysningene til. Dernest forutsetter dagens lovgivning at den behandlingsansvarlige har god kontroll med hvordan andre aktører (databehandlere) gjør bruk av de persondataene som han velger å sette ut for videre behandling (for eksempel lagring). Hvis det er slik at persondata formidles mellom mange aktører i skyen og formidlingen skjer på måter som det er vanskelig å holde oversikt over, kan dette skape utfordringer i forhold den behandlingsansvarliges kontroll med hvordan databehandlere håndterer personopplysninger. Til slutt forutsettes det at opplysningene ikke overføres og behandles hvor som helst i verden, men at overføringen bare skjer til land som gir den samme beskyttelse mot personvernkrenkelser som det Norge og EU garanterer. Dermed kan territorialitet - hvor virksomheter som behandler våre persondata befinner seg - legge visse begrensninger på bruken av tjenester i skyen.

I tillegg kan ”Cloud Computing” komme i konflikt med dagens norske og europeiske personvernlovgivning hvis aktørene i skyen benytter persondata som en handelsvare eller som et ”betalingsmiddel”: noe man kan velge å gi fra seg kontrollen over - uten den registrertes vitende og vilje - for å oppnå visse forretningsmessige fordeler eller motytelser. Denne frie og markedsstyrte flyten av persondata kan bl.a. være i strid med forutsetningen om at den registrerte skal sikres en viss råderett over egne opplysninger.

For det andre viser fremstillingen at de utfordringene som er skissert ovenfor ikke er like viktige eller aktuelle i forhold til alle typer skyformasjoner. Hvilke distribusjonsmodeller som velges – privat sky, delt sky, offentlig sky, osv. – har derfor betydning for (a) hvor tungt utfordringene gjør seg gjeldende og (b) hvordan utfordringene kan løses. Det er disse spørsmålene vi nå vil rette oppmerksomheten mot.



Vurderingskriterier knyttet til noen mulige bruksscenarier

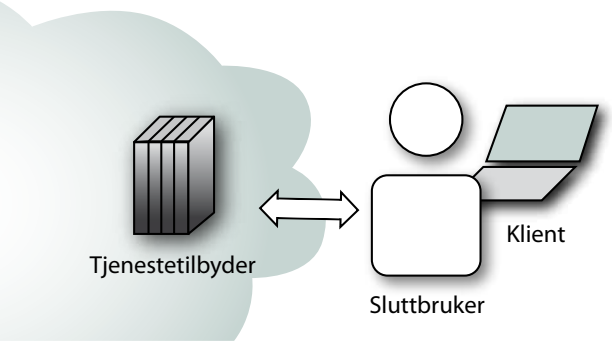
1. Sluttbruker til sky	Applikasjoner som kjører i skyen og aksesseres av sluttbrukere
2. Virksomhet til sky til sluttbruker	Applikasjoner som kjører allment tilgjengelig i skyen, og aksesseres av sluttbrukere
3. Virksomhet til sky	Applikasjoner i skyen som er integrert med interne IT-tjenester
4. Virksomhet til sky til virksomhet	Applikasjoner som kjører allment tilgjengelig i skyen, og som samhandler med samarbeidspartnere
5. Privat sky	En sky som driftes av en virksomhet, innenfor virksomhetens egen brannmur
6. Virtuell privat sky	En sky som er dedikert til en virksomhet, men driftes eksternt av en tjenestetilbyder over en kryptert nettforbindelse
7. Endre sky-tilbyder	En virksomhet som benytter tjenester i skyen bestemmer seg for å skifte tilbyder, eller benytte flere tilbydere
8. Hybrid-sky	Multiple skyer samkjøres, ved hjelp av en samordningstjeneste (eng.: broker) som sammenstiller data, applikasjoner, brukeridentitet, sikkerhet og andre detaljer

Standarder og rammeverk bidrar til å regulere og trygge forholdet mellom tjenestetilbyder og virksomheter, spesielt vedrørende internkontroll og sikkerhet. På dette området foreligger det ingen offentlig tilgjengelig standarder som spesifikt berører Cloud Computing når dette skrives. I vurderingskriteriene nedenfor har vi derfor valgt en mer prinsipiell tilnærming som eventuelt kan knyttes til sektorens og de enkelte virksomhetens egne behov og kontrollrammer.

De fleste av scenariene nedenfor er hentet fra "Cloud Computing Use Case White Paper Version 2"[21], kollektivt utarbeidet av "the Cloud Computing Use Cases Discussion Group"[22] og utdypet med juridiske vurderinger knyttet til mulig bruk i grunnopplæringen. Utvalget er ikke ment å være komplett, men et utgangspunkt for å vurdere anvendbarhet for sektoren.

Scenario 1: Sluttbruker til sky

I dette scenariet aksesserer en sluttbruker data eller applikasjoner i skyen – typisk nettsteder for sosiale nettverk eller epost. Brukere av Gmail, Facebook eller LinkedIn aksesserer applikasjonen og tilhørende data via hvilken som helst nettleser på hvilken som helst mobil eller stasjonær enhet. Brukerne ønsker ikke å ta vare på noe annet enn et passord, og resten av brukernes data lagres og forvaltes i skyen. Brukerne aner lite eller ingenting om den underliggende arkitekturens virkemåte. Hvis de har tilgang til Internett, har de tilgang til dataene.



Roller og ansvar

- **Den registrerte:** Sluttbrukeren (vedkommende person som opplysningene gjelder).
- **Behandlingsansvarlig:** Tjenestetilbyderen (for eksempel Facebook). Her vil det vanligvis være nødvendig med samtykke fra sluttbrukeren for at tjenestetilbyderen skal ha lov til å behandle persondata. Før samtykke gis, er det viktig at sluttbrukeren å sjekker tjenestetilbyderens personvern-policy (spesielt hvis tjenestetilbyderen befinner seg utenfor EU/EØS-området). I personvern-policyen skal sluttbrukeren kunne finne informasjon om hvordan tjenestetilbyderen håndterer persondata, for eksempel om opplysningene videreformidles til andre aktører, hvilke rettigheter sluttbrukeren har og hvordan de ivaretas.
- **Databehandler:** Kun aktuelt hvis tjenestetilbyderen benytter seg av andre aktører i skyen (og hvis det overføres persondata fra tjenestetilbyderen til disse aktørene). Da plikter tjenestetilbyderen å inngå

skriftlig avtale med sine "underleverandører" om hvordan de skal håndtere persondata (se beskrivelse av databehandleravtaler ovenfor).

