Cloud computing:

Rettslige utfordringer ved bruk av nettskyen

Temaet for denne artikkelen er det rettslige rammeverket for nettskyen, og hvilke juridiske utfordringer en virksomhet må være oppmerksom på når den vurderer bruk av nettskyen.

Artikkelen er forfattet av:

Advokatfullmektig
Cato Løwer
Arntzen de Besche

Advokat
Espen Sandvik
Partner Arntzen de Besche

Et stadig vanligere fenomen er at private og offentlige virksomheter tar «nettskyen» i bruk for å dekke sine IT-behov. Nettskyen – eller cloud computing – er eksterne serverparker tilknyttet internett som tilbyr datalagring av informasjon, dataprosessering og programvare til private og offentlige virksomheter.[1] Fordelene med nettskyen er blant annet at virksomheten ikke trenger å foreta store investeringer i IT-infrastruktur, at virksomheten lettere får tilgang til den seneste programvaren på markedet, og at mye komplisert IT-arbeid blir overlatt til nettskyleverandøren. Til tross for disse fordelene har enkelte uttrykt skepsis til nettskyen, særlig med tanke på virksomhetskritiske data og funksjoner. Det er først og fremst faren for at informasjon vil komme på avveie, eksempelvis ved hacking eller en uredelig ansatt hos nettskyleverandøren, som kan tale mot nettskyen. Et annet aspekt ved nettskyen er den kontrollutfordringen som ligger i at data ikke bare lagres eksternt hos en tjenesteleverandør, men også kan flyttes fra sted til sted og fra land til land. Dette gjøres av hensyn til mest mulig hensiktsmessig utnyttelse av leverandørens lagringskapasitet. Konsekvensen er at eier av dataene ofte ikke vet hvor i verden dataene befinner seg.

Nettskyens mange fordeler gjør at den uansett er kommet for å bli, og vil utgjøre en sentral del av IT-løsningene til svært mange virksomheter i tiden fremover. EU-kommisjonen vedtok i september 2012 en strategi for «Unleashing the Potential of Cloud Computing in Europe», der økt bruk av nettskyen ble uttalt som en målsetning. Dette vil ifølge kommisjonen kunne føre til økt produktivitet, vekst og sysselsetting i Europa. Kommisjonen viser også til mulige miljøeffekter ved bruk av nettskyen i form av redusert energiforbruk, og undersøkelser fra USA, som tilsier at amerikanske selskaper kan spare USD 12 milliarder årlig i energikostnader ved å gå over til bruk av nettskyen.

Nettskyen reiser også en rekke *rettslige* problemstillinger. Bruken kan i enkelte sammenhenger være ulovlig. Det er fort gjort å overse dette, ettersom nettskytjenester er enkelt tilgjengelig, og tilbys uten advarsler om regulatoriske krav. Det er da

KOMMET FOR Å BLI: Nettskyen er kommet for å bli, og vil utgjøre en sentral del av IT-løsningene til svært mange virksomheter i tiden fremover.

1 Veilederen til Datatilsynet, side 4 (www.datatilsynet.no). Privatpersoner kan også bruke nettskyen, men vi går ikke inn på de rettslige problemstillingene som oppstår for dem.

heller ikke tjenesten som sådan som er problemet, men nettskykundens bruk av denne til bestemte typer databehandling.

Det rettslige rammeverket kan deles inn i to kategorier. Den første kategorien er de restriksjonene og kravene som følger av ufravikelig *lovgivning*. Den andre kategorien er *avtalen* som inngås mellom nettskyleverandøren og virksomheten. Ofte vil det være et nært samspill mellom disse to kategoriene. Personopplysningsloven stiller eksempelvis krav til hva avtalen mellom nettskyleverandøren og nettskykunden må inneholde med hensyn til lagring av personopplysninger.

Når det gjelder lovgivningen, er det særlig personopplysningsloven som setter begrensninger for bruken av nettskyen. Svært ofte vil bruk av nettskyen innebære at nettskykunden overfører personopplysninger til nettskyleverandøren. De problemstillingene dette reiser, behandles i neste punkt. Øvrige regulatoriske problemstillinger oppstår i forbindelse med lovpålagte *oppbevaringsplikter* i blant annet bokføringsloven og arkivloven, samt forskjellige former for taushetsplikt og krav til sikring av data. Spørsmålet blir da om oppbevaring i nettskyen er i samsvar med disse pliktene (omtales senere i artikkelen), eller om regelverket krever at oppbevaringen skjer på annen måte. Det kontraktsrettslige forholdet mellom nettskyleverandøren og nettskykunden reiser egne problemstillinger, og omtales i punktet «Det kontraktsrettslige forholdet til nettskyleverandøren».

Hvilke krav stiller personopplysningsloven til nettskyen?[2]

Hvorfor personopplysningsloven er relevant

Personopplysningsloven vil være relevant for nettskybruk av to årsaker: dels begrenser loven adgangen til overhodet å behandle personopplysninger, dels stiller den krav til hvordan personopplysningene skal behandles. Med behandling av personopplysninger menes både innsamling, lagring, utlevering og overføring av slike opplysninger, jf. lovens § 2 nr. 2 og § 3 første ledd bokstav a. Bruk av nettskyen kan innebære både overføring og lagring av personopplysninger, og faller derfor inn under lovens virkeområde. Begrepet «personopplysning» er svært vidt, og dekker alle «opplysninger og vurderinger som kan knyttes til en enkeltperson», jf. § 2 nr. 1. I praksis vil svært mye av den informasjonen som lagres i nettskyen, inneholde en eller flere personopplysninger. Typiske eksempler er kundedata og informasjon om virksomhetens ansatte. De personvernrettslige aspektene ved nettskyen må derfor vurderes før personopplysningene overføres til nettskyen.

Ansvarsfordelingen mellom nettskykunden og nettskyleverandøren

I personopplysningslovens terminologi vil nettskykunden anses som «behandlingsansvarlig», mens nettskyleverandøren normalt anses som «databehandler», jf. § 2 nr. 4 og 5. Et viktig poeng i denne sammenhengen er at nettskykunden ikke blir fritatt for sitt ansvar ved å inngå en avtale med nettskyleverandøren. Hovedansvaret for overholdelse av personopplysningsloven ligger fortsatt hos

2 Hvis det er tale om helseopplysninger, er det også viktig å undersøke reglene i helseregisterloven.

nettskykunden. Dette betyr at nettskykunden risikerer å havne i ansvar som følge av at nettskyleverandøren ikke overholder personopplysningsloven. Straffansvar og erstatningsansvar utenfor kontrakt vil imidlertid forutsette at nettskykunden selv har vært uaktsom.[3] Det vil som den klare hovedregel ikke være tilfellet dersom valget av databehandleren (nettskyleverandøren) er forsvarlig, og det foreligger en avtale som tilfredsstiller kravene i personopplysningsloven (blant annet med hensyn til sikringstiltak, jf. punktet «Kravet til sikringstiltak» nedenfor). Hvis nettskyleverandøren opptrer som en kontraktsmedhjelper for nettskykunden overfor sistnevntes kontraktsparter, vil imidlertid nettskykunden identifiseres med sin underleverandørs (nettskyleverandørens) feil etter alminnelige kontraktsrettslige prinsipper.

Plikten til å inngå databehandleravtale med nettskyleverandøren

Nettskytjenester vil i praksis reguleres i en avtale, jf. punktet om «Det kontraktsrettslige forholdet til nettskyleverandøren» nedenfor. Hvis nettskytjenesten innbefatter lagring av personopplysninger, vil en slik avtale også være en nødvendighet av regulatoriske årsaker. Personopplysningsloven krever at behandlingsansvarlig (nettskykunden) og databehandleren (nettskyleverandøren) inngår en avtale om hvordan personopplysningene skal behandles. Plikten til å inngå en databehandleravtale fremgår ikke direkte av loven, men følger forutsetningsvis av personopplysningsloven § 15 første ledd. Bestemmelsen sier at databehandleren ikke kan «behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige».

En rekke forhold må nedfelles i databehandleravtalen. Datatilsynet har skrevet en veileder om hvilke *minimumskrav* som skal være med i en databehandleravtale.[4] Her nevnes noen hovedpunkter: formålet med bruken av personopplysningene skal være beskrevet, hvorvidt opplysningene skal oppbevares som et arkiv eller også bearbeides, om opplysningene skal slettes eller tilbakeføres etter at kontraktsperioden løper ut og at databehandleren plikter å holde personopplysningene adskilt fra den resterende informasjonen han besitter.

