Kommunal- og moderniseringsdepartementet

Strategi

Nasjonal strategi for bruk av skytenester

Forord

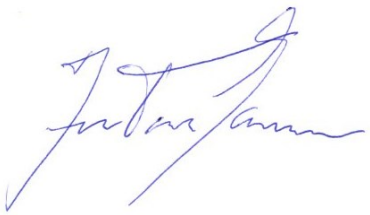
Norske offentlege og private verksemder har i mange år brukt tenesteutsetting for å kunne fokusere på kjerneverksemda si og overlate for eksempel drift av IKT til andre. Dei siste åra har skytenester etablert seg som eit viktig alternativ for tenesteutsetting. Vi ser at stadig fleire tenester, både infrastrukturtenester og programvare, blir leverte som skytenester. Dette gjeld òg tenester retta mot offentleg sektor.

Så kan ein spørje seg kvifor vi treng ein eigen strategi for skytenester? Tenesteutsetting har vi jo drive med lenge? Men skytenester skil seg frå tradisjonell tenesteutsetting på viktige område som vi ser skaper utfordringar for verksemder som vurderer å ta i bruk slike tenester – og kanskje særleg for offentlege verksemder: Ein kan ikkje alltid vite nøyaktig kor informasjonen blir lagra eller behandla til kvar tid, og kontraktane ein bruker er ofte standardkontraktar frå leverandøren. Mange verksemder er usikre på om det å bruke skytenester er trygt nok, og om regelverket tillèt at dei bruker slike tenester.

I åra som kjem må offentleg sektor bli meir kostnadseffektiv. Bruk av IKT og digitalisering av tenester er ein viktig del av dette. Men dei digitale tenestene og dei offentlege IKT-systema skal òg drivast kostnadseffektivt. I *digitaliseringsrundskrivet* for 2016, som gjeld alle verksemder i statleg sektor, har vi derfor tatt inn ei anbefaling om at offentlege verksemder skal vurdere skytenester som eit alternativ når dei skal skaffe IKT-tenester. I denne strategien legg vi fram fleire tiltak som skal gjere det enklare for både offentlege og private verksemder å gjennomføre denne typen vurderingar.

Samtidig er det viktig for oss at offentlege verksemder driv IKT-en sin på ein sikker og forsvarleg måte. Ein sentral del av arbeidet med denne strategien har vore å vurdere regelverket, slik at det er tydeleg kva som er tillate og ikkje. I oppfølginga av strategien vil vi etablere ressursar som kan rettleie offentlege verksemder i viktige vurderingar ein må gjere om ein ønsker å kjøpe inn skytenester: verdivurdering av eigne data, informasjonstryggleik, risikovurderingar og oppfølging av kontraktar. Slike ressursar vil òg kunne ha overføringsverdi for næringslivet.

I løpet av arbeidsperioden har det vore gjennomført fleire samlingar med både statlege verksemder, kommunane og IKT-bransjen. Det har òg blitt etablert ei rådgivande gruppe med representantar frå stat, kommune og viktige aktørar innan personvern og tryggleik. KS har i same periode arbeidd med å sjå på bruk av skytenester i kommunane. Det har vore tett og god dialog med KS i denne prosessen. Eg vil gjerne takke alle dei involverte for viktige bidrag.



Jan Tore Sanner
Kommunal- og moderniseringsminister

Innhald

1 Innleiing og samandrag

Framtidig vekst og velferd i Noreg er avhengig av at produktiviteten held fram med å vekse.[1] Viktige faktorar for vekst er innovasjonsevne og nyetablering. Betre utnytting av teknologi er nødvendig for å møte behova for offentlege tenester i framtida. I privat sektor, og særleg i tenesteytande næringar, treng ein å bli flinkare til å ta i bruk ny teknologi for å sikre vidare produktivitetsvekst.

Innan offentleg sektor er det store variasjonar mellom verksemdene, med ulike behov og ulik risikoprofil, ulik økonomi og ulik tilgang på kompetanse. Det dei har til felles er eit ansvar for å velje dei mest hensiktsmessige og kostnadseffektive IKT-løysingane som dekker verksemda sine behov. Det same gjeld sjølvsagt for næringslivet.

Det offentlige har ei plikt til å drive mest mogleg kostnadseffektivt. Men dei har òg eit ansvar for å ta god vare på innbyggarane sine data og ta i vare innbyggarane sine interesser. Då er det viktig at dei, når dei skal velje IKT-løysingar, kan vurdere alle dei løysingane som er tilgjengelege – òg skytenester. Allmenne skytenester vil vere det rette for nokre verksemder, men ikkje for andre. Ofte kan den beste løysinga vere ein kombinasjon av fleire leveransemodellar.

Når ein spør verksemder om kva som er motivasjonen deira for å vurdere skytenester, er vanlege svar «reduserte kostnadar» og «auka fleksibilitet». Men det er òg eit anna svar ein høyrer stadig oftare: «Det er slik løysingane blir leverte nå. Om vi vil ha nyaste versjon av dei systema vi ønsker å bruke, så må vi velje sky.» Om ein skal etablere ny verksemd eller nye tenester, kan bruk av skytenester redusere behovet for investeringar og slik redusere risikoen ved etableringa.

Men mange verksemder – både offentlege og private – synest det er vanskeleg å vite om det er lovleg å bruke skytenester. Eller om det er sikkert nok. Og er det eigentleg greitt å lagre personopplysningar i utlandet? Med denne strategien ønsker regjeringa å klare opp i slike spørsmål.

Mål med strategien

Hovudmålet med *Nasjonal strategi for bruk av skytenester* er å gi offentlege og private verksemder større rom for handling når dei skal velje IKT-løysingar. Verksemdene skal – såframt det ikkje strid mot andre viktige omsyn – kunne velje å bruke skytenester der det vil gi best resultat og vere den mest kostnadseffektive løysinga.

Målet er at dette skal gi:

- meir kostnadseffektiv IKT
- auka merksemd på kjerneverksemda
- auka fleksibilitet
- betre tryggleik gjennom meir profesjonalisert og standardisert IKT
- lågare terskel for innovasjon og nyetablering
- redusert klimaavtrykk frå IKT-drift

[1] NOU 2015:1 *Produktivitet – grunnlag for vekst og velferd. Produktivitetskommisjonens første rapport*

Målgruppe for strategien

Denne strategien er retta mot alle verksemder – både offentlege og private. Mykje av strategien er spesielt retta mot offentleg sektor, men òg desse delane av strategien vil ha overføringsverdi for næringslivet. For dei delane av næringslivet som leverer IKT-løysingar til offentleg sektor vil det ikkje minst vere viktig å kjenne til kva prinsipp offentlege verksemder skal legge til grunn når dei skal skaffe nye IKT-tenester.

Strategien er i utgangspunktet ikkje retta mot forbrukarar. Det finst ei rekke interessante problemstillingar knytte til forbrukarretta skytenester, men desse fell utanfor måla for arbeidet med denne strategien. Barne- og likestillingsdepartementet og Forbrukarrådet arbeider med slike problemstillingar.

Samandrag

Strategien er bygd opp slik at dei generelle delane – som rettar seg mot både offentleg og privat sektor – kjem først.

I kapittel 2 går vi gjennom viktige kjenneteikn på skytenester, i tillegg til fordelar og utfordringar ved bruk av slike tenester. I dette kapittelet går vi òg gjennom nokre viktige generelle vurderingar ein må gjere når ein tenker på å kjøpe skytenester.

Ein viktig del av arbeidet med strategien har vore å gå igjennom det norske regelverket for å avdekke om det finst hindringar for bruk av skytenester, og å vurdere om dette er hindringar ein ønsker å gjere noko med. Det har òg vore viktig å sjå på område der regelverket er komplisert eller uklart, for å vurdere om ein kan gjere det meir tydeleg kva reglar som gjeld for bruk av skytenester.

Den juridiske vurderinga har resultert i nokre viktige tiltak:

- Revisjon av arkivforskrifta, og eventuelt delar av arkivlova, for blant anna å tilpasse arkivregelverket betre til digitalisering. Ein vil blant anna vurdere behov for endring slik at offentlege organ kan ta i bruk skytenester med serverar utanfor Noreg for arkiv.
- Vurdering av grunnlaget og handlingsrommet for å utvide tilgangen til å lagre bokføringsdata utanfor Noreg. På dette området er det òg viktige initiativ i gang i EU, og desse vil Noreg følge tett.
- Arbeid med å få til harmonisert praksis for tilsyn, så langt som mogleg, slik at verksemdene ikkje opplever motstridande krav knytt til skytenester frå ulike tilsyn.
- Bidrag til EU sitt arbeid med å få på plass sameinte kriterium (standardar, sertifiseringsordningar og liknande) for skytenester.

Dei juridiske utfordringane blir gjennomgåtte meir i detalj i kapittel 3.

Regjeringa har allereie gjennomført eit viktig tiltak retta mot bruk av skytenester.
I *digitaliseringsrundskrivet* for 2016, som blir sendt ut til alle statlege verksemder, er prinsipp om bruk av skytenester tatt inn:

- *Skytenester skal vurderast på linje med andre løysingar når ein står overfor større endringar eller omleggingar av IKT-system eller -drift:*
  - *ved innkjøp av nye system eller større oppgraderingar*
  - *ved større utskiftingar av maskinvare*
  - *når eksisterande driftsavtalar går ut*

- *Når skytenester gir den mest hensiktsmessige og kostnadseffektive løysinga, og det ikkje ligg føre spesielle hindringar for å ta i bruk slike tenester bør ein velje å bruke skytenester.*
- *Den valde løysinga må tilfredsstille verksemda sine krav til informasjonstryggleik. Dette krev at verksemda kjenner verdien av eigne system og data, og gjer ei risikovurdering av den valde løysinga.*

Prinsipp for bruk av skytenester er nærare beskrive i kapittel 4 – Vilkår for bruk av skytenester i offentleg sektor.

I kapittel 4 drøftar vi òg dei spesielle behova offentleg sektor har for kontroll, og kva kontroll-mekanismar som finst for skytenester. I dette kapittelet legg vi òg fram dei tiltaka som skal gjere det enklare for offentlege verksemder å vurdere skytenester:

- Etablering av eit rettleiings- og kompetansemiljø som kan støtte verksemdene når dei skal vurdere, og eventuelt kjøpe inn, skytenester.
- Vurdering av ulike modellar for ein mogleg marknadsplass/innkjøpsordning for skytenester retta mot offentleg sektor.
- Tilrettelegging for betre utnytting av eksisterande offentlege datasenterressursar for dei verksemdene som har behov for så sterk kontroll at dei vurderer å kjøpe særleg sikre datasentertenester eller etablere sitt eige datasenter i Noreg. I slike tilfelle skal verksemda vurdere om det er mogleg å utnytte ledig kapasitet hos – eller gå i sam-arbeid med – andre verksemder med tilsvarande behov.

2 Kva er skytenester?

Skytenester er skalerbare tenester som blir leverte over nett. Den viktigaste forskjellen på skytenester og meir tradisjonell tenesteutsetting er forretningsmodellen, der kunden berre betaler for den kapasiteten han har brukt. Målet er å tilby kostnadseffektive, sikre, skalerbare IT-tenester til kundane.