Krav til tilbyder

- **Identitet:** Sky-tjenesten må autentisere brukeren
- **Åpen klient:** Tilgang til sky-tjenesten må ikke kreve en bestemt plattform eller teknologi
- **Sikkerhet:** Sikkerhet (inkludert personvern) er et gjennomgående krav i alle bruksscenariene, selv om de detaljerte kravene kan variere mye fra det ene scenariet til det neste
- **SLA (Service Level Agreement):** Selv om tjeneste-avtalene for sluttbrukere normalt er langt enklere enn for virksomheter, må sky-tilbydere være tydelige med hensyn til hvilke tjenestegarantier de gir

Scenario 2: Virksomhet til sky til sluttbruker

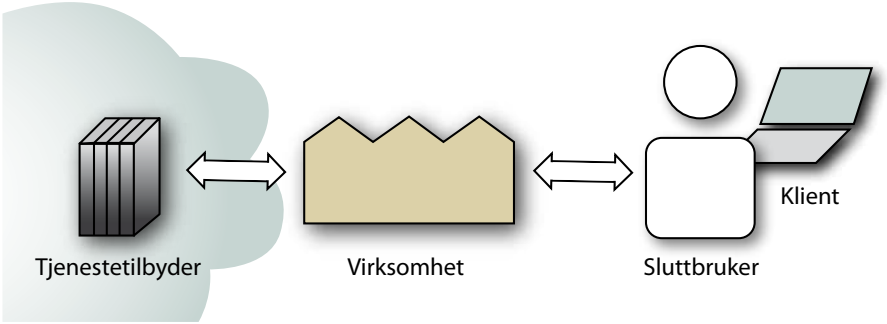
I dette scenariet benytter en virksomhet skyen til å levere data og tjenester til sluttbrukeren. Brukerens interaksjon med virksomheten resulterer i at virksomheten henter og/eller manipulerer data, som så oversendes til slutt-brukeren. Sluttbrukeren kan være noen i virksomheten eller en ekstern.

Roller og ansvar

- Den registrerte: Sluttbrukeren (vedkommende person som opplysningene gjelder).
- Behandlingsansvarlig: Virksomheten. Også her vil samtykke vanligvis være grunnlaget for virksomhetens lovlige bruk av opplysningene. Derfor er det viktig for sluttbrukeren å sjekke virksomhetens personvern-policyen før samtykke gis (se også merknader under scenario 1).
- Databehandler: Ingen (så lenge tjenestetilbyderne i skyen kun er passive kanaler for overføring av data til og fra den registrerte).

Krav til tilbyder

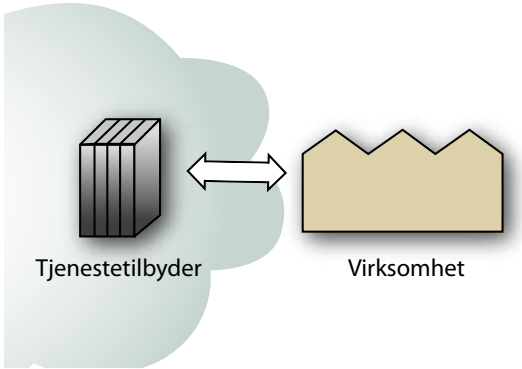
- **Identitet:** Sky-tjenesten må autentisere brukeren
- **Åpen klient:** Tilgang til sky-tjenesten må ikke kreve en bestemt plattform eller teknologi
- **Felles identitet:** I tillegg til enhver sluttbrukers grunnleggende identitetsbehov har en bruker i en virksomhet trolig en egen virksomhetsspesifikk identitet. Ideellt sett burde virksomhetsbrukeren bare behøve å forholde seg til én identitet, bygget på en infrastruktur som samlet håndterer andre identiteter som kreves av tjenester i skyen.
- **Lokaliseringskontroll:** Juridiske forhold kan legge avgjørende føringer på tjenestens faktiske lokasjon, avhengig av hva slags data virksomheten håndterer på brukerens vegne. Dette er helt sentralt, selv om det bryter med idealforestillingen om at skyen skal skjule detaljene rundt fysisk infrastruktur. Mange applikasjoner kan ikke flyttes til skyen før sky-leverandørene tilbyr et programmeringsgrensesnitt som gjør det mulig å fastslå lokasjonen til den fysiske maskinvaren som leverer en gitt sky-tjeneste.
- **Forbruksmåling og overvåking:** Alle sky-tjenester må overvåkes og ressursbruken må måles med henblikk på kostnadskontroll, tilbakeføring av kjøp, og allokering av tjenesteressurser.
- **Administrasjon og overoppsyn:** Tilbydere av offentlige skyer gjør det veldig enkelt å opprette en konto og ta i bruk tjenester i skyen, og den lave terskelen øker risikoen for at noen i virksomheten tar i bruk tjenester i skyen på eget initiativ. Virtuelle maskiner og tjenester som lagring, databaser og meldingskøer i skyen må administreres for å kunne følge med på hvilke tjenester som er i bruk. For å sikre overholdelse av policy og offentlig regelverk er det av avgjørende betydning å holde overoppsyn med bruken av tjenester i skyen. Eventuelle geografiske og sektorspesifikke krav til overoppsyn kan komme i tillegg.
- **Sikkerhet:** Virksomhetsbasert bruk vil nødvendigvis stille mer avanserte sikkerhetskrav enn individuell bruk. Tilsvarende vil de mer avanserte påfølgende virksomhetsscenariene stille ennå mer avanserte sikkerhetskrav.