Personopplysningsloven § 15 første ledd sier videre at opplysningene heller ikke kan «overlates til noen andre for lagring eller bearbeidelse» uten en databehandleravtale. Hvis det er aktuelt at nettskyleverandøren skal benytte underleverandører, må avtalen derfor eksplisitt bemyndige nettskyleverandøren til dette.

Plikten til å nedfelle forhold som nevnt i databehandleravtalen må sees i sammenheng med personopplysningsloven § 14. Bestemmelsen forplikter den behandlingsansvarlige til å «etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene» i personopplysningsloven og dens forskrifter. I praksis fungerer databehandleravtalen som en instruks fra nettskykunden til nettskyleverandøren for å sikre at kravene i personopplysningsloven overholdes.

Et annet viktig element i databehandleravtaler er kravet til sikringstiltak. Personopplysningsloven § 15 annet ledd sier at databehandleravtalen skal forplikte databehandleren (nettskyleverandøren) til «å gjennomføre slike sikringstiltak som følger av § 13».

Kravet til sikringstiltak

Ifølge personopplysningsloven § 13 første ledd skal den behandlingsansvarlige og databehandleren «gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger». Personopplysningsforskriften kapittel 2 inneholder en nærmere utdyping av kravene til informasjonssikkerhet. Reglene er forholdsvis omfattende, og får også anvendelse ved behandling av personopplysninger i nettskyen. Det stilles blant annet krav til at det skal foretas en risikovurdering for å klargjøre sannsynligheten for og konsekvensene av et sikkerhetsbrudd (§ 2–4), at det jevnlig skal foretas sikkerhetsrevisjon av bruk av informasjonssystemet (§ 2–5), at det skal treffes tiltak som sikrer konfidensialitet (§ 2–11), at det skal treffes tiltak for å sikre tilgang til personopplysninger hvor tilgjengelighet er nødvendig (§ 2–12) og at det skal foreligge sikkerhetstiltak som skal hindre uautorisert bruk av informasjonssystemet (§ 2–14).

Kapittel 2 om informasjonssikkerhet bygger på et forholdsmessighetsprinsipp. De planlagte og systematiske tiltakene som treffes i medhold av forskriften, skal «stå i forhold til sannsynligheten for og konsekvens av sikkerhetsbrudd», jf. § 2–1. Hvilke tiltak som er nødvendig i det enkelte tilfellet, må bero på en konkret vurdering. Dette vil blant annet bero på hva slags personopplysninger som behandles, herunder om det gjelder sensitive opplysninger.

I praksis må vurderingen av sikkerhetstiltakene ved bruk av nettskyen gjøres på bakgrunn av de opplysninger nettskyleverandøren gir om sine systemer og rutiner med tanke på sikkerhet. Dersom opplysningene fra nettskyleverandøren ikke gir grunnlag for en slik vurdering, må ytterligere informasjon etterspørres.

Plikten til å informere om bruken av nettskyen

Personopplysninger kan innhentes direkte fra den opplysningene angår, eller fra andre kilder. Dersom personopplysningene innhentes fra den opplysningene angår, krever personopplysningsloven § 19 at vedkommende gis nærmere informasjon om bruken av personopplysningene. Den registrerte skal informeres om navn og adresse på den behandlingsansvarlige og dennes eventuelle representant, formålet med behandlinger, hvorvidt opplysningene vil bli utlevert og hvem som er mottaker, at det er frivillig å gi fra seg opplysningene og at den registrerte skal bli gitt den informasjonen som gjør vedkommende i stand til å bruke rettighetene etter personopplysningsloven på best mulig måte.

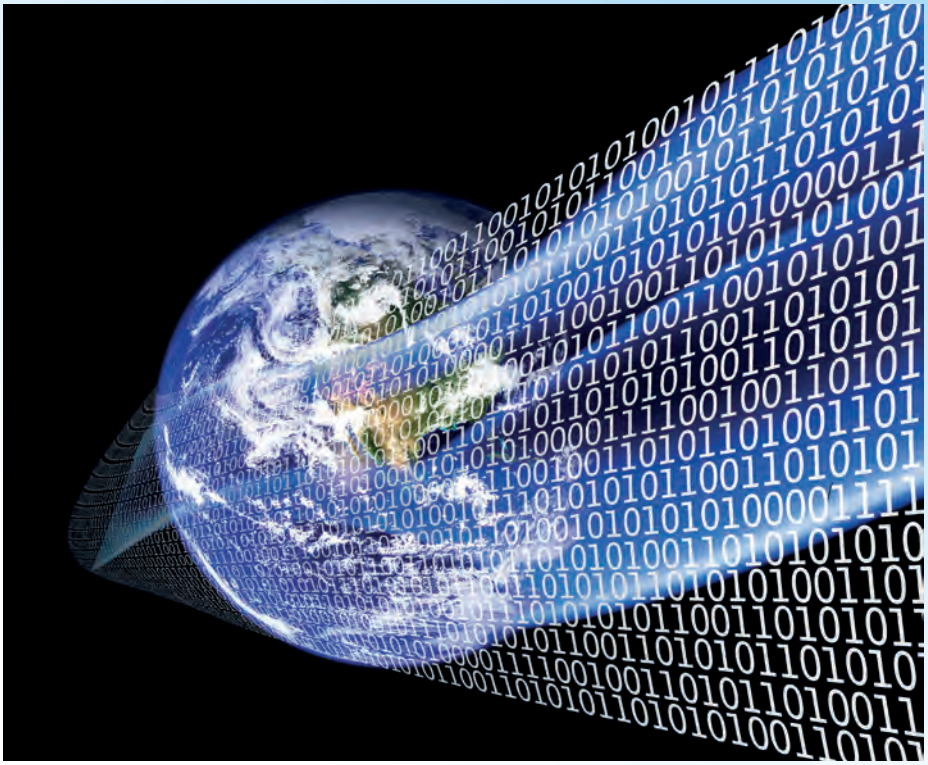
Varsel er ikke nødvendig «dersom det er på det rene at den registrerte allerede kjenner til informasjonen», jf. § 19 annet ledd. «På det rene» betyr at den registrerte må ha faktisk kjennskap til informasjonen; det er ikke tilstrekkelig at han «antas å ha» eller «burde ha» kjennskap til informasjonen.

Begrensninger i adgangen til å overføre personopplysninger til utlandet

Svært ofte vil nettskyens servere befinne seg utenfor Norge. Dette innebærer at personopplysninger føres ut av landet, enten som del av hovedlagringen, eller i forbindelse med back-up løsninger.

Utgangspunktet er at overføring av personopplysninger til utlandet ikke er tillatt, med mindre det er til land som «sikrer en forsvarlig behandling av opplysningene», jf. § 29 første ledd. Det omfatter alle landene i EU/EØS, samt noen få godkjente «tredjeland», som blant annet

3 Personopplysningsloven §§ 48 og 49.
4 datatilsynet.no/Sikkerhet-internkontroll/Databehandleravtale/



SIKRER FORSVARLIG BEHANDLING: Overføring av personopplysninger til utlandet er i utgangspunktet ikke er tillatt, med mindre det er til land som «sikrer en forsvarlig behandling av opplysningene».

Argentina, Canada og Sveits. USA anses i sin alminnelighet ikke for å ha et tilfredsstillende beskyttelsesnivå. Gjennom den såkalte «Safe Harbor»-ordningen kan personopplysninger likevel overføres til virksomheter i USA som er «Safe Harbor-sertifisert».

Personopplysningsloven § 30 oppstiller enkelte unntak fra kravet i § 29 om at mottakerstaten må sikre en forsvarlig behandling av personopplysningene. Overføring til land med dårligere beskyttelse av personvernet er blant annet tillatt hvis den registrerte samtykker.[5] Et slikt samtykke må være frivillig, uttrykkelig og informert,[6] hvilket blant annet innebærer at vedkommende må gis tilstrekkelig informasjon om overføringen til å forstå hva han samtykker til. Det er verdt å merke seg at det ikke er nettskykunden som skal gi et slikt samtykke, men den personopplysningene gjelder. En virksom-

5 Et problem med å anvende samtykke-unntaket er at arbeidet med å skaffe de nødvendige samtykker kan være kostnadskrevende. Det kan formodentlig løses ved at ansettelses- og kundeavtalene eksplisitt angir at personopplysninger kan bli overført til en nettsky.

6 Personopplysninglovens § 2 nr. 7.

het må derfor ha tilstrekkelige rutiner og systemer for å innhente de nødvendige samtykker fra sine kunder, ansatte osv.

Overføring av data til en databehandler (nettskyleverandør) utenfor EU/EØS og godkjente tredjeland er dessuten tillatt dersom behandlingsansvarlig/oppdragsgiver og databehandler/nettskyleverandøren har inngått EUs standardkontrakt for overføring inntatt i kommisjonsbeslutning 2010/87/EU datert 5. februar 2010, jf. personopplysningsforskriften § 6–3. Denne avtalen kan inngås som en del av avtaleverket mellom oppdragsgiver og nettskyleverandør. Den behandlingsansvarlige må varsle Datatilsynet om overføringen ved innsending av utfylt og signert standardkontrakt. Overføringen til nettskyen i utlandet kan først finne sted når slikt varsel er sendt.

Det må understrekes at de spesifikke reglene om overføring til utlandet kommer i tillegg til de generelle betingelsene som gjelder for enhver databehandling. Behandlingen (overføringen til utlandet/bruken av nettskyen) må ha et saklig begrunnet formål og et gyldig behandlingsgrunnlag, jf. personopplysningsloven §§ 8, 9 og 11.

Hindrer arkivloven offentlige virksomheter i å bruke nettskyen?

Statlige, fylkeskommunale og kommunale institusjoner og enheter er forpliktet til å ha arkiv over dokumenter som har blitt til i deres virksomhet. Arkivet «*skal vera ordna og innretta slik at dokumenta er tryggja som informasjonskjelder for samtid og ettertid*», jf. arkivloven § 6. Arkivmaterialet skal videre ikke «*førast ut or landet, dersom dette ikkje representerer ein naudsynt del av den forvaltningsmessig eller rettslege bruken av dokumenta*», jf. arkivloven § 9 bokstav b.

Spørsmålet er om dette er til hinder for at offentlige virksomheter benytter nettskyen.

Riksarkivaren avga høsten 2014 en uttalelse i en pressemelding hvor han konkluderte med at arkivloven § 9 bokstav b krever at arkivdatabasen skal være lagret og tilgjengelig på server som er fysisk plassert i Norge.[7] Riksarkivaren var også av den oppfatning at sikkerhetskopien heller ikke kunne lagres i utlandet. Riksarkivarens begrunnelse er «*At arkivmaterialet er tilgjengeleg frå Noreg via Internett er etter vårt skjønn ikkje tilstrekkeleg, fordi det ikkje vil gi god nok kontroll, med ei rekkje risikofaktorar*». Riksarkivarens forståelse av loven er ikke rettslig avgjørende. I praksis må den likevel legges til grunn, ettersom Riksarkivaren har veilednings- og tilsynsansvaret for arkivarbeidet i offentlige organer, jf. arkivloven § 7.

Trolig rammer arkivloven § 9 bokstav b bare forholdsvis varig lagring i utlandet.[8] Basert på en slik tolkning vil nettskytjenester som medfører en *midlertidig lagring* av informasjon, falle utenfor forbudet i arkivloven § 9 bokstav b.

Arkivloven § 9 bokstav b har uansett vesentlige implikasjoner. Den hindrer at kommuner med anstrengt økonomi benytter utenlandske nettskyer for å redusere IT-kostnadene ved varig lagring. Arkivloven ble vedtatt på et tidspunkt der lagring i nettskyer ikke var et aktuelt tema. Restriksjonene er etter vårt syn dårlig begrunnet ut fra dagens løsninger. Et arbeid med endring av lovverket er påbegynt, se punktet «Avslutning» til slutt i artikkelen.

Private virksomheter er ikke underlagt arkivloven, men kan ha andre arkiveringsforpliktelser som kan reise spørsmål ved bruk av nettskyen, se nærmere nedenfor.

Kan plikten til oppbevaring etter bokføringsloven overholdes ved bruk av nettskyen?

Bokføringsloven § 13 krever i utgangspunktet at regnskapsmateriale skal oppbevares i Norge. Materialet skal i henhold til § 13 tredje ledd oppbevares slik at det er «sikret mot ødeleggelse, tap og endring». Regnskapsmaterialet skal videre oppbevares i sin originale utforming. Nettskybruk reiser spørsmål for alle disse vilkårene.

De fleste av dagens nettskytilbud er såpass sikre at de tilfredsstiller kravene til sikkerhet mot ødeleggelse og tap, mm. Hvorvidt kravet til sikkerhet er oppfylt, beror på en faktisk vurdering av den tekniske løsningen, og ikke hva leverandøren har påtatt seg av ansvar i kontrakten.

Bokføringsloven § 13 annet ledd åpner dessuten for at originalt regnskapsmateriale kan erstattes ved overføring av regnskapsinformasjon til «andre media». Nettskyen vil regnes som «andre media». Betingelsen for å overføre regnskapsmaterialet til andre media er at «muligheten til å etterprøve pliktig regnskapsrapportering i regnskapsmaterialets oppbevaringstid ikke svekkes». Regnskapsmaterialet skal også «kunne framlegges for offentlig kontrollmyndighet i hele oppbevaringsperioden i en form som muliggjør etterkontroll». Regnskapsmateriale som overføres til nettskyen vil i prinsippet kunne oppfylle disse vilkårene.

Forskrift om oppbevaring av elektronisk regnskapsmateriale i andre EØS-land oppstiller et unntak fra kravet om oppbevaring i Norge. I henhold til forskriften kan regnskapsmateriale også oppbevares elektronisk på servere i Danmark, Finland, Island og Sverige. Skriftlig melding om slik oppbevaring må sendes til Skattedirektoratet. Det må fremgå av meldingen hvilket regnskapsmateriale som oppbevares i utlandet, hvor regnskapsmaterialet oppbevares, og hvordan kontrollmyndighetene til enhver tid kan få adgang til regnskapsmaterialet.

Hovedregelen for servere plassert i utlandet er likevel fortsatt at permanent oppbevaring er forbudt, noe som rammer mange nettskytilbud.[9]

Regnskapspliktig materiale kan riktignok oppbevares *midlertidig* i utlandet til årsregnskapet er fastsatt, også i tilfellene registeringen helt eller delvis skjer fra Norge mot en server i utlandet.[10] Det følger av bokføringsforskriften § 7–4 første ledd at den bokføringspliktige innen én måned fra fastsetting av årsregnskapet og senest sju måneder etter regnskapsårets slutt, må overføre regnskapsmaterialet til oppbevaring i Norge. Regelverket er heller ikke til hinder for at back-up kopier lagres i utlandet, forutsatt at hovedlagringen skjer i Norge på en måte som tilfredsstiller lovens krav.

Andre plikter som kan begrense bruken av nettskyen

Lovverket inneholder en rekke andre *oppbevaringsplikter*, foruten bestemmelsene i bokføringsloven. Et eksempel er plikten til å oppbevare lister over personer som har mottatt innsideinformasjon i fem år, jf. verdipapirhandelloven § 5. Et annet eksempel er hvitvaskingslovens § 22 annet ledd, som stiller krav til at regnskapsførere,

7 Se nærmere: arkivverket.no/arkivverket/Arkivverket/Om-oss/Aktuelt/Nyhetsarkiv/Riksarkivaren-seier-nei-til-skyarkivering-i-utlandet. Malin Tønseth har drøftet Riksarkivarens uttalelse i *Arkivloven og skytjenester* i LoD-2014–120–1.

8 Slik Malin Tønseth i *Arkivloven og skytjenester* i LoD-2014–120–1.

9 Med mindre departementet bruker sin kompetanse til å gi unntak fra dette forbudet, jf. § 13 siste ledd.

10 skatteetaten.no/no/Radgiver/Rettskilder/Uttalelser/Prinsipputtalelser/Midlertidig-oppbevaring-av-regnskapsmateriale-i-utlandet/

maestro

kingdesign.no

Maestro gjør din jobb litt enklere.

Sammen med våre brukere utvikler vi fremtidens løsninger for årsoppgjør og økonomisk rapportering.

Med så mye kunnskap på laget er vi opptatt av å utvikle de mest fleksible produktene og den beste brukerstøtten. Bli Maestro-bruker du også!

> *Maestros raske og gode support, samt vilje og evne til å tilpasse systemene til våre behov, gjør at vi er godt fornøyd med Maestro som vår leverandør av konsern- og årsoppgjørprogramvare.*
>
> Martin Aasen, Partner BDO

Ta kