FØYEN TORKILDSEN ADVOKATFIRMA

Sjekkliste ved anskaffelse av skybaserte løsninger

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

KS FoU

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

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

	SJEKKLISTE	KOMMENTAR
3	Sjekk hvordan tap av data reguleres i kontrakten. Ofte tar ikke leverandøren ansvar for dette overhodet. Det må vurderes om dette er akseptabelt for din virksomhet. Verdt å merke seg for kommuner er at for dårlig sikring mot eventuelt tap av data vil kunne komme i konflikt med plikten til å oppbevare visse kategorier av data i en gitt periode.	
4	Sjekk om avtalen gir leverandøren mulighet til leveransenekt ved manglende betaling (selv om betalingsmisligholdet ikke er vesentlig). Mange leverandører opererer med slike krav, noe som kan skape utfordringer om avtalen ikke endres på dette punkt.	