- **Sammenstilling av data og applikasjoner:** Virksomhetsapplikasjoner vil trolig ha behov for å sammenstille data fra flere skybaserte tjenester, og koordinere applikasjoner som kjører i ulike skyer.
- **SLA og målemetoder:** En avtale om tjenestegaranti (eng.: SLA - "Service Level Agreement") er bindeleddet som regulerer forholdet mellom tjenestetilbyder og virksomhet, og et av de mest effektive verktøyene virksomheten har for å sikre informasjon i skyen. En SLA kan spesifisere et eventuelt felles kontrollrammeverk og forventningene knyttet til en tredjepartsrevisjon. En grundig og omfattende avtale som gir rett til en like grundig og omfattende tjenesterevisjon vil bidra til å sikre at virksomhetens forventninger til håndtering, bruk, oppbevaring og tilgjengelighet av informasjon blir ivaretatt. Virksomheter som inngår avtaler basert på SLAer som går ut over de grunnleggende sluttbrukerkravene, vil ha behov for en standardisert målemetode. Det må finnes en entydig måte å definere hva en tjenestetilbyder skal levere, og en entydig målemetode for hva som faktisk ble levert.
- **Håndtering av livssyklus:** Virksomheter må kunne gjøres i stand til å håndtere applikasjoners og dokumenters livssyklus, inkludert versjonering av applikasjoner og ivaretakelse og destruksjon av data. (Gjen)finnbarhet er sentralt for mange virksomheter, ettersom det kan ha store juridiske konsekvenser dersom visse data ikke lenger er tilgjengelige. Tilbyders kontinuitet og planer for katastrofegjenoppretting må være godt dokumentert og testet. Den dynamiske arkitekturen i mange av tjenestetilbudene kan medføre forsinkelser når informasjon skal gjenopprettes. Mål for gjenopprettingstid bør være angitt i kontrakten.

Scenario 3: Virksomhet til sky

I dette scenariet innlemmer virksomheten tjenester i skyen i interne prosesser. Dette gir virksomheten mest kontroll, og vil derfor trolig være det vanligste bruksscenariet i tidlige faser.



I scenariet bruker virksomheten ulike sky-baserte tjenester som supplement til ressurser den trenger:

- Lagring i skyen for backup, eller lagring av data som ikke brukes ofte
- Virtuelle maskiner i skyen som tilbyr ekstra prosessorkraft til håndtering av lasttopper (og kan stenges ned når det ikke lenger er behov for ekstra kapasitet)
- Applikasjoner i skyen (SaaS) for enkelte funksjonelle områder (epost, kalender, CRM, m.v.) i virksomheten
- Databaser i skyen som en del av applikasjonsprosesseringen. Kanskje spesielt nyttig med hensyn til muligheten for å dele databasen med samarbeidspartnere, offentlige etater, osv.

Roller og ansvar

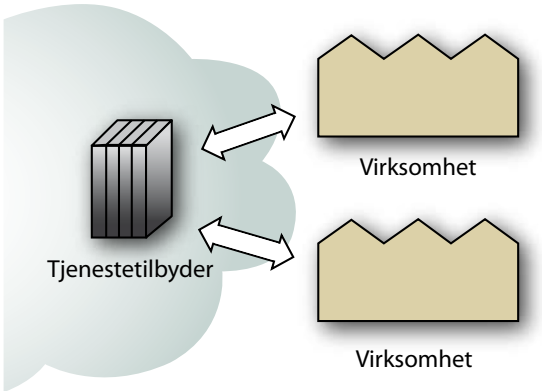
- **Den registrerte:** Sluttbrukeren (vedkommende person som opplysningene gjelder).
- **Behandlingsansvarlig:** Virksomheten. De samme merknadene gjelder i forhold til dette scenariet som i forhold til scenario 1 og 2.
- **Databehandler:** De tjenestetilbyderne i skyen (for eksempel aktører som leverer lagring/back-up, epost, kalender, osv.) som virksomheten benytter seg av. Prinsippet er igjen at det er nødvendig å inngå en databehandleravtale med disse aktørene før persondata overføres til dem (fra den behandlingsansvarlige) for videre behandling.

Krav til tilbyder

De grunnleggende kravene for scenariet er de samme som for "Virksomhet til sky til sluttbruker" over, med følgende tillegg:

- **Industri-spesifikke standarder og protokoller:** Mange sky-baserte løsninger mellom virksomheter vil benytte eksisterende standarder, avhengig av anvendelsesområde og sektor.

Scenario 4: Virksomhet til sky til virksomhet



Dette scenariet tar utgangspunkt i at to virksomheter bruker samme sky, og fokuserer på deling av ressurser slik at virksomhetenes applikasjoner kan samhandle.

Roller og ansvar

- **Den registrerte:** Sluttbrukeren (vedkommende person som opplysningene gjelder).
- **Behandlingsansvarlig:** Virksomhetene er ansvarlige for "sine" persondata: de opplysningene som hver av de to virksomhetene har skaffet seg lov til å behandle (vanligvis basert på samtykke fra den registrerte). Dermed vil virksomhetene også ha litt ulike formål med behandlingen av persondata og de bestemmer selv hvilke elektroniske hjelpemidler som skal benyttes (det er dette som er definisjonen på en behandlingsansvarlig).
- **Databehandler:** Virksomhetene er databehandlere for hverandre: de benytter persondata som den andre virksomheten har skaffet seg råderett over (les: lov til å bruke). De må derfor ha databehandleravtaler med hverandre for at de skal kunne utveksle persondata seg i mellom. Om de også trenger databehandler-avtaler med tjenestetilbydere i skyen, avhengiger av hva aktørene i skyen gjør med opplysningene (ikke nødvendig hvis de bare benyttes som passive overføringskanaler).

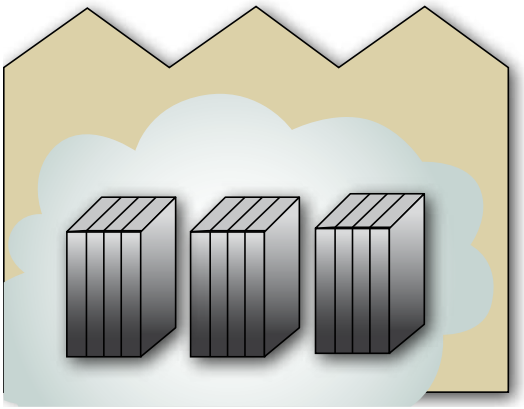
Krav til tilbyder

De grunnleggende kravene for scenariet er de samme som for "Virksomhet til sky" over, med følgende tillegg:

- **Transaksjoner og samtidighet:** Håndtering av transaksjoner og samtidighet er avgjørende for applikasjoner og data som deles av flere virksomheter. Hvis to eller flere virksomheter benytter samme applikasjon, virtuelle maskin, mellomvare eller datalager i skyen er det viktig at endringene ivaretas på en trygg måte
- **Interoperabilitet:** Interoperabilitet er en avgjørende forutsetning når mer enn én virksomhet er involvert

Scenario 5: Privat sky

Bruksscenariet for private skyer skiller seg fra de andre, ettersom skyen helt og holdent forvaltes og brukes internt i virksomheten selv. Dette kan gi verdi for store virksomheter. Hvis for eksempel lønnskjøringer medfører lasttopper én eller to dager i måneden, må maskinvare-kapasiteten dimensjoneres for den største belastningen, selv om det daglige kapasitetsbehovet er langt lavere. Med en privat sky kan den overskytende kapasiteten deles med resten av virksomheten. Lønningskontoret får nødvendig kapasitet når de trenger det, og andre avdelinger får ekstra kapasitet når det trenger det. Dette kan innebære betydelige kostnadsbesparelser for virksomheten som helhet. Samtidig er det viktig å påpeke at private skyer fortsatt må kjøpes, bygges og driftes av virksomheten selv. Det betyr at virksomheten ikke realiserer det kanskje viktigste økonomiske potensialet ved "Cloud Computing"-modellen, som er de lavere initielle kapitalkostnadene og den reduserte administrative ressursbruken.



Roller og ansvar

- **Den registrerte:** Sluttbrukeren (vedkommende person som opplysningene gjelder).
- **Behandlingsansvarlig:** Virksomheten som har skaffet seg råderett over opplysningene (vanligvis basert på samtykke fra den registrerte). Så lenge virksomheten befinner seg innenfor EU/EØS-området, gjelder reglene for behandling av opplysningene som er skissert ovenfor. Det kan imidlertid oppstå problemer i forhold til virksomheter i land utenfor Europa: Google hevder for eksempel at selskapet ikke er underlagt norsk og europeisk personvernlovgivning fordi det har sitt hovedkontor i USA. Dermed blir det også her viktig for sluttbrukeren å sjekke (a) hvor virksomheten har sitt hovedkontor og (b) vilkårene for bruken av tjenesten (personvern-policy).
- **Databehandler:** Ingen (virksomheten har full og uavkortet kontroll over de persondata som den har skaffet seg lov til å behandle).

Krav til tilbyder

De grunnleggende kravene i bruksscenariet for private skyer er en **åpen klient, forbruksmåling og overvåking, administrasjon og overoppsyn, sikkerhet, interoperabilitet** og **SLAer**, som beskrevet over.

En privat sky forutsetter ikke at eksterne tilbydere er involvert i håndteringen av identitet, transaksjoner, industristandarder eller håndtering av livssyklus, og – kanskje viktigst av alt – lokaliseringen av data. Sistnevnte kan være avgjørende for enkelte virksomheter.

Scenario 6: Virtuelt privat sky

Såkalte ”virtuelt private” skyer er enkelte tjenestetilbyderes tilbud til virksomheter som ønsker en grad av kontroll som i prinsippet skal ligge nærmere scenariet ”Privat sky” (scenario 5, over), men med flere av fordelene fra scenariet ”Virksomhet til sky” (scenario 3, over), som lavere initiell kapitalkostnad og redusert administrativ ressursbruk. En kryptert VPN-basert nettverksbro gjør tilbyderens ressurser tilgjengelig over virksomhetens egne subnett og brannmur- og administrasjonsregimer. Omvendt kan virksomhetens datakilder også gjøres tilgjengelige for ressurser i skyen, og dette kan i prinsippet gi bedre lokaliseringskontroll over dataene. I praksis avhenger dette av hvordan tjenesten håndterer data.

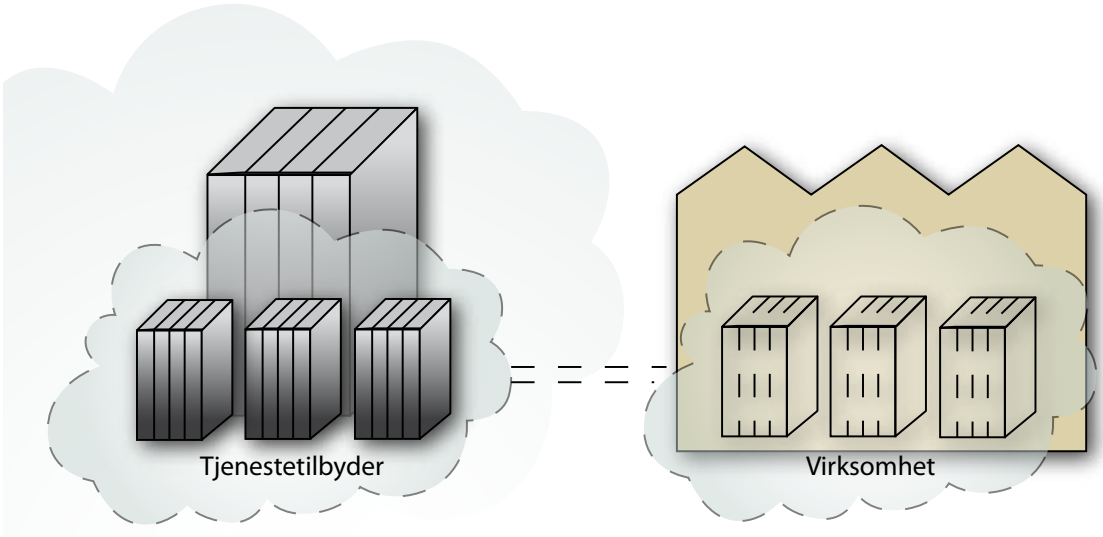
Roller og ansvar

- **Den registrerte:** Sluttbrukeren (vedkommende person som opplysningene gjelder).
- **Behandlingsansvarlig:** Virksomheten som har skaffet seg lov til å behandle persondata, og som i tillegg bestemmer hensikten/formålet med bruken av opplysningene, samt hvilke elektroniske hjelpemidler som skal benyttes.
- **Databehandler:** Den eller de tjenestetilbyderne i skyen som virksomheten velger å benytte seg av (og som forvalter persondata på vegne av virksomheten).

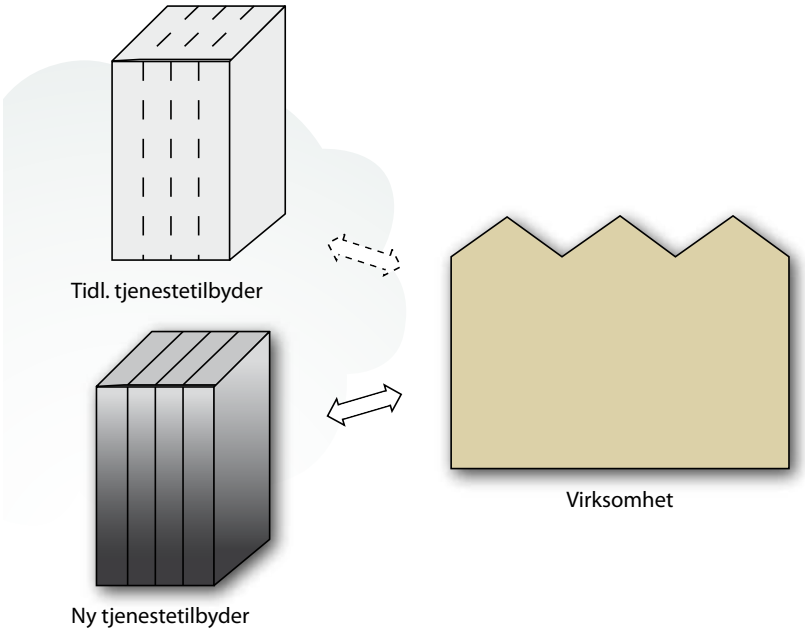
Krav til tilbyder

De grunnleggende kravene for scenariet er de samme som for ”Virksomhet til sky” over, med følgende tillegg:

- **Kryptert nettverksbro (VPN):** Tjenester i skyen som gjøres tilgjengelige over en kryptert nettverksbro kan fungere som om de sitter direkte på det datanettet som broen er koplet til, og tildeles ip-adresser fra dette datanettet. Tjenestene har adgang til alle de tjenester som finnes på det datanettet de er koblet til, og omvendt. Noen velger å styre adgangen ved å knytte broen i en DMZ (sikret sone) i brannmuren.



Scenario 7:
Bytte sky-tilbyder



Dette brukstilfellet handler om å ta i bruk en annen sky-tilbyder, enten i tillegg til, eller i stedet for en eksisterende, noe som kan være relevant for alle de omtalte brukstilfellene i denne veilederen. Den største fordelen med åpenhet og standardisering er muligheten til å ta i bruk andre tilbydere uten store endringer.

Brukstilfellet omfatter fire scenarier som hver leder til litt ulike krav. Generelt vil et bytte av sky-tilbyder forutsette **åpen klient, lokaliseringskontroll, sikkerhet, SLAer,** et **felles filformat for virtuelle maskiner** og **felles programmeringsgrensesnitt for lagring og mellomvare.** Detaljene diskuteres i avsnittene nedenfor.

Scenario 7a:
Bytte SaaS-leverandører

Antar her at tjenestebruker bytter fra en sky-leverandør til en annen, der begge tilbyr tilnærmet samme applikasjon (f.eks. LMS, regnskap, tekstbehandler). Data og dokumenter opprettet med den ene applikasjonen bør da kunne importeres av den andre leverandørens programvare. I noen tilfeller kan det også være aktuelt for tjenestebrukeren å benytte leverandørene om hverandre.

Roller og ansvar

- **Den registrerte:** Sluttbrukeren (vedkommende person som opplysningene gjelder).
- Behandlingsansvarlig: Virksomheten som har skaffet seg lov til å behandle persondata, og som i tillegg (a) bestemmer hensikten/formålet med bruken av opplysningene og (b) hvilke elektroniske hjelpemidler som skal benyttes.
- **Databehandler:** De to tjenestetilbyderne i skyen (tidligere og ny). Virksomheten trenger databehandleravtaler med dem begge - begge behandler persondata etter oppdrag fra den som har skaffet seg lov til å bruke opplysningene. Når opplysningene overføres fra den tidligere til den nye tjenestetilbyderen, er det viktig at virksomheten forsikrer seg om at den tidligere tjenestetilbyderen sletter alle persondataene fra sine systemer.

Krav til tilbyder

- **Industrispesifikke standarder:** Flytting av data og dokumenter fra én leverandørs applikasjon til en annen avhenger av at begge applikasjonene støtter samme format. Formatet avhenger som regel av type applikasjon.

I noen tilfeller kan det også være påkrevet med standard programmeringsgrensesnitt for ulike typer applikasjoner.

Det er ikke noe ved dette kravet som er spesielt for applikasjoner i skyen. Standardene som muliggjør flytting av et dokument fra *Zoho* til *Google Docs* er de samme standardene som muliggjør flytting av et dokument fra *Microsoft Office* til *OpenOffice*.

Scenario 7b: Bytte mellomvare-leverandører[23]

I dette scenariet bytter tjenestebruker leverandør av mellomvare i skyen. Eksisterende data, spørringer, meldingskøer og applikasjoner må kunne eksporteres fra én leverandør og importeres hos en annen.

Roller og ansvar

- **Den registrerte:** Sluttbrukeren (vedkommende person som opplysningene gjelder).
- **Behandlingsansvarlig:** Samme som i scenario 7a.
- **Databehandler:** Samme som i scenario 7a.

Krav til tilbyder

- **Industrispesifikke standarder:** Som for bytte av SaaS-leverandører, over
- **Felles programmeringsgrensesnitt for mellomvare i skyen:** Dette omfatter alle funksjoner som støttes av dagens mellomvare i skyen, inkludert meldingskøer og databaser, eksempelvis connect, create og drop av databaser og tabeller.

Leverandører av databaser i skyen legger visse restriksjoner på tjenestene for å sikre skalerbarhet og fleksibilitet (”elastistitet”), og begrense mulighetene for svært ressurskrevende spørringer mot store datasett. Noen databaser i skyen støtter eksempelvis ikke join over flere tabeller, og andre støtter ikke reelle databaseskjemaer. Ved bytte av databaseleverandør i skyen er disse restriksjonene en stor utfordring, spesielt for applikasjoner som forutsetter en reellt relasjonell modell.

Meldingskøer og andre mellomvaretjenester likner hverandre mer, og det burde i prinsippet være enklere å finne fellesnevnere mellom dem.

Scenario 7c: Bytte leverandør for lagring i skyen

Scenariet dreier seg om tjenestebrukers bytte av lagringsleverandør i skyen. Hyppige korte og lange forsinkelser (eng.: ”latency”) i nettverket er svært vanlig, og en viktig årsak til at data i databaser og annen tilstandsinformasjon gjerne lagres nettverksmessig ”nært” kjørende tjenester, foruten eventuelle vurderinger rundt nettverkskostnader.[24] Det er derfor grunn til å anta at dette scenariet er mest relevant for lagring av data som ikke representerer løpende applikasjonstilstand. I praksis representerer dette en form for binding (eng.: ”lock in”) til tjenestetilbyder som har hatt lite fokus så langt.

Roller og ansvar

- **Den registrerte:** Sluttbrukeren (vedkommende person som opplysningene gjelder).
- **Behandlingsansvarlig:** Samme som i scenario 7a.
- **Databehandler:** Samme som i scenario 7a.

Krav til tilbyder

- **Et felles programmeringsgrensesnitt for lagring i skyen:** Kode som leser og skriver data i et lagringssystem i skyen bør fungere for et annet med så få endringer som mulig, og endringene bør være begrenset til konfigurasjonskode. Eksempelvis er URL-formatet og drivernavnet forskjellig for ulike databaseleverandørers JDBC-applikasjoner, mens koden som interagerer med databasen er den samme.

Virksomheter som inngår en avtale med en ny tilbyder av lagringstjenester, bør foreta en ”vareopptelling” av de aktuelle data- og informasjonskategoriene, for å sikre at de er riktig klassifisert og merket. Dette vil bidra til å avgjøre hva som bør spesifiseres i en tjenestegaranti-avtale (SLA), eventuelle krypteringsbehov knyttet til informasjonen som overføres eller lagres, og eventuelle ytterligere føringer for informasjon som er sensitiv eller av høy verdi for virksomheten.

Scenario 7d: Bytte tjenestetilbyder for virtuelle maskiner

Tjenestebruker ønsker i dette scenariet å kjøre en virtuell maskin bygget på én leverandørs system på en annen leverandørs system i skyen.

Roller og ansvar

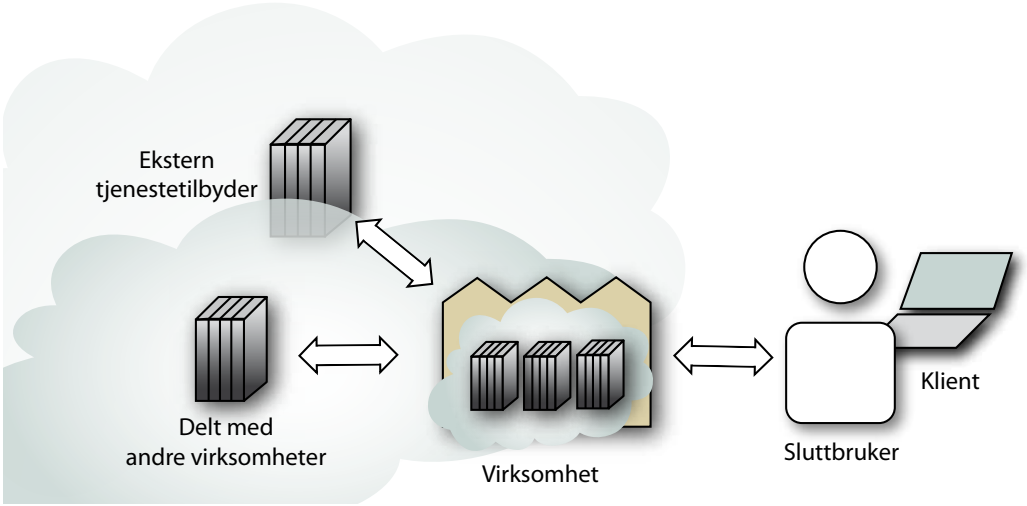
- **Den registrerte:** Sluttbrukeren (vedkommende person som opplysningene gjelder).
- **Behandlingsansvarlig:** Samme som i scenario 7a.
- **Databehandler:** Samme som i scenario 7a.

Krav til tilbyder

- **Felles format for virtuelle maskiner:** VM-formatet bør fungere på tvers av operativsystem

Kravet forutsetter at de virtuelle maskinene selv kjører et operativsystem som Windows eller Linux. Brukeren av den virtuelle maskinen har med andre ord valgt plattform før den virtuelle maskinen bygges for skyen, slik at det ikke foreligger spesielle sky-relaterte krav for programvaren som kjører i den virtuelle maskinen.

Scenario 8: Hybrid-sky



Bruksscenariet kjennetegnes ved at flere skyer, både private og offentlige, brukes sammen på en slik måte at de framstår som én sky. Tilbydere av hybridsky-tjenester kan kombinere egne ressurser med andre tilbyderes, eller tilby en tjeneste som bare er sammensatt av andre tilbyderes tjenester.

For en sluttbruker vil dette scenariet framstå som identisk med ”sluttbruker til sky”, ettersom sluttbrukeren ikke ser hvordan tilbyderen har bygget opp sin tjeneste.

Roller og ansvar

- **Den registrerte:** Sluttbrukeren (vedkommende person som opplysningene gjelder).
- **Behandlingsansvarlig:** Virksomheten som har skaffet seg lov til å behandle persondata, og som i tillegg bestemmer (a) hensikten/formålet med bruken av opplysningene og (b) hvilke elektroniske hjelpemidler som skal benyttes.
- **Databehandler:** For det første vil alle eksterne tjenestetilbydere (se figuren ovenfor) være data-behandlere for virksomheten. Men virksomheten vil også selv være databehandler for opplysninger som hentes inn fra andre virksomheter og som så benyttes i egne forretningsprosesser. Her vil det derfor være nødvendig med en rekke databehandler-avtaler for å sikre sluttbrukeren mot misbruk av opplysninger som gjelder han eller hun.

Krav til tilbyder

Alle kravene for foregående bruksscenarier gjelder også her, spesielt sikkerhet, sammenstilling av data og applikasjoner og interoperabilitet.

- **Maskinlesbare SLAer:** Et standardisert, maskinles-bart format for SLAer gjør det mulig for tilbydere av hybride skyer å velge ressurser basert på kundens vilkår uten å involvere mennesker

Kravene til delte skyer er et subsett av kravene til hybrid-skyer. En delt sky deles mellom virksomheter med felles hensikter.

Skiftende skydekke...?

De siste 40 årene har vi sett "Moores lov" holde stand – prosessorkraften dobles fortsatt omkring hver 18. måned, og derved har også prisen på datakraft falt svært bratt og ulineært i fire tiår. Det samme har også langt på vei vært tilfellet for prisen på lagring. Båndbredde-kostnadene har derimot bare falt lineært, og dette ser ikke ut til å endre seg med det første.

Mange mobiler har i dag mer lagringsplass og datakraft enn en fullverdig desktop-PC for et tiår siden, og ytelsen øker raskere enn den gjør for PCer - bare begrenset av batterikapasitet. Historien om databehandling kan i store trekk sies å ha vært preget av overføring av kapasitets-vekst fra tunge, sentrale aktører til befolkningen generelt, og mye tyder på at denne trenden fortsetter:

- **Servere:** 7,3 millioner enheter globalt i 2009, **ned** 19,5% fra 2008[25]
- **PCer:** 291,4 millioner enheter (i hovedsak bærbare) globalt i 2009, opp 10,5% fra 2008[26]
- **Smarttelefoner:** 170,0 millioner enheter globalt i 2009, opp 23,6% fra 2008[27]

Vi er inne i en periode der vi kan anta at en betydelig andel av de 7,3 millioner serverforsendelsene vil gå til å bygge og skalere opp tjenester i skyen, men slett ikke alle. Det er verdt å merke seg at veksten i datakraft fortsatt er langt større *utenfor* skyen - på "klientsiden". Det betyr ikke bare at mengden data og tilgjengelig prosessorkraft i dag er langt mindre i skyen enn på klientsiden, men at forskjellen stadig *øker*.

Hvis det skal lønne seg å prosessere i skyen, må kostnadsbesparelsen ved å flytte prosesseringen være større enn kostnaden ved å flytte dataene[28]. I praksis viser det seg at de fleste typiske virksomhetsrelaterte prosesseringsoppgaver er *dataintensive*, og både henter inn og leverer ut mye data, slik at prosesseringen bør skje nettverksmessig "nær" dataene.

Selv om prosessering i skyen får mye oppmerksomhet i dag, er det derfor rimelig grunn til å tro at mye prosessering vil fortsette å desentraliseres – og trolig i økende grad mot mobile enheter i hendene på sluttbrukerne. Det stadig økende antallet webapplikasjoner med såkalte "rike" grensesnitt (eng.: "*Rich Internet Applications*" – *RIA*) i *AJAX* (JavaScript), *Flash/AIR* og *Silverlight* er ett tegn på dette, foruten lette, dynamiske distribusjons-modeller som *ClickOnce*, *Java Web Start* og *Zero Install*.

De enkle ovennevnte økonomiske og tekniske betrakt-ningene[29] gir selvsagt ikke et fullverdig bilde. Mengder av billig maskinvare er ikke nødvendigvis verken kosteffektivt eller miljøvennlig, og disse faktorene, sammen med en rekke nye forretningsmuligheter for tilbyderne, vil drive utviklingen mot tjenester i skyene i mange år framover.

Økende prosesseringskraft i hendene på sluttbrukeren (eleven, læreren eller begge) kan også tenkes å ha konsekvenser for spørsmål knyttet til personvern og informasjonssikkerhet. Hvis trenden med desentralisering av prosessorkraft fortsetter, er det for eksempel mulig at elevenes og lærernes råderett over egne persondata styrkes - og at skoleeier kan legge til rette for denne råderetten. Isteden for at store mengder persondata overlates til virksomheter eller tjenestetilbydere i skyen, kan det altså tenkes at (a) skoleeier kan sette den eller de som opplysningene gjelder i stand til å utøve kontroll over egne persondata, slik at (b) kommersielle (og internasjonale) aktørers rolle som viktige opplysnings-forvaltere svekkes.

I et slikt scenario slipper den behandlingsansvarlige (skoleeiere) å feste like stor lit til at aktører i skyen vet å håndtere persondata på en skikkelig måte. Dette er i så fall en utvikling som i større grad harmonerer med prinsippene i norsk og europeisk personvernlovgivning – den behandlingsansvarlige (skoleeier) skal opptre på måter som ivaretar den registrertes (eleven, læreren, osv.) råderett over egne persondata – enn hva flere av scenariene som er diskutert ovenfor legger opp til.

Men når den behandlingsansvarlige (skoleeieren) får større muligheter til å ivareta den registrertes (eleven, læreren, osv.) personvernrettigheter, innebærer dette samtidig at skoleeieren plikter å vurdere informasjons-sikkerheten ved de løsningene som velges. Den behandlingsansvarlige (skoleeier) bør for eksempel sørge for tilfredsstillende sikring av lokale og mobile enheter mot bl.a. "tapping" av persondata og mot at enhetene mistes eller ødelegges. Før denne typen løsninger tas i bruk, blir det derfor viktig for skoleeier å (1) vurdere risikoen for konfidensialitets-, integritets- og tilgjengelighetsbrudd og (2) hvis risikoen for sikkerhets-brudd vurderes å være uakseptabel, enten (a) avstå fra å ta løsningene i bruk eller (b) iverksette tekniske, organisatoriske eller andre typer tiltak som redusere sjansen for og de personvernmessige virkningene av mulige sikkerhetsbrudd.

Økt lokal kontroll over persondata fritar derfor ikke skoleeieren fra sine rettslige plikter, spesielt (men ikke begrenset til) hensynet til informasjonssikkerheten: pliktene er de samme, men forutsetningene for å ivareta dem kan sies å være styrket når kontrollen over person-data tilbakeføres til de som i utgangspunktet har det rettslige ansvaret for håndteringen av opplysningene.

Sluttnoter

[1] Rohit Khare: ”Privacy Theater: Why Social Networks Only Pretend To Protect You”, http://www.techcrunch.com/2009/12/27/privacy-theater/

[2] Jim Gray: ”Distributed Computing Economics” (Microsoft Research, 2003), http://research.microsoft.com/apps/pubs/default.aspx?id=70001

[3] Se http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc (2009)

[4] Se http://en.wikipedia.org/wiki/Cloud_computing

[5] Se http://en.wikipedia.org/wiki/Cloud_computing#History

[6] Dette avsnittet, samt definisjonene av DaaS, CaaS og HaaS er hentet fra Youseff et al: ”Toward a Unified Ontology of Cloud Computing” http://www.cs.ucsb.edu/%7Elyouseff/CCOntology/CloudOntology.pdf (2009)

[7] Se http://en.wikipedia.org/wiki/Cloud_computing#Private_cloud

[8] Se http://en.wikipedia.org/wiki/Cloud_computing#Hybrid_cloud

[9] Se http://en.wikipedia.org/wiki/Cloud_computing#Criticism_of_the_term

[10] Lydopptak på http://www.youtube.com/watch?v=0FacYAI6DY0

[11] Se http://en.wikipedia.org/wiki/Edge_computing

[12] Se f.eks. ”Is intimate personal information a toxic asset in cloud datacenters?”, http://radar.oreilly.com/2009/08/is-intimate-personal-informati-1.html, og/eller side 18 og utover i artikkelen ’A historical perspective on developing foundations for privacy-friendly client cloud computing: The Paradigm Shift from ”Inconsistency Denial” to ”Practical Semantic Integration(TM)”’, http://arxiv.org/ftp/arxiv/papers/0901/0901.4934.pdf#page=18

[13] Se http://web.archive.org/web/20071018161644/http://blog.pmarca.com/2007/09/the-three-kinds.html

[14] Med behandling av persondata menes all bruk av opplysningene, for eksempel innsamling, lagring, sammenstilling, offentliggjøring, videreformidling og sletting.

[15] Se www.datatilsynet.no.

[16] På skolenes hjemmesider presenteres informasjon om hva skolen som institusjon holder på med. Det presenteres vanligvis mindre informasjon om hva enkeltpersoner tilknyttet skolen driver med

[17] For videre diskusjon av hvordan persondatabegrepet skal forstås, se www.datatilsynet.no/upload/wp136_da.pdf.

[18] Datatilsynet er adressat både for søknad om konsesjon for behandling av sensitive persondata og meldinger om behandling av alminnelige persondata.

[19] I sitt veiledningsmateriale til kommuner og fylkeskommuner anbefaler Datatilsynet at IT-systemer som behandler sensitive persondata er fysisk atskilt fra Internett

[20] Hvis det samles inn unødvendige persondata (såkalt overskuddsinformasjon), er regelen at disse skal slettes så raskt som mulig.

[21] Se http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-2_0.pdf

[22] Se http://groups.google.com/group/cloud-computing-use-cases

[23] På grunn av populariteten til tjenester som tilbyr lagring i skyen, er det her skilt scenariemessig mellom lagring og mellomvare (databaser, meldingskøer, MapReduce, ...), selv om begge klassifisert som PaaS

[24] Jim Gray, Microsoft: ”Computing economics are changing. Today there is rough price parity between (1) one database access, (2) ten bytes of network traffic, (3) 100,000 instructions, (4) 10 bytes of disk storage, and (5) a megabyte of disk bandwidth. This has implications for how one structures Internet-scale distributed computing: one puts computing as close to the data as possible in order to avoid expensive network traffic.”: http://research.microsoft.com/apps/pubs/default.aspx?id=70001

[25] Estimert på bakgrunn av kvartalstall - se https://www.gartner.com/it/page.jsp?id=905914, https://www.gartner.com/it/page.jsp?id=1000326, https://www.gartner.com/it/page.jsp?id=1161313, https://www.gartner.com/it/page.jsp?id=1238521

[26] http://www.idc.com/getdoc.jsp?pid=23571113&containerId=prUS22140709

[27] https://www.gartner.com/it/page.jsp?id=1256113

[28] Jim Gray: ”Distributed Computing Economics” (Microsoft Research, 2003), http://research.microsoft.com/apps/pubs/default.aspx?id=70001

[29] Basert på Vineet Guptas ”Edge vs. Cloud Computing”: http://vineetgupta.spaces.live.com/blog/cns!8DE4BDC896BEE1AD!1326.entry

Senter for IKT i utdanningen • Postboks 530 • 9256 Tromsø
www.iktsenteret.no • post@iktsenteret.no