Det å kjøpe tenester frå eksterne leverandørar er ikkje noko nytt. Bruk av skytenester inneber i utgangspunktet ein tilsvarande risiko som ved tradisjonell utsetting av IKT-drift, der risiko og sårbarheit er knytte til val av leverandør, lokalisering, kommunikasjonskanalar og arkitektur.[2]

Regjeringa har valt å bruke den amerikanske standardiseringsorganisasjonen NIST (National Institute of Standards and Technology) sin definisjon på skytenester.[3]

NIST trekker fram følgande kjenneteikn på skytenester:

- *Behovsbaserte*
  Skytenester blir levert etter kvart som ein har bruk for dei. Dei kan skaffast raskt, og kunden betener seg sjølv på nett når han har bruk for auka kapasitet (for eksempel servertid eller lagring), utan at han treng å involvere leverandøren.
- *Leverte over nett*
  Tenestene er tilgjengelege over nettet, og kunden får tilgang gjennom standard-mekanismar som kan nyttast gjennom ulike typar klientar – frå mobiltelefonar og nettbrett til PC-ar.
- *Delte ressursar*
  Leverandøren kan fordele dataressursane sine dynamisk etter dei ulike kundane sine behov.
- *Umiddelbar fleksibilitet*
  Dei tenestene kunden treng kan skalerast opp eller ned etter kva kunden har bruk for, slik at ressursane i praksis blir opplevde som uendelege.
- *Betaling etter bruk*
  Ressursbruken blir målt, kontrollert og rapportert, og er gjennomsiktig for både kunden og leverandøren av tenesta.

Fem kjenneteikn	Tre tenestemodellar	Fire leveransemodellar
Behovsbasert – gjerne sjølvbetent	Programvare som teneste (SaaS) *Eks: Kontorstøtte, CRM, Rekneskap*	Allmenn sky (Public Cloud)
Levert over nett	Plattform som teneste (PaaS) *Eks: Database, utviklingsmiljø, operativsystem*	Gruppesky *Liknande verksemder går saman om ei nettsky*
Ressursdeling	Infrastruktur som teneste (IaaS) *Eks: Lagring, behandling, virtualisering*	Privat sky
Umiddelbart fleksibelt (Rapid elasticity)		Hybrid sky *Allmenn sky kombinert med privat sky/gruppesky*
Betaling etter bruk		

[2] NOU 2015: 13 *Digital sårbarhet – sikkert samfunn*

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

Eksempel: UNINETT – ein skymeklar for UH-sektoren

UNINETT er eigd av Kunnskapsdepartementet og leverer nett og nettenester for universitets- og høgskulesektoren (UH) i Noreg. I 2016 har departementet gitt UNINETT i oppdrag å etablere ei felles skyteneste for norske universitet og høgskular. Med utgangspunkt i dette vil UNINETT etablere ein skymeklarfunksjon der heile UH-sektoren kan finne sikre skytenester, blant anna kommersielle skytenester som er lagde til rette for sektoren.

UNINETT har allereie etablert programmet UH-sky i samarbeid med universiteta i Trondheim, Oslo, Bergen og Tromsø. Arbeidet med skymeklarfunksjonen vil vere ei vidareføring av dette.

UNINETT arbeider òg med skybaserte infrastrukturplattformer der dei vil gjere typiske datasenteroppgåver tilgjengelege frå skya. Nokre universitet samarbeider òg om å etablere ei sektorintern infrastrukturplattform i datasentera sine, slik at dei på sikt kan tilby infrastrukturtenester til andre i sektoren.

Kjelde: UNINETT

Tenestemodellar

Det er mogleg å kjøpe tenester i skya på ulike nivå, avhengig av kva verksemda har bruk for. Programvare eller applikasjonar som køyrer på datasenter «i skya», og som kunden/brukaren får tilgang til gjennom internett, kallar vi *programvare som teneste* (Software as a Service, SaaS). Bruk av programvare i skya gjer at kunden slepp å kjøpe, installere, oppdatere og vedlikehalde programvara lokalt. I staden køyrer brukaren programmet gjennom ein nettlesar eller ein annan tynn klient. Eksempel på tenester er kontorstøtte som tekstbehandling og rekneark, rekneskapssystem eller system for å følgje opp kundar (CRM).

Plattform som teneste (Platform as a Service, PaaS) omfattar alt som trengst for å støtte bygging og levering av digitale tenester. Ei plattform kan vere ein database, eller heile utviklings- eller testmiljø som blir køyrt hos skyleverandøren.

Infrastruktur som teneste (Infrastructure as a Service, IaaS) omfattar alle dei dataressursane ein normalt vil ha i sitt eige datasenter eller datarom: serverar, nettverk og lagring. Sjølv om kjøp av programvare og plattformtenester i skya etter kvart blir meir utbredt, er det fortsatt kjøp av lagrings- og behandlingskapasitet som er mest vanleg.

Leveransemodellar

Skytenester kan leverast på mange ulike måtar:

Den allmenne skya (Public cloud) er skytenester som blir selt i den opne marknaden – det vil seie standardiserte løysingar som stort sett er like for alle kundar. Dei største og mest kjende leverandørane er Google, Amazon og Microsoft.

Den allmenne skya kan òg vere ein del av arkitekturen til programvareleverandørar – òg norske – som tilbyr programvara si levert over internett. Ein sluttkunde kan dermed vere brukar av den allmenne skya utan sjølv å ha kjøpt ei slik infrastrukturteneste.

Ei *privat sky* (Private cloud) er ei lukka skyteneste som er avgrensa til ei verksemd, eller til ei gruppe verksemder (oftast omtalt som *gruppesky)*. Her vil miljøet som skytenesta blir levert frå

blir avsett til den enkelte kunden eller kundegruppa. Ei verksemd kan òg drifte si eiga sky, men dersom verksemda ikkje er veldig stor, vil ein ikkje oppnå dei same stordriftsfordelane som ein får med å bruke ei allmenn sky. Samtidig vil ein heller ikkje vere utsett for dei same risikoane.

Dersom ei verksemd bruker ein kombinasjon av den allmenne skya og tradisjonelle lokalt drifta IKT-system, ei privat sky eller ei gruppesky, kallar vi det *hybrid sky*.

Dei fleste verksemder har informasjon som dei av ulike årsaker synest det er vanskeleg å plassere i den allmenne skya. Det kan vere informasjon som er kritisk for verksemda, informasjon der gjeldande reglar ikkje tillèt lagring i utlandet, eller data der ein ikkje toler den forseinkinga behandling ein annan stad fører med seg. Samtidig kan allmenne skytenester vere eit godt alternativ når ein treng ekstra kapasitet, som ein plass å lagre tryggleikskopiar, eller for system verksemda brukar som ikkje er kritiske eller inneheld informasjon som må lagrast lokalt. Ein arkitektur med ei hybrid sky gjer at verksemda både kan utnytte fordelane med den allmenne skya, og samtidig halde kritiske komponentar under eigen kontroll. Hybrid sky er den leveransemodellen som veks raskast for tida.[4]

I denne strategien er det først og fremst problemstillingar knytte til bruk av *allmenne skytenester* som blir omtalte. Ei klargjering av kva som er lov og anbefalt når det gjeld allmenn sky, vil kunne overførast til ulike modellar med gruppesky eller hybrid sky der den allmenne skya inngår som ein del av arkitekturen.

Fordelar og utfordringar med skytenester

Økonomiske innsparingar er det som oftast blir trekt fram som fordelen med bruk av skytenester. Det er òg dette som har vore motivasjonen i mange av dei landa der styresmaktene allereie har etablert ein IKT-strategi der skytenester speler ei viktig rolle. Storbritannia har for eksempel innført ein preferansepolitikk for skytenester,[5] og forventar at ein overgang til rimelige og standardiserte IKT-løysingar skal gi reduserte IKT-kostnadar for det offentlege.

I ein studie frå KS[6] oppgir dei spurde kommunane at dei viktigaste drivarane for å ta i bruk skytenester er: økonomi, eit ønske om å fokusere på tenesteutvikling, skalering og fleksibilitet og auka tilgjenge til kommunen sine løysingar for innbyggarane.

Økonomi

Mange tenker automatisk på reduserte kostnadar når dei høyrer ordet «skytenester». Det er fleire grunnar til dette: Fordi ei skyteneste ikkje krev lokal infrastruktur, blir både investeringar og kostnadar til drift av IKT påverka. Skytenester kan òg føre til reduserte kostnadar til oppdateringar, administrasjon av programvarelisensar og liknande.

Prisingsmodellen for skytenester, med måling av og betaling for bruk, gjer òg at kostnadane for kvar teneste blir transparente. Ein slepp å betale for meir datakraft, meir lagring eller fleire programvarelisensar enn ein treng til kvar tid. Ein slik prismodell er spesielt gunstig dersom

[4] Rightscale (2016): *State of the cloud report*

[5] HM Government (2011): *Government Cloud Strategy. A sub strategy of the Government ICT Strategy*

[6] Advokatfirmaet Føyen Torkildsen AS (2015): *Utredning av juridiske forhold ved bruk av nettsky i kommunal sektor – en mulighetsstudie*. KS FoU-prosjekt 144008

Eksempel: Moss kommune

Moss kommune har 32 000 innbyggarar og 2500 tilsette. Kommunen forvaltar ca 100 applikasjonar og har 8,2 årsverk på IKT.

Kommunen måtte skaffe mange fleire e-postlisensar då han skulle gi alle tilsette tilgang til e-post. Kommunen fann at Office 365 i nettskya kosta mykje mindre enn tilsvarande programvare installert lokalt. Kommunen har valt ei hybrid løysing der delar av system-porteføljen (blant anna arkiv) blir drifta lokalt, mens for eksempel kontorstøtte blir drifta i ei allmenn skyteneste (Microsoft Azure). Kommunen vurderte òg tradisjonell outsourcing, men kom til at dette ville bli mykje dyrare enn ei skyløysing, og òg dyrare enn å halde fram med lokal drift.

Kjelde: Moss kommune

ein har prosessar som krev mykje kapasitet, men som ein sjeldan treng å køyre – for eksempel faste månadlege eller årlege jobbar som utsending av fakturaer eller køyring av lønn.

Ikkje alle verksemder som tar i bruk skytenester opplever at det er rimelegare enn andre løysingar. Dette gjeld spesielt om ein har særskilde behov som ikkje kan leverast som ei standardløysing, eller om skytenesta skal gå inn i ein komplisert arkitektur med mykje integrasjon mot eksisterande system.

Skalering

Skytenester tilbyr nær uavgrensa kapasitet for databehandling og -lagring. Ressursane i nettskya blir allokerte til verksemda berre når det er bruk for dei. Dette gjer at verksemder ikkje treng uroe seg for å sleppe opp for kapasitet, dersom for eksempel ei publikumsteneste blir mykje meir brukt enn forventa. Dette er òg ein fordel dersom ein har tenester som er utsette for spesielle belastningar i korte tidsrom – gjerne utan at ein kan seie i førevegen at det kjem til å skje.

Dei elementa som gjer skytenester kostnadseffektive og skalerbare kan òg skape utfordringar for verksemder som skal forvalte personopplysningar, konfidensiell informasjon eller opp-lysningar innanfor andre område der det finst reglar for kva land ein kan overføre data til. For å kunne tilby rimelege tenester unyttar leverandørane den ledige kapasiteten dei har i systema sine. Dermed kan ein ikkje alltid vite kva datasenter – eller kva land – informasjonen er lagra i til kvar tid. Det kan òg vere at leverandøren av ei programvareteneste i skya bruker fleire ulike underleverandørar, utan at dette går tydelig fram av beskrivinga av tenesta.

Tryggleik

Utkontraktering av skytenester kan gi auka teknisk IKT-tryggleik når leverandøren har betre kompetanse og ressursar enn kunden.[7] Dette gjeld ikkje minst fysisk sikring av lokala der maskinvara er plassert. Store datasenter har som regel omfattande sikringstiltak, og det er strenge restriksjonar på kven som får komme inn i anlegga. Leverandørane skifter ut maskin-vare og oppgraderer programvare regelmessig. Det finst sertifiseringsordningar for data-senter som angir kva tryggleiksnivå datasenteret tilfredsstiller.

[7] NOU 2015: 13 *Digital sårbarhet – sikkert samfunn*

Eksempel: Banedanmark

I desember 2010 flytta Banedanmark informasjonsnettsida si til ei skyteneste (Microsoft Azure). Om vinteren blei det store problem med transporttenestene i Danmark. Dei andre transportselskapa opplevde at informasjonstenestene svikta på grunn av stor pågang frå publikum. Dette skjedde ikkje med Banedanmark. På det meste hadde dei 5,5 millionar brukarar på ein dag, mot normalt 50 000. Den auka kapasiteten dei trong i denne perioden betalte dei 179 DKK for.

Kjelde: Center for Digital Forvaltning (2013): *Public sector use of cloud based solutions – the Danish experience*. Undersøking på vegne av Microsoft

Når programvare blir levert i form av ei skyteneste, betyr det som oftast at kunden får ei standardisert løysing frå leverandøren. Det betyr òg at alle kundar får tryggleiksoppdateringar og andre programvareoppdateringar samtidig. For mange kundar kan dette føre til ei auke i tryggleik, fordi dei har mangla gode eigne rutinar for slik oppdatering.

Tryggleikskopiering er vanlegvis ein del av tenesteporteføljen når ein kjøper tenester i nettskya. Lagring av data på fleire stader (redundans) og automatisk overføring til ein ny lokasjon dersom noko går gale på primærlokasjonen, er òg som oftast ein del av standardtenesta.

Ei teneste som er i framvekst i nettskya er *Security as a Service* (SECaaS). Gjennom SECaaS kan ei verksemd abonnere på ulike typar tryggingstenester, som anti-virusprogram og kontinuerlege virusoppdateringar, autentisering, angrepsdeteksjon og administrasjon av tryggleikshendingar.

Sjølv om skytenester i mange tilfelle kan gi betre tryggleik, er det viktig at verksemdene vurderer om det er delar av informasjonen dei forvaltar som bør sikrast særskilt – av økonomiske, konkurransemessige eller andre årsakar. For mange verksemder kan det òg vere relevant å vurdere dei tryggingspolitiske konsekvensane av å bruke skytenester som er baserte utanfor EØS-området. I nokre land er det slik at styresmaktene har større rom for innsyn i utanlandske data enn i data til eigne innbyggarar og verksemder. Det kan vere aktuelt å vurdere slike forhold òg for verksemder som ikkje er underlagde tryggingslova.

Det er verdt å nemne at informasjon som i utgangspunktet ikkje er skjermingsverdig, kan bli betrakta som skjermingsverdig om han blir lagra i eit felles datasenter eller ei skyteneste der informasjonen til fleire samfunnsfunksjonar er samla. Då vil skadepotensialet ved tap av den samla informasjonen kunne få innverknad på den nasjonale tryggleiken. Dette kan gjere risikovurderingar meir kompliserte, ettersom ein risikerer å måtte vurdere ikkje berre sine eigne data, men òg summen av data som er lagra på same stad.

Mange verksemder føler det er trygt å ha eigne serverar og data nær seg. Det å lagre og behandle data langt unna – kanskje utan å vite nøyaktig kor informasjonen er til kvar tid – fører til ei kjensle av kontrolltap. Dette kan ein kompensere gjennom andre mekanismar for kontroll. Mekanismar for kontroll blir særskilt omtalte i kapittel 4.

Energieffektivitet

Leverandørar av allmenne skytenester kan dele maskinvareressursane mellom ei stor mengde kundar. Dette gir meir effektiv energibruk enn om alle kundane skulle hatt sine eigne datasenter med eiga maskinvare, kjøling med meir.

Det er ein trend at leverandørar av sky- og datasentertenester konsoliderer datasentera sine til store, og stadig meir energieffektive einingar. Desse datasentera blir gjerne lagde til stader der det er stabil tilgang på billeg energi.

Fleksibilitet

Bruk av skytenester gjer det i mange tilfelle lettare å legge til rette for at tenestene (for eksempel eit saksbehandlingssystem i ein kommune) kan nyttast frå fleire ulike stader og ulike typar klientar (PC, nettbrett, mobil).

Det blir stadig vanlegare for verksemder – òg offentlege – å la dei tilsette bruke eigne PC-ar, nettbrett og liknande. Dette blir gjerne omtalt som *Bring Your Own Device,* eller *BYOD*. BYOD fører med seg nye utfordringar, når det gjeld både tryggleik og tilgjenge. Skytenester kan gjere det meir naturleg for brukarane å lagre arbeidet sitt på verksemda sitt område i skya, i staden for lokalt på eigne terminalar som er utanfor verksemda si kontroll. I dei fleste verksemder finst det tilsette som allereie bruker uautoriserte skytenester berekna på forbrukarmarknaden for å kunne ha ein fleksibel arbeidskvardag. Dette utgjer ein risiko for verksemdene, ikkje minst fordi sluttbrukaravtalane for forbrukarmarknaden ofte gir leverandørane vide fullmakter for kva dei kan gjere med informasjonen frå kundane sine.

Etter kvart som verksemdene kjøper stadig fleire tenester som skytenester, vil dette påverke kva kompetanse ein treng lokalt. Dette kan gi redusert kompetanse på enkelte område fordi dei tilsette ikkje lenger arbeider med området i kvardagen. Samtidig kan det òg fri viktig kompetanse frå rutineoppgåver, slik at ein kan bruke meir energi internt på strategisk planlegging og tenesteutvikling.

Innovasjon

Bruk av skytenester kan redusere investeringane som trengst for å sette opp ei ny verksemd. Fordi ein ikkje treng å gjere store investeringar i maskinvare og infrastruktur eller programvarelisensar, blir behovet for startkapital redusert.

Dette er spesielt relevant dersom ein skal starte ei verksemd som leverer tenester til kundane over internett: Det kan vere vanskeleg å estimere kor mange kundar ein kjem til å få, og kor raskt. Samtidig er det risikabelt å ikkje ha tilstrekkeleg kapasitet til å levere ei teneste dersom ho raskt blir ein suksess. Ein skybasert infrastruktur som kan skalere etter kor raskt ein får kundar, og der ein betaler for bruken, reduserer risikoen for store tap på infrastrukturinvesteringane. Ein slik modell gjer òg at ein kan vere meir tolmodig og bruke tid på å tilpasse og vidareutvikle tenesta i startfasen om ein ikkje lukkast med ein gong.

Av same grunn kan skytenester gjere det enklare for eksisterande verksemder å sette opp plattformer for utvikling og innovasjon, slik som testmiljø eller pilotprosjekt. Dette kan senke terskelen for å prøve ut nye løysingar, både internt og mot kundar.

For det offentlege kan slike plattformer gjere det enklare å teste ut og ta i bruk nye innbyggarretta tenester. Dette er ikkje minst viktig for kommunane, som gjerne har lite ressursar å sette

Eksempel: Comoyo

Comoyo var Telenor si satsing på strøyme-TV. Tenesta blei etablert allereie i 2011.

Så seint som i mai 2013 uttalte Telenor: «Med nyetablerte Comoyo skal Telenor kapre 130 millionar forbrukarar i alle kanalar og på alle plattformer.» Telenor avvikla Comoyo i november 2013, etter at store internasjonale aktørar som Netflix og HBO etablerte seg med strøyme-TV i Norden og tok det meste av marknaden.

Telenor brukte Amazon sin infrastruktur til å levere tenesta på. Dermed betalte dei berre for den kapasiteten dei trong for å betene dei kundane dei hadde til kvar tid. Då tenesta blei lagt ned, satt dei derfor ikkje igjen med store investeringar i infrastruktur dei ikkje lenger hadde bruk for.

Kjelder: Teknisk Ukeblad/Comoyo/Telenor

av til slikt arbeid. Slik kan skytenester bidra til både effektivisering og tenesteutvikling i det offentlege.

Viktige vurderingar før anskaffing av skytenester

Regjeringa ønsker å gjere det enklare for offentlege verksemder og næringsliv å vurdere skytenester som alternativ når dei skal skaffe nye IKT-tenester. Eit viktig grunnlag for å kunne gjere dette er den avklaringa av regelverk som blir omtalt i kapittel 3. Men det finst òg mange omsyn ein må ta når ein skal vurdere skytenester som ikkje er direkte knytte til regelverket.

Sourcing

Dei strategiske vala ei verksemd gjer når det gjeld kva tenester som skal skaffast frå eksterne leverandørar, og kva tenester verksemda av strategiske grunnar vel å handtere sjølv, kallar vi *sourcingstrategi.*

Slik strategi omfattar ikkje berre IKT; ei verksemd kan òg velje å sette ut for eksempel økonomi og rekneskap, logistikk eller andre oppgåver verksemda ikkje ser på som ein del av kjerneverksemda si. Dette blir som oftast kalla *outsourcing.* Ein grunn til å sette ut tenester kan vere at ein gjennom dette kan oppnå stordriftsfordelar, slik at det blir meir kostnadseffektivt enn å produsere tenestene sjølv.

Kjøp av skytenester er ei form for sourcing. Det same er det å velje å produsere eller drifte IKT-løysingane sine internt i verksemda. Same kva for ein sourcingstrategi ein vel, må ein gjere ein analyse for å avgjere om den valde løysinga tilfredsstiller krava som gjeld for den typen informasjon systemet behandlar, og om risikoen med den valde strategien er akseptabel. Det å vurdere risiko eller passe på at ein har databehandlaravtalar på plass, er ikkje noko som er spesielt for anskaffing av skytenester – det må ein gjere uansett kva strategi ein vel.

Arkitektur

Difi har definert eit sett overordna arkitekturprinsipp[8] som fungerer som felles retningslinjer for alt arbeid med IKT i offentleg sektor. Det er i utgangspunktet obligatorisk for statlege verksemder å følge prinsippa, mens prinsippa er anbefalte for kommunal sektor.

Sjølv om ei verksemd ikkje kan sjå at det finst skytenester i dag som tilfredsstiller dei krava ho har til det systemet ho skal utvikle eller skaffe, så vil ho, gjennom å følge Difi sine arkitekturprinsipp, sikre at ho ikkje har sperra for bruk av nettsky som plattform seinare.

Dei viktigaste prinsippa for å sikre at ein ikkje låser seg mot bruk av sky er:

- *Teknisk interoperabilitet*: Dette inneber å bruke tekniske standardar som legg til rette for veldefinerte grensesnitt, overføringsprotokollar og format.
- *Fleksibilitet:* IKT-løysingar skal utformast slik at dei ikkje avgrensar seinare endringar i arbeidsprosessar, innhald, organisering, eigarforhold eller infrastruktur.
- *Skalering:* IKT-løysingar skal kunne skalerast ved endringar i bruk. Endringar kan for eksempel vere knytt til talet på brukarar, volum, responstider eller liknande. Det må vere mogleg å skalere løysinga opp eller ned etter at ho er sett i drift.

Dei andre prinsippa – som tryggleik og tenestorientering – er sjølvsagt like viktige og relevante for eit IKT-prosjekt der ein vurderer å bruke skytenester som for andre typar prosjekt.

Dersom ei verksemd skal utvikle nye, lokale system, er det viktig at verksemda vel ein arkitektur som kan dra nytte av dei karakteristiske fordelane med skytenester, og som eignar seg for overgang til skya, om verksemda skulle ønske å gjere dette på eit seinare tidspunkt.

Informasjonstryggleik

Dei tryggleiksvurderingane ein må gjere dersom ein tenker på å ta i bruk skytenester, er ikkje så ulike dei vurderingane ein må gjere om ein elles skal sette ut tenester til ein ekstern leverandør. I praksis betyr dette at ein må ha eit forhold til dei formelle garantiane leverandøren gir, for eksempel for kor data vil bli lagra eller behandla.

Risikoen ved å bruke skytenester vil variere avhengig av kor sensitive data ein skal lagre eller behandle, og korleis den valde skytenesteleverandøren har implementert sine spesifikke skytenester. Kor omfattande vurderinga av leverandøren må vere, vil avhenge av kva som er verdien av den informasjonen det er snakk om, og kor alvorlege konsekvensane kan vere dersom noko går gale.

Informasjonstryggleik handlar om korleis integritet og konfidensialitet blir handtert, og kor tilgjengeleg informasjonen er.[9]

Integritet er tryggleik for at informasjonen er fullstendig, nøyaktig og ikkje utdatert. Integriteten seier òg noko om at det ikkje er gjort uautoriserte endringar i informasjonen.

Konfidensialitet er tryggleik for at informasjonen ikkje blir avslørt for uvedkommande, og at berre autoriserte personar – det vil seie personar som har rett til det – får tilgang til informasjonen.

[8] Direktoratet for forvaltning og IKT (2012): *Overordnede IT-arkitekturprinsipper for offentlig sektor*. Versjon 2.1, 17. september 2012

[9] Fornyings-, administrasjons- og kyrkjedepartementet (2013): *Nasjonal strategi for informasjonssikkerhet*

Tilgjenge er tryggleik for at ei teneste fyller krav til stabilitet, slik at den aktuelle informasjonen er tilgjengeleg når det er bruk for han.

Tidlegare var hovudtyngda av uroa rundt tryggleik knytt til konfidensialitet. Ein var først og fremst uroleg for om uvedkommande kunne få tak i for eksempel forretningsløyndomar eller sensitiv informasjon om personar. Vi ser nå stadig meir uro knytt til integritet. Uautorisert endring av data kan skje både som følgje av tekniske faktorar og som ei vondsinna handling. Dersom ein ikkje kan føle seg trygg på integriteten i systemet ein brukar, kan det få alvorlege konsekvensar om ein skal bruke informasjonen til å ta viktige avgjerder, eller om han for eksempel inngår i system som er kritiske for verksemda eller kundane.

Etter kvart som samfunnet blir meir avhengig av å ha tilgang til IKT og nettverk for å fungere, blir òg tilgjenge stadig viktigare i vurderinga av informasjonstryggleiken. Dersom ei viktig teneste ikkje er tilgjengeleg over ei tid, kan det få alvorlege konsekvensar for ei verksemd. Mange verksemder har kritiske system der ein ikkje toler noko nedetid i det heile.

Utvalet som er sett ned for å vurdere den digitale sårbarheita i samfunnet har òg trekt fram eit fjerde tryggingsmål: *sporbarheit.*[10] Sporbarheit dreier seg om å kunne finne ut kva som har skjedd i ettertid, for eksempel gjennom endringsloggar og loggar over andre typar hendingar.

Offentlege verksemder skal – og private verksemder bør – gjennomføre risiko- og sårbarheitsanalysar ved større endringar, som etablering av nye digitale tenester, omlegging av drifta, skifte av leverandørar og liknande. Om ein behandlar personopplysningar gjeld dette alle verksemder. Verksemda må då vurdere kva konsekvensar ulike hendingar kan få, både for brukarane av verksemda sine tenester, for verksemda sjølv og for sektoren i det heile. Verksemda må så vurdere kor sannsynleg det er at desse konsekvensane vil inntreffe. Risikonivået er gitt av kombinasjonen av konsekvens og kor sannsynleg det er at ei hending skal inntreffe.

På same måte må kvar verksemd vurdere kva konsekvensane vil bli dersom det skjer brot på informasjonstryggleiken innanfor dei tre dimensjonane: Kva vil skje dersom eit system eller ei teneste blir utilgjengeleg over eit gitt tidsrom? Kva er konsekvensen om uvedkommande får innsyn i informasjonen? Kva kan konsekvensane bli om uautoriserte personar kan endre på informasjonen slik at han ikkje lenger er til å stole på? Kor sannsynlege er dei ulike konsekvensane? Kva konsekvens gir den største risikoen? Kva krav bør ein stille til ein intern eller ekstern leverandør for å handtere slik risiko?

Hensikta med ei risikoanalyse er å hjelpe den verksemda som vurderer å skaffe skytenester til å gjere ei informert vurdering av om bruk av skytenester er innanfor eit risikonivå som er akseptabelt. Ei slik vurdering må ein òg gjere for andre former for sourcing der verksemda må gi kontroll over data til ein ekstern partner.

Behandling av personopplysningar

Det er viktig å sjekke at den databehandlaravtalen som blir brukt tilfredsstiller krava i personopplysningslova. Når den nye personvernforordninga (sjå kapittel 3) har tredd i kraft, slik at det same regelverket gjeld for all behandling av personopplysningar om innbyggarar i EU/EØS-området, vil ein truleg sjå meir standardiserte avtalar frå leverandørindustrien.

[10] NOU 2015: 13 *Digital sårbarhet – sikkert samfunn*

Det digitale sårbarheitsutvalet

I juni 2014 sette regjeringa ned eit utval som skulle kartlegge den digitale sårbarheita i samfunnet (Lysne-utvalet). Utvalet overleverte utgreiinga si til justis- og beredskaps-ministeren 30. november 2015.

Om skytenester skriv utvalet blant anna:

- Ressurssterke tilbydarar av skytenester kan i mange tilfelle gi betre tryggleik enn det mange mindre verksemder kan greie sjølve. Dette vil sjølvsagt avhenge av tilbydaren. Det er brukaren av skytenesta som må vurdere om dei opplysningane han tenker å legge i skya er sårbare dersom dei kjem utanfor norsk jurisdiksjon, og vege konsekvensane og risikoen opp mot fordelane med skytenesta.
- Styresmaktene må ikkje gjere det vanskeleg å ta i bruk hensiktsmessig og kostnadseffektiv teknologi så lenge det finst løysingar som er trygge nok. Det er viktig at norsk lovgiving ikkje hindrar auka konkurransekraft.
- Arkivlova §9, som seier at arkiv ikkje kan førast ut av landet, blei til for over 20 år sidan, og tar ikkje omsyn til ei moderne teknologisk utvikling og nye behov.

Tilrådingar frå utvalet

Opplysningar kan delast inn i tre kategoriar:

1. informasjon som berre bør lagrast i Noreg
2. informasjon som kan lagrast i utlandet, men som ein må kunne ta heim om det blir særleg behov for det, og på bestemte vilkår
3. informasjon som kan lagrast i utlandet utan vilkår

Kategori 1 – informasjon som berre bør oppbevarast innanfor norsk territorium og jurisdiksjon, gjeld særleg for gradert informasjon. Utvalet meiner det er den enkelte sektoren som må vurdere kva informasjon som fell inn under dei ulike kategoriane. Samtidig peiker utvalet på at sektorane i mange tilfelle har vanskeleg for å koordinere seg på tvers, slik at det òg er bruk for krav og rettleiing på tvers av sektorane.

Utvalet meiner det er bruk for harmonisering av tilsynspraksisen på tvers av sektorar. Som ein del av dette arbeidet bør ein sjå nærare på korleis ein kan bruke tredjepartsrevisjonar.

Kjelde: NOU 2015: 13 *Digital sårbarhet – sikkert samfunn*

Merk at det i siste instans *alltid* er verksemda sjølv (den behandlingsansvarlege) som har ansvaret for at informasjon blir behandla forsvarleg. Dette ansvaret blir ikkje overført til leverandøren sjølv om ein har alle avtalar på plass. Med den nye personvernforordninga vil leverandøren (databehandlaren) òg ha eit ansvar, men det erstattar ikkje ansvaret til den behandlingsansvarlege.

Datatilsynet har laga ei sjekkliste med punkt verksemder må vurdere før dei tar i bruk skytenester som skal behandle personopplysningar.[11] Sjekklista er basert på regelverket og beste praksis.

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

- Verksemda må gjere grundige risikovurderingar, inkludert analyse av risiko- og sårbarheit.
- Verksemda må inngå ein tilfredsstillande databehandlaravtale, i tråd med norsk regelverk. Det er den behandlingsansvarlege, det vil seie den enkelte verksemda, som har ansvar for at krava i loven er følgt. Det må komme klart fram kor data blir behandla, òg for underleverandørar.[12] Avtalen kan ikkje innehalde noko om at leverandøren (databehandlar) kan bruke personopplysningar til eigne formål, for eksempel til å forbetre tenestene sine.
- Verksemda må revidere bruken av skytenester jamleg. Det vil seie at verksemda sjølv, eller ein tredjepart, gjer ein tryggingsrevisjon og sikrar at databehandlaravtalen er følgt. Dersom det er kontroll, må verksemda kunne legge revisjonsrapporten fram for Datatilsynet.
- Den behandlingsansvarlege må sørge for at overføring av data til andre land følger loven.
- Det må vere sikker kommunikasjon, og kommunikasjonen må vere kryptert. Ein må kryptere sensitive personopplysningar.
- Personopplysningar frå ulike kundar (behandlingsansvarlege) må vere skilt frå kvarandre hos skyleverandøren (databehandlar).
- Løysinga som blir brukt må vere tilstrekkeleg dokumentert, og verksemda må kunne legge fram dokumentasjon for kontroll.

Innkjøp

Kjøp av skytenester bryt på mange måtar med den tradisjonelle måten å drive innkjøp på i offentleg sektor. Sjølv om regelverket for anskaffing i offentleg sektor ikkje i seg sjølv inneber noka avgrensing av høvet til å skaffe eller bruke skytenester, er det mange viktige ting ein må ta omsyn til ved innkjøp av slike tenester:

Samanlikning av prisar

Formålet med regelverket for offentleg anskaffing er å sikre best mogleg utnytting av ressursane i samfunnet. Derfor er det kostnaden for den innkjøpte vara eller tenesta gjennom heile levetida som er viktig. Dette omtaler vi gjerne som total levetidskostnad (*Total Cost of Ownership, TCO).*

TCO ved eiga drift kan bereknast som summen av kostnadane til:[13]

- energiforbruk (straum til maskinane, nødstraum, straum til kjøling)
- tilsette (lønn og sosiale kostnadar)
- nettverk
- bygningar (nedskriving, vedlikehald, evt. leige, tryggingstiltak mm)
- lisensar og vedlikehaldsavtalar
- maskinvare

Det er særskilt relevant å ta omsyn til dette når ein skal vurdere kostnaden for ei teneste som består av ein kombinasjon av for eksempel programvare som teneste og drift av denne

[12] Dette kravet er henta frå Artikkel 29-gruppa: *Opinion on C-SIG Code of Conduct on Cloud Computing*

[13] The Scottish Government (2014): *Scotland's Digital Future: Data Hosting and Data Centre Strategy for the Scottish Public Sector*

programvara hos skyleverandøren, opp mot det å kjøpe programvara som produkt og sjølv stå for drifta, eventuelt kjøpe driftstenester hos ein tredjepart.

Korleis spesifisere behov?

For å sikre at ein vel det mest fordelaktige tilbodet, er det viktig å spesifisere kva funksjonar ein treng, og ikkje først og fremst komme med detaljerte tekniske spesifikasjonar. Då er det mindre sjanse for at ein stenger ute nokon teknologiske plattformer frå starten av.

Val av kontrakt

For skytenester kan det òg vere vanskeleg for kunden å velje kontraktsform. Skytenester blir ofte selde med standard vilkår som er felles for alle kundar. Difi reviderte staten sine standardavtalar (SSA) i 2015, og dei nye avtalane er betre tilpassa skytenester enn dei gamle avtalane som skilde strengt mellom programvare og drift. Dei nye SSA-ane opnar for å ta inn standard lisens- og avtalevilkår frå leverandøren. Dei kan derfor brukast for kjøp av tilgang til standardsystem i skya. SSA-en blir då supplert med leverandøren sin standard tenesteavtale og eventuelt databehandlaravtale basert på Datatilsynet sin mal.

For meir kompliserte kjøp kan det vere vanskeleg å få skytenester til å passe inn i dei standardavtalane som finst, der ein skil mellom kjøp av program- og maskinvare[14] og kjøp av driftstenester[15].

Exit-kostnadar

Korleis får ein tak i eigne data hos leverandøren når kundeforholdet er avslutta – uavhengig av grunn? Korleis får ein flytta data til ein ny leverandør? Og kva skjer med data som oppstår som eit resultat av drifta, slik som bruksstatistikk? Som ved kjøp av anna programvare, er det viktig å passe på at ein ikkje endar opp med å vere låst til éin spesiell leverandør, eller at ein ikkje har kontroll over eigne data. Det er derfor viktig å sikre at ein kan få tak i opplysningane sine i eit format som ein kan bruke vidare. Det er verdt å merke seg at den nye personvernforordninga til EU inneheld krav om portabilitet. Dette gjeld for personopplysningar, men vil truleg i praksis få effekt for alle typar data.

Dei fleste verksemder vil ha nytte av å lagre data over tid, og det er derfor ikkje usannsynleg at ein vil flytte data mellom leverandørar. For det offentlege – som har arkivplikt – er det spesielt viktig å ta omsyn til bevaring for ettertida. Det er arkivskaparen sin plikt å sikre at alt arkivverdig materiale som er digitalt skapt blir fanga opp, og at det ikkje går tapt viss ein for eksempel bytter leverandør eller leverandøren går konkurs.

[14] Difi: *Kjøpsavtalen* (SSA-K). Denne avtalen gjeld kjøp av IT-utstyr og/eller programvare

[15] Difi: *Driftsavtalen* (SSA-D). Driftsavtalen dekker eit spekter av driftssituasjonar, med fokus på standardiserte driftstenester

3 Skytenester og utfordringar i regelverket

Ei interdepartemental arbeidsgruppe har gått gjennom lover og forskrifter og vurdert kva for regelverk som skaper utfordringar for bruk av skytenester. Gruppa har òg sett fram forslag til moglege endringar. Motivasjonen med arbeidet har vore å oppretthalde vern av personopplysningar, god tryggleik og sikring av viktige dokument for ettertida. I arbeidet har gruppa vurdert intensjonen i lovverket opp mot dagens teknologiske verkelegheit, og vurdert om det er mogleg å vareta denne intensjonen samtidig som ein opnar for å utnytte det potensialet som ligg i skyteknologien.

I vurderinga av regelverket opp mot skytenester, er det først og fremst reguleringa av *kor* ein kan lagre data som gir utslag. Det finst ikkje regelverk som eksplisitt regulerer bruken av *teknologien* skytenester bygger på, men gjennom å stille krav til at data skal lagrast innanfor eit geografisk område, kan ei lov eller forskrift sette grenser for bruken av allmenne skytenester.

Det er to viktige lover – i tillegg til tryggingslova – som klart stiller slike krav til kor data skal lagrast: arkivlova og bokføringslova.[16] Personopplysningslova stiller òg krav til lagring og behandling av data, men desse krava set ikkje like store grenser for kva land personopplysningane kan lagrast eller behandlast i.

Arkivlova

Offentlege organ har plikt til å ha arkiv som er innretta slik at dokumenta er trygga som informasjonskjelder for samtid og ettertid, jf. arkivlova §6. Offentlege organ må derfor stille krav til leverandørar av skytenester om tilgjenge, konfidensialitet og integritet (sjå kapittel 4 for meir om vilkår for bruk av skytenester i offentleg sektor).

I §9 bokstav b i arkivlova heiter det at arkivmateriale ikkje kan *«førast ut or landet».* Lagring av arkiv i ei skyteneste som bruker serverar utanfor Noreg vil dermed stride mot lova, sjølv om verksemda sjølv har vurdert at innhaldet i arkivet er av ein slik karakter at det kan lagrast i utlandet. Riksarkivaren kan gi særskilt samtykke til slik lagring. Dette følgjer av arkivlova §9 bokstav b.

Arkivlova med tilhøyrande forskrifter regulerer ikkje bruken av skytenester for private personar, organisasjonar og private verksemder. Riksarkivaren kan fastsette at private rettssubjekt med offentleg tilknyting skal følge forskrift for offentlege arkiv, jf. arkivlova §§19 og 20.

Kulturdepartementet har sett i gang arbeid med revisjon av arkivforskrifta og vil i den samanhengen vurdere om det òg er behov for endringar i arkivlova. Intensjonen med arbeidet er mellom anna å tilpasse arkivregelverket til digitalisering. I samband med revisjonen ønsker departementet å vurdere behov for endring slik at offentlege organ kan ta i bruk skytenester med serverar utanfor Noreg for arkiv.

[16] Kommunal- og moderniseringsdepartementet (2015): *Kartlegging av hindringer i lovverket for bruk av skytjenester*. Rapport fra interdepartemental arbeidsgruppe med deltakelse fra Finansdepartementet, Justis- og beredskapsdepartementet, Kommunal- og moderniseringsdepartementet, Kulturdepartementet, Kunnskapsdepartementet, Nærings- og fiskeridepartementet og Samferdselsdepartementet

Riksarkivaren vurderer òg kva krav som skal stillast for å kunne gi særskilt samtykke til lagring av arkiv i skytenester med serverar utanfor Noreg. Riksarkivaren tar sikte på å ha dette klart i løpet av våren 2016.

Bokføringslova

Bokføringslova var tidlegare ei av dei lovene som la dei største hindringane i vegen for digitalisering i næringslivet, fordi lova stilte krav om fysisk lagring av rekneskap. Etter ein revisjon av lova, kan nå det meste av rekneskapsmateriale lagrast digitalt. Fordi rekneskap og fakturahandtering er område som eignar seg godt som tenester i nettskya, er krav til lagring av bokføringsdata spesielt interessant å vurdere nærare.

Bokføringslova fastset i dag at bokføringspliktige kan *«oppbevare elektronisk regnskapsmateriale i et annet EØS-land dersom avtale eller overenskomst med det aktuelle landet sikrer norske skatte- og avgiftsmyndigheter tilfredsstillende adgang til regnskapsinformasjonen i oppbevaringstiden, og slik oppbevaring ikke vil være til hinder for effektiv norsk politietterforskning.»* Av forskrifta til lova går det fram at det berre er dei nordiske landa som tilfredsstiller desse krava per i dag. Ei bedrift kan dermed lagre rekneskapsdata i ei skyteneste som er basert i Norden, dersom det er sendt melding til Skatteetaten om dette. Det kan vere vanskeleg å finne allmenne skytenester som kan garantere lagring i Norden. Dette skaper utryggleik, særleg hos mindre verksemder som ser at dei kan redusere kostnadane sine med å bruke skytenester for rekneskap og fakturabehandling.

Det er mogleg å søke dispensasjon for å lagre i andre land. Slike dispensasjonar blir gitte regelmessig for lagring av opplysningar i utlandet som ein del av ei felles rekneskapsløysing innan eit konsern eller ei liknande samanslutning. Det er eit vilkår at ein må kunne ha elektronisk tilgang til rekneskapsopplysningane frå Noreg.

Hensikta med krava til lagring er at Skattedirektoratet skal få tilgang til bokføringsdata for kontroll. Ei verksemd som ønsker å bruke skytenester som behandlar eller lagrar data utanfor Norden, kan derfor gjere dette så lenge ein kopi av rekneskapen blir overført til Noreg eller eit anna godkjent land så snart som mogleg, og seinast sju månadar etter at rekneskapsåret er slutt.

Regjeringa vil følge med på kva initiativ som kjem frå EU på dette området, og vurdere om det kjem tiltak som kan tilfredsstille krava i lova om å sikre norske styresmakter tilgang til informasjonen, slik at det kan opnast for lagring i fleire land enn i dag.

Arbeid i EU – Digital Single Market

Det finst fleire land som har liknande reglar som Noreg på dette området. EU-kommisjonen la i mai 2015 fram sin *Digital Single Market (DSM) Strategy*. Initiativ for å møte avgrensingar i den frie flyten av data innanfor EØS-området og unødige restriksjonar på lagring eller behandling av data, er ein viktig del av DSM-strategien. Rekneskap og bokføringsdata er identifisert som eit område der det ofte er krav om lagring innanfor dei enkelte landa.

Tryggingslova

Formålet med tryggingslova er å motverke truslar mot sjølvstendet og tryggleiken til staten og andre vitale nasjonale tryggleiksinteresser. I tillegg skal lova bidra til å ta i vare rettstryggleiken til den enkelte, og trygge tilliten til og kontrollen med tryggingstenesta. Lova gjeld for forvaltningsorgan, og for verksemder som leverer tryggleiksgradert utstyr og -tenester til forvaltningsorgan.

Tryggingslova og verneinstruksen stiller krav til forvaltning av informasjonssystem som gjer at det ikkje er formålstenleg å lagre slik informasjon hos utanlandske leverandørar. Det er berre Nasjonalt tryggingsorgan (NSM) som eventuelt kan godkjenne og gi tillating til bruk av slike tenester for graderte dokument. NSM må godkjenne alle informasjonssystem som skal behandle, lagre eller sende gradert informasjon. Elektroniske dokument som er omfatta av verneinstruksen skal behandlast på same måten som dokument som er gradert avgrensa etter tryggingslova.

Regjeringa har oppnemnt eit utval som skal foreslå nytt lovgrunnlag for førebyggande nasjonal tryggleik (Tryggingsutvalet). Forslaget frå utvalet skal sikre at nytt regelverk tar omsyn til teknologisk utvikling, demografiske endringar og endra tryggleikssituasjon. Utvalet skal levere rapport hausten 2016.

Særskilt om personopplysningar og teieplikt

Eit område der mange føler seg utrygge, men der regelverket i utgangspunktet ikkje legg spesielle hindringar i vegen for bruk av skytenester, er lagring av personopplysningar. Reguleringa av dette området gir likevel viktige rammer for bruken av allmenne skytenester.

Personopplysningslova fastset at personopplysningar *«kan bare overføres til stater som sikrer en forsvarlig behandling av opplysningene»*, og ein kan derfor ikkje utan vidare overføre slike data til land utanfor EØS-området. Det finst likevel ein del unntak. Blant anna kan enkeltoverføringar godkjennast på førehand av Datatilsynet, og dersom det er inngått avtale med databehandlaren gjennom standardkontraktane til EU, vil det vere lovleg grunnlag for overføring av data. I tillegg er enkelte land utanfor EU, som Canada, Australia og Sveits, godkjende av EU som trygge mottakarstatar. Tidlegare kunne ein òg overføre data til verksemder i USA som var sertifiserte etter *Safe Harbour.* Denne ordninga blei kjend ulovleg av EU-domstolen hausten 2015, men det er venta at ho blir erstatta av ei ny ordning – *EU-US Privacy Shield* (sjå tekstboks).

Etter at EU-domstolen kjende Safe Harbour-avgjerda til kommisjonen ugyldig, har ein vore nøydd til å ta spesielle omsyn når ein har inngått kontraktar som fører til at data blir overførte til USA. Fram til ei ny ordning er på plass, må ein bruke avtalar som dekker EU sine standardkontraktar for personopplysningar, og ein må varsle Datatilsynet.

Mange verksemder er usikre på om dei må ta omsyn til Snowden-avsløringane når dei skal vurdere om dei kan bruke skytenester. Til tross for den debatten avsløringane til Edward Snowden har utløyst, er ikkje norsk lovgiving eller praksis når det gjeld behandling og lagring av personopplysningar, eller andre opplysningar som er underlagde teieplikt, endra. Ulike land kan sjølve gi reglar for korleis for eksempel tryggingsorgan får tilgang til data nasjonalt for å kjempe mot terror eller kriminalitet. Det skaper utfordringar når ulike land som driv utstrakt utveksling av data har ulikt syn på kva som er greitt og ikkje når det gjeld retten til å

EU-US Privacy Shield

EU-US Privacy Shield er eit rammeverk som skal beskytte rettane til EU-borgarar når data om dei blir overførte til verksemder i USA. Det nye rammeverket vil stille strenge krav til verksemdene om å beskytte personopplysningar. I tillegg er det krav til at amerikanske styresmakter må følgje opp og handheve rammeverket.

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

Kjelde: European Commission press release: *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield*, 2. februar 2016

overvake data og kommunikasjon. Dette er ikkje noko det enkelte landet kan løyse på eiga hand; desse utfordringane må løysast på internasjonalt plan.

Ny personvernforordning i EU

EU har lenge arbeidd for å få på plass eit nytt regelverk for behandling av personopplysningar. I dag gjeld personverndirektivet innanfor EØS-området. Direktivet er implementert på ulike måtar i ulike land, og dette gjer det tungvint å tilpasse seg for verksemder som opererer i fleire ulike land, slik bedrifter som tilbyr skytenester gjerne gjer.

Ei personvern*forordning* vil, i motsetning til eit direktiv, automatisk bli lov i alle land innanfor EU, og det er sannsynleg at ho vil tatt inn i EØS-avtalen.

Landa i EU er nå einige om kva den nye forordninga skal innehalde. Dei områda av forordninga som er mest relevante for bruken av skytenester er:

- Tidligare var det den behandlingsansvarlege som hadde ansvaret dersom data gjekk tapt, uvedkommande fekk tilgang til data eller liknande. I den nye forordninga vil både behandlingsansvarleg og databehandlar få dette ansvaret. Det blir dermed eit større ansvar på skyleverandøren når denne er databehandlar.
- Det vil bli ein rett å kunne ta med seg data når ein vil skifte leverandør (krav til portablilitet). Denne retten gjeld i utgangspunktet forbrukarar, men når stadig fleire leverandørar må utvikle mekanismar for å handtere dette, er det truleg at det vil påverke forretningsmarknaden òg.
- Kundar – både forbrukarar og verksemder (og eventuelt verksemda sine kundar som er ramma) – skal bli varsla raskt etter datainnbrot eller ved tap av data.
- Data kan førast ut av EU dersom ein bruker dei ordningane som EU-kommisjonen har vedtatt.
- Forordninga gjeld for alle verksemder som er etablerte i EØS-området. Ho gjeld òg for verksemder som behandlar personopplysningar om EØS-borgarar som følge av at dei tilbyr varer og tenester i EØS-området, uavhengig av kor verksemdene er etablerte.
- Det vil bli viktigare for alle verksemder som forvaltar personopplysningar å overhalde regelverket. Dersom ein bryt reglane kan ein få gebyr på inntil 4 prosent av global årleg omsetting.

Forordninga vil truleg gjelde frå 2018.

Teieplikt

Etter forvaltningslova har *«[e]nhver som utfører tjeneste eller arbeid for et forvaltningsorgan»* teieplikt for opplysningar om personlege forhold og forretningsrelaterte opplysningar som det vil vere viktig å halde hemmeleg av konkurranseomsyn. Om ei offentleg verksemd inngår ein avtale med eit privat firma om å behandle eller lagre data, vil teieplikta òg gjelde dei i dette firmaet som eventuelt får kjennskap til informasjon som er omfatta av teieplikta. Dersom ein bruker leverandørar som igjen bruker underleverandørar, er det viktig å sikre at teieplikta er omfatta av dei avtalane som gjeld.

E-forvaltningsforskrifta seier at risikoen for ulovleg innsyn ved bruk av elektronisk kommunikasjon må *«være forebygget på tilfredsstillende måte».* Forskrifta seier òg at *«forvaltningsorganet skal opplyse generelt om hvordan taushetsbelagte opplysninger og personopplysninger sikres under behandling i forvaltningsorganet.»* Dette gjeld ved bruk av IKT generelt, og er ikkje spesielt for bruk av skytenester.

Tilsyn

Innan fleire sektorar er det behov for å kunne kontrollere IKT-systema som blir brukte i behandlinga av verksemdene sin informasjon. Ei rekke tilsynsorgan praktiserer derfor såkalla «tilsyn på staden» innan sitt ansvarsområde. Eit krav frå eit tilsyn om fysisk kontroll av IKT-systema vil vere vanskeleg å møte for verksemder som bruker skytenester. Dei fleste skyleverandørar vil for eksempel ønske å avgrense talet på personar som får sleppe inn i datasentera, fordi uautoriserte personar er ein trussel mot tryggleiken.

Krav til trygging av IKT-system og infrastruktur kan òg gjere det vanskeleg for verksemdene å avgjere om dei kan bruke skytenester eller ikkje. Krava i regelverket til trygging av IKT-system for ulike sektorar er ofte kompliserte. For verksemder som er underlagde fleire ulike sektorregelverk (for eksempel verksemder som tilbyr både kraft og kommunikasjonstenester) er det ei utfordring at krava i dei ulike sektorane ikkje er harmoniserte. Dette kjem som oftast til utrykk i samband med tilsyn og tilsyna si praktisering av eige regelverk.

Regjeringa vil sjå på tilsynsfunksjonen innan fleire sektorar samla for å vurdere forhold rundt auka bruk av skytenester. Spørsmål om praktisering av tilsyn på staden, tilsyn over landegrenser og krav til trygging av system er aktuelle tema som fleire tilsyn møter, og der det er bruk for å etablere ein felles praksis. Eit sentralt spørsmål er bruken av tredjepartsrevisjonar, og korleis ein kan sikre at dei verksemdene som gjer slike revisjonar er reelt uavhengige.

Tiltak: Fjerne utryggleik som kjem av at regelverket er uklart når det gjeld bruk av skytenester

Regjeringa vil:

- Revidere arkivforskrifta og eventuelt delar av arkivlova for blant anna å tilpasse arkivregelverket betre til digitalisering. Som ein del av dette vil ein vurdere behov for endring slik at offentlege organ kan ta i bruk skytenester med serverar utanfor Noreg for arkiv.
- Vurdere grunnlaget og handlingsrommet for å utvide tilgangen til å lagre bokføringsdata utanfor Noreg. På dette området er det òg viktige initiativ i gang i EU, som Noreg vil følge tett
- Harmonisere praksis for tilsyn så langt som mogleg, slik at verksemdene ikkje opplever motstridande krav knytte til skytenester frå ulike tilsyn

  Bidra i EU sitt arbeid med å få på plass sameinte kriterium (standardar, sertifiseringsordningar og liknande) for skytenester

4 Vilkår for bruk av skytenester i offentleg sektor

Mange verksemder er utrygge på dei juridiske rammevilkåra for bruk av skytenester.[17] Gjennomgangen av regelverk i kapittel 3 viser at det er stort rom for å bruke skytenester lovleg for verksemder i Noreg – òg innan offentleg sektor.

Prinsipp for bruk av skytenester

I tillegg til ei avklaring av regelverket, har både IKT-næringa og dei offentlege verksemdene sjølv etterlyst klare retningslinjer frå sentrale styresmakter når det gjeld bruk av skytenester.

Regjeringa har derfor etablert nokre prinsipp for bruk av skytenester i offentleg sektor:

- *Skytenester skal vurderast på linje med andre løysingar når ein står overfor større endringar eller omleggingar av IKT-system eller -drift:*
  - *ved innkjøp av nye system eller større oppgraderingar*
  - *ved større utskiftingar av maskinvare*
  - *når eksisterande driftsavtalar går ut*
- *Når skytenester gir den mest hensiktsmessige og kostnadseffektive løysinga, og det ikkje ligg føre spesielle hindringar for å ta i bruk slike tenester bør ein velje å bruke skytenester.*
- *Den valde løysinga må tilfredsstille verksemda sine krav til informasjonstryggleik. Dette krev at verksemda kjenner verdien av eigne system og data, og gjer ei risikovurdering av den valde løysinga.*

Sjølv om det kan vere fleire fordelar med å bruke skytenester, er det ikkje slik at denne typen tenester alltid er det som passar best. Det kan vere mange forhold hos ei verksemd som tilseier at andre løysingar for utvikling og drift er betre eigna for å møte dei behova verksemda har, for eksempel særskilde krav til nasjonal tryggleik, eller eksisterande system og infrastruktur i verksemda som gjer at bruk av skytenester ikkje vil vere kostnadseffektivt. Regjeringa vil derfor ikkje *pålegge* statlege verksemder å bruke skytenester, men gjennom prinsippa vil ein sikre at skytenester er med i vurderinga når statlege verksemder skal skaffe nye IKT-system eller driftsløysingar.

Prinsipp for bruk av skytenester i offentleg sektor er ein del av digitaliseringsrundskrivet frå 2016. Digitaliseringsrundskrivet er ei samanstilling av pålegg og anbefalingar om digitalisering som gjeld for alle departement, ordinære statlege forvaltningsorgan, forvaltningsorgan med særskilde fullmakter og forvaltningsbedrifter.

Digitaliseringsrundskrivet stiller blant anna krav til arkitektur og standardar for verksemder i statleg sektor.

Sjølv om kommunar og fylkeskommunar ikkje er omfatta av rundskrivet, er prinsippa eit viktig signal òg for desse, og dei kan sjølvsagt velje å følge prinsippa om dei ønsker det.

Prinsippa vil bli følgde opp med rettleiing og hjelpemiddel som skal gjere den praktiske anskaffinga av skytenester enklare for verksemdene.

[17] Nexia Management Consulting (2015): *Kartlegging og analyse av landskapet for offentlige datasenter i Norge.* Utarbeidd for Kommunal- og moderniseringsdepartementet, juni 2015

Behov for rettleiing og kontroll

Offentleg sektor har eit spesielt behov for kontroll over kven som forvaltar informasjon, og kor dette blir gjort. Kva form for kontroll, og kor sterk kontrollen må vere, vil avhenge av kva type informasjon verksemda behandlar. Det finst ulike mekanismar for å utøve slik kontroll:

Gjennom kontraktar
I ein kontrakt kan ein stille særskilde krav til behandling og lagring viss det er behov for det. Ein kan òg tenke seg at det er mogleg å bruke standardkontraktar frå leverandøren dersom desse inneheld garantiar om bruk av bestemte teknologiar eller standardar, eller oppfyller krav til ei bestemt sertifisering, som gjer at avtalen tilfredsstiller dei krava den offentlege verksemda har. Ein kan òg avtale mekanismar for revisjon og oppfølging av kontrakten, om ein har særskilt behov for dette.

Gjennom prekvalifisering av leverandørar
Ein kan tenke seg at leverandørar kan prekvalifisere seg for behandling av gitte typar informasjon, enten generelt eller for bestemte sektorar**.** KMD vil vurdere om det er mogleg og ønskeleg å etablere ein marknadsplass for skytenester retta mot offentleg sektor i Noreg. Ein slik marknadsplass vil kunne fungere som ei form for prekvalifisering av leverandørar. I Storbritannia sin marknadsplass for skytenester er det òg mogleg for verksemder å bli akkrediterte for forvaltning av informasjon som krev eit gitt tryggingsnivå.[18]

Gjennom å inngå felles avtalar på vegner av offentleg sektor
Staten kan inngå avtalar med leverandørar av datasenter/skytenester på vegner av offentleg sektor. Avtalane kan settast ut på anbod i marknaden, med krav som tilfredsstiller dei verksemdene som har dei strengaste krava til tryggleik ved behandling og lagring av informasjon. Dette er òg ei form for kontroll gjennom kontrakt, men kontrakten blir forhandla og følgt opp av sentrale styresmakter og ikkje den enkelte verksemda.

Gjennom å etablere eigne datasenter for statleg eller offentleg sektor
Ein kan tenke seg at sentrale styresmakter sjølve etablerer eit eller fleire datasenter som tilfredsstiller dei strengaste krava til tryggleik, enten for bruk i statlege verksemder eller for heile offentleg sektor.

Kommunal- og moderniseringsdepartementet har gjennom ulike møte og aktivitetar kartlagt behov for kontroll knytt til skytenester og IKT-drift i offentleg sektor. Som ein del av dette har ein undersøkt landskapet for offentlege datasenter i Noreg, saman med dei planane og behova verksemdene har for framtida.[19] Både statlege-, kommunale- og fylkeskommunale verksemder har vore med i kartlegginga. Gjennom dei aktivitetane Kommunal- og moderniseringsdepartementet har gjennomført, er det ikkje avdekka behov for at sentrale styresmakter forhandlar fram felles avtalar om datasenterdrift, eller etablerer eit felles datasenter for statleg- eller offentleg sektor. Desse alternativa er derfor ikkje drøfta nærare i strategien.

I dei undersøkingane Kommunal- og moderniseringsdepartementet har gjort, kjem det klart fram at det verksemdene treng mest, er rettleiing frå sentrale styresmakter for å sikre at dei sjølve gjer gode innkjøp, og at kontraktane dei inngår er balanserte og tilfredsstiller det norske

[18] Cabinet office (2013): *G-Cloud or PSN Service Description and Commitment for Security Accreditation*. Template Version 4.04

[19] Nexia Management Consulting (2015): *Kartlegging og analyse av landskapet for offentlige datasenter i Norge.* Utarbeidd for Kommunal- og moderniseringsdepartementet, juni 2015

regelverket. Verksemdene meiner òg at det ville vere enklare og sikrare å kjøpe skytenester om det fanst ei form for prekvalifisering, godkjenning eller akkreditering av leverandørar.

Regjeringa ønsker å etablere mekanismar som kan hjelpe verksemdene å sikre nødvendig kontroll gjennom gode innkjøp og kontraktar som tilfredsstiller offentlege krav, og oppfølging av dei inngåtte kontraktane. Som eit utgangspunkt bør inngåing av rett utforma kontraktar og oppfølging av desse vere tilstrekkeleg kontroll for verksemder som ikkje er omfatta av tryggingslova.

Kontroll gjennom kontraktar

Kontraktar er den viktigaste mekanismen for å regulere forholdet mellom kunde og leverandør. Når det gjeld skytenester retta mot forbrukarar, har det lenge vore ei utfordring at sluttbrukaravtalane er lange og vanskelege å forstå, og at det gjerne er stilt urimelege vilkår. Det er ikkje mogleg for forbrukaren å påverke korleis avtalen er utforma.

I bedriftsmarknaden er bildet meir nyansert. I denne marknaden er det òg mykje bruk av standardavtalar, ettersom det er standardiserte tenester og kjøpsprosessar som bidrar til å gjere skytenester rimelege. Det har likevel vore ein tendens mot meir balanserte avtalar enn i forbrukarmarknaden. Dette er blant anna påverka av stadig strengare krav frå offentleg sektor, og meir bevisste kundar. Det beste for alle partar er å kunne bruke standardavtalar som tilfredsstiller kunden sine krav. For at dette skal vere realistisk, er det viktig at det offentlege – helst på europeisk nivå – er einig om felles krav. Slike krav kan både vere sektorovergripande, og spesifikke for den enkelte sektoren. Fordi Noreg er eit land med tidleg adopsjon av teknologi på mange område, er vi i ein gunstig posisjon for å kunne påverke leverandørar som gjerne ønsker offentlege referansekundar. Samtidig er det viktig at Noreg òg arbeider aktivt med EU om å få på plass felles standardar og krav.

Skytenester passar dårleg inn i standardiserte rammeverk som *Statens standardavtaler (SSA).* Det vil derfor vere viktig å få på plass sjekklister som gjer at verksemder kan sjekke at leverandøren sine standardkontraktar ikkje bryt med norsk regelverk, og at dei dekker dei same områda som staten sine standardavtalar. Utvikling av slike sjekklister vil vere ein del av rettleiingsarbeidet til Difi (sjå under).

Det er sjølvsagt mogleg å bruke skytenester sjølv om ein har særskilde krav og treng å forhandle fram eigne avtalevilkår. Prosessen med å kjøpe inn skytenesta vil då bli meir som ein tradisjonell innkjøpsprosess.

Enten ein bruker ein standardavtale eller har forhandla fram eigne vilkår, er det viktig å sikre at ein har mekanismar for å følge opp kontrakten. Ein slik mekanisme kan vere bruk av ein uavhengig tredjepart til å gjennomføre revisjonar for å sjekke at leverandøren overheld dei vilkåra som ligg i kontrakten. Det er viktig å sikre at slike tredjepartar er reelt uavhengige frå leverandøren.

Rettleiing hos Direktoratet for forvaltning og IKT (Difi)

Kommunal- og moderniseringsdepartementet vil gi Difi i oppdrag å etablere eit kompetansemiljø og ein nettbasert ressurs der verksemder som ønsker å kjøpe inn skytenester, kan få rettleiing. På sikt er det ønskeleg at rettleiinga kan vere tilpassa ulike typar målgrupper som har liknande krav og behov, og spesielle sektorbehov.

Ein slik ressurs må dekke alle ledda i innkjøpsprosessen, og ikkje berre dei juridiske problemstillingane som er knytte til sjølve innkjøpet. Aktuelle problemstillingar og oppgåver kan vere:

- Korleis gjennomføre innkjøpsprosessen på ein korrekt måte når ein trur at ei skyteneste vil vere det beste alternativet?
- Risikovurderingar tilpassa kompleksiteten og behova til ulike typar verksemder – gjerne med eksempel på beste praksis.
- Krav til databehandlaravtalar
- Rettleiing i å sette opp ein kostnad-nytte-analyse for bruk av skytenester.
- Beste praksis på valde løysingar – gjerne med eksempel innanfor ulike typar representative verksemder, som grunnskule, kommuneadministrasjon eller fastlegekontor.
- Korleis kan ein sikre oppfølging av kontraktane gjennom for eksempel tilsyn og uavhengige tredjepartsrevisjonar?

I utgangspunktet vil tilbodet frå Difi vere retta mot offentlege verksemder – inkludert kommunane – og indirekte leverandørar til offentleg sektor. Det er samtidig klart at det òg er behov for denne typen ressurs i næringslivet, særleg for små og mellomstore bedrifter. Difi sine ressursar for det offentlege vil kunne danne modell for ei tilsvarande rettleiing retta mot næringslivet, for eksempel i regi av ein eller fleire bransjeorganisasjonar.

Sektorvise vurderingar av informasjon

Offentleg informasjon kan delast inn i tre kategoriar:[20]

1. informasjon som berre bør lagrast i Noreg
2. informasjon som kan lagrast i utlandet, men som ein kan ta heim når det er særleg behov for det, og på bestemte vilkår
3. informasjon som kan lagrast i utlandet utan vilkår

Det er den enkelte sektoren som er best eigna til å vurdere kva for informasjon som fell inn under dei ulike kategoriane. Fleire sektorar er allereie i gang med å ta stilling til krav ved bruk av skytenester eller med å utarbeide rettleiarar for sektoren. Regjeringa vil be alle sektorstyresmakter om å sørge for å få utarbeidd ei vurdering av informasjonen i sektoren og korleis denne kan behandlast i nettskya.

For enkelte sektorar er det truleg personopplysningslova som avgjer kva kategori informasjonen fell inn under. Personopplysningar vil hamne i kategori 2 eller 3, så framt EU sine krav til overføring av personopplysningar til utlandet er tilfredsstilte. Datatilsynet har utarbeidd gode rettleiarar for lagring og behandling av personopplysningar i skya. For andre kan det vere eigne sektorregelverk som speler inn, slik som helseregisterlova eller beredskapsforskrifta for kraftforsyninga. Slike sektorar må gjere eigne analysar baserte på eigen informasjon og eigne behov. I slike analysar må ein òg vurdere kva omstende som kan krevje at ein tar informasjonen heim, korleis dette er regulert i kontrakten med leverandøren, og korleis ein kan gjennomføre det i praksis.

[20] NOU 2015:13 *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden*

Skjermingsverdig informasjon er truleg den viktigaste informasjonstypen som vil falle inn under kategori 1, men ein kan òg tenke seg at enkelte sektorar eller verksemder kan vurdere annan type informasjon som så kritisk at ein vurderer lagring i Noreg som einaste alternativ.

For verksemdene som treng rettleiing er det viktig at det finst ein autoritativ ressurs der ein veit at informasjonen om klassifisering av data er oppdatert og korrekt, uavhengig av sektor. Difi si rolle som rettleiar bør derfor òg omfatte koordinering og samling av arbeidet i dei ulike sektorane. Dette arbeidet bør utførast i nært samarbeid med NSM.

Krav til sertifiseringar

Det finst ei lang rekke sertifiseringsordningar som er relevante for skytenester. I tillegg finst det krav både frå EU og frå enkeltland som mange av leverandørane vel å følgje. Slike krav kan vere:

- internasjonale standardar som ISO 27001
- krav frå styresmakter, slik som EU sine standardkontraktar og «EU-US Privacy Shield»
- standardar som ikkje er internasjonale, men som er blitt aksepterte som de facto standardar på sitt område, for eksempel FedRAMP, SOC, UK G-Cloud og Singapore MTCS
- standardar som er knytte til spesifikke sektorar, slik som HIPAA (helse), FISC (finans) og PCI DSS (betalingskort)

Dei store skyleverandørane, som Google, Amazon og Microsoft, har stort sett alle sertifiseringane. Mindre leverandørar har gjerne valt seg ut sertifiseringar som er spesielt relevante for deira sektor eller for den marknaden dei først og fremst retter tenestene sine mot. Det er dyrt for mindre leverandørar å bli sertifiserte – og å oppretthalde sertifiseringane – på så mange område. Derfor er det ønskeleg med eit mindre, sameint sett standardar som alle kan ta utgangspunkt i.

Vi veit at felles europeiske krav – for eksempel til behandling av personopplysningar eller til sertifiseringar innan tryggleik – gjerne fører til at skyleverandørar tilpassar tenestene og standardavtalane sine slik at dei møter desse krava. Dette gjer det enklare for verksemdene å vurdere tenestene. Regjeringa ønsker derfor å bidra i EU sitt arbeid med å få på plass sameinte kriterium for skytenester på ulike nivå.

Regjeringa vil òg stille krav om at leverandørar til offentleg sektor i Noreg har relevante sertifiseringar eller kan dokumentere at dei oppfyller dei standardane som er sette for den sektoren dei leverer tenester til. Dei enkelte sektorane må vurdere kva standardar eller sertifiseringar som bør gjelde på deira område, såframt det er relevant. Difi får ansvaret for å koordinere dette arbeidet.

Eksempel på standardar og sertifiseringar

ISO 27001:	ISO 27001:2013 spesifiserer eit styringssystem for informasjonstryggleik. Denne standarden ligg til grunn for dei fleste sertifiseringsordningar.
ISO 27018:	ISO 27018:2014 spesifiserer retningsliner for vern av personopplysningar i den allmenne skya etter at ein har gjennomført ei vurdering av personvernrisikoen. Det finst p.t. inga publisert standard for å gjere slike vurderingar.
SOC1, SOC2, SOC3:	Service Organization Control-rapportering. Rapportar utvikla av organisasjonen for sertifiserte amerikanske revisorar (AICPA). SOC1 rapporterer på finansielle data. SOC2 tar føre seg kontrollmekanismar som er meir spesifikke for datalagring og -behandling, slik som tryggleik, tilgjenge, behandlingsintegritet, konfidensialitet og personvern. SOC3 omfattar dei same elementa som SOC2, men er meir overordna og mindre teknisk.
FedRAMP:	Federal Risk and Authorization Management Program. Standardisert tilnærming til verifisering av tryggleik, autorisasjon og overvaking i sky-tenester som blir brukte av føderale byrå i USA.
UK G-Cloud:	Verksemder som ønsker å bli akkrediterte for eit høgre tryggingsnivå i Storbritannia sitt rammeverk, G-Cloud, kan søke om dette. Det er National Technical Authority for Information Assurance (CESG) som står for akkrediteringa.
MTCS:	Multi-Tier Cloud Security. Frå Singapore. Open sertifiseringsordning for skyleverandørar, basert på ISO 27001. Tre tryggingsnivå, Tier 1 til Tier 3, der Tier 3 oppfyller strenge krav til informasjonstryggleik. Sertifiseringa blir gjort av uavhengige sertifiseringsorgan som DNV-GL og British Standards Institution (BSI).
HIPAA:	The Health Insurance Portability and Accountability Act. Amerikansk lov som regulerer behandling av pasientinformasjon. Ein uavhengig tredjepart sjekkar om databehandlaren overheld krava i lova.
FISC:	Center for Financial Industry Information Systems. Frå Japan. Retningsliner for tryggleik i finansielle informasjonssystem.
PCI DSS:	Payment Card Industry Data Security Standard. Global sertifiserings-standard for organisasjonar som behandlar betalingskorttransaksjonar.

Eksempel: UK Cloud Store – Digital Marketplace

Cloud Store er eit rammeverk for skytenester retta mot offentleg sektor i Storbritannia. Rammeverket fungerer slik at det med faste intervall (kvar 6. til 9. månad) blir opna for at leverandørar kan registrere seg.

På ei eiga nettside registrerer leverandøren informasjon om verksemda si, kva tenester han kan tilby, og til kva pris. Tenesta må tilfredsstille skytenestedefinisjonen til NIST. Leverandøren legg òg inn informasjon om seg sjølv og om måten tenesta blir levert på, kva tryggingsnivå verksemda er godkjend for, med meir. Dette er i hovudsak basert på sjølvdeklarering. Godkjenning av verksemder for eit gitt tryggingsnivå blir gjort av den britiske ekvivalenten til NSM.

Dei offentlege kundane kan gå inn i Cloud Store og søke etter leverandørar. Dei kan be om meir informasjon, for eksempel om dei har spesielle krav til tryggleik. Dei kan òg velje leverandør direkte, utan å gjennomføre ein tradisjonell prosess for anskaffing. Styresmaktene i Storbritannia reknar vilkåra for offentlege innkjøp som tilfredsstilte gjennom utlysinga til registrering i rammeverket. Prisane i rammeverket er transparente, slik at tilbydarane kan endre prisane sine for å vere konkurransedyktige.

Ein viktig tanke bak Cloud Store er at det skal vere enklare for små og mellomstore selskap å konkurrere om offentlege kontraktar.

Kjelde: UK Cabinet Office – Government Digital Service

Marknadsplass for skytenester retta mot offentleg sektor

Regjeringa ønsker ei form for prekvalifiserings- og/eller akkrediteringsordning for leverandørar av skytenester. Kommunal- og moderniseringsdepartementet vil greie ut moglege modellar for ein marknadsplass for skytenester retta mot offentleg sektor og vurdere om dette er aktuelt å innføre i Noreg. Ein eventuell marknadsplass vil vere eit tiltak for å gjere det enklare for verksemdene å vurdere skytenester som eit alternativ når dei skal skaffe nye IKT-system, og kan blant anna omfatte mekanismar for sjølvdeklarasjon, prekvalifisering og/eller akkreditering for ulike tryggingsnivå. Utgreiinga skal gjennomførast i 2016.

Krav til samordning ved etablering av nye datasenter

Verksemder eller sektorar som vurderer at dei har informasjon som fell inn under kategori 1), informasjon som bør lagrast i Noreg, kan tenke seg å ville etablere eit eige datasenter, eventuelt kjøpe tenester frå ein (norsk) leverandør som kan levere særskilt sikre tenester.

I slike tilfelle ønsker regjeringa å legge til rette for betre utnytting av eksisterande datasenterressursar i offentleg sektor. Verksemder som har eit særleg behov for sikre tenester, skal vurdere om det er mogleg å utnytte ledig kapasitet hos – eller gå i samarbeid med – andre verksemder med tilsvarande behov. Dette krev ei oversikt over innrettinga og kapasiteten i offentlege datasenter, først og fremst i statleg sektor. Difi vil få ansvar for å vurdere korleis ei slik ordning kan settast ut i livet.

Eksempel: Skyscape

I Storbritannia har aktørar i marknaden etablert eit datasenter som møter behova til statlege verksemder med særleg strenge krav til tryggleik. *Skyscape* er ein leverandør av infrastrukturtenester (IaaS) i det britiske G-cloud-rammeverket. Utgangspunktet for Skyscape er ein allianse av ulike leverandørar: det delvis statseigde forsvarsindustri-selskapet QinetiQ, VMWare, Cisco, EMC og Ark Data Centres. Selskapet sine datasenter- og skytenester er akkrediterte av britiske styresmakter for data opp til «official – sensitive». Skyscape er òg akkreditert av *The Health and Social Care Information Centre* (HSCIC) til å levere tenester til den britiske helsetenesta NHS.

Skyscape blir ikkje brukt av statlege verksemder med lågare krav til tryggleik. Skatt og toll i Storbritannia (HMRC) har for eksempel valt Google Apps i ei skyløysing for kontorstøtte. Som ein del av avtalen har dei godtatt at data kan lagrast i Google sine datasenter utan-for Storbritannia.

Kjelder: Skyscapecloud.com, digi.no, Financial Times

System som behandlar gradert og skjermingsverdig informasjon, inkludert elektroniske dokument som er omfatta av verneinstruksen, må i utgangspunktet vere lokaliserte i Noreg. Verksemder som er underlagde tryggingslova, vil måtte gjere særskilde vurderingar dersom dei ønsker å bruke tenester frå den allmenne skya. For desse er det naturleg å søke råd hos NSM.

Tiltak: Gjere det enklare for offentlege verksemder og næringsliv å vurdere skytenester som alternativ når dei skal skaffe nye IKT-tenester

Regjeringa vil:

- Etablere eit rettleiings- og kompetansemiljø som kan støtte verksemdene når dei skal vurdere, og eventuelt kjøpe inn, skytenester:
  - På kort sikt vil ein samle og legge til rette eksisterande materiell for rettleiing ved innkjøp av skytenester.
  - På lengre sikt skal det byggast opp eit miljø og utviklast meir omfattande ressursar for rettleiing ved innkjøp av skytenester i offentleg sektor. Viktige område der det er bruk for rettleiing, er verdivurdering av informasjon, risikovurderingar og informasjonstryggleik. Arbeidet må koordinerast med dei vurderingane av informasjon og utvikling av rettleiarar som blir utførde i sektorane.
  - Miljøet vil komme med anbefalingar til sertifiseringar eller bruk av standardar som leverandørar av skytenester til gitte sektorar bør oppfylle. Dei enkelte sektorane må vurdere kva standardar eller sertifiseringar som bør gjelde på deira område.
  - Det er naturleg at dette miljøet blir etablert hos Difi, og at arbeidet inngår som ein del av rettleiinga Difi gir innan IKT-innkjøp. Kompetansemiljøet vil ta initiativ til samarbeid med relevante organisasjonar for næringslivet, slik at dei – om dei ønsker – kan utnytte Difi sine ressursar til rettleiing mot eigne verksemder
- Gi Kommunal- og moderniseringsdepartementet i oppdrag å undersøke og vurdere ulike modellar for ein mogleg marknadsplass/innkjøpsordning for skytenester retta mot offentleg sektor.
- Legge til rette for betre utnytting av eksisterande offentlege datasenterressursar for dei verksemdene som har behov for så sterk kontroll at dei vurderer å kjøpe tenester eller etablere sitt eige datasenter i Noreg. I slike tilfelle skal verksemda vurdere om det er mogleg å utnytte ledig kapasitet hos – eller gå i samarbeid med – andre verksemder med tilsvarande behov. Dette krev ei oversikt over innrettinga og kapasiteten i eksisterande datasenter, først og fremst i statleg sektor. Difi vil få ansvar for å vurdere korleis ei slik ordning kan realiserast.

Utgitt av:
Kommunal- og moderniseringsdepartementet

Publikasjonskode: H-2365

Omslagsfoto: Jan Hausken/KMD
Omslag: Service- og tryggingsorganisasjonen til departementa 05/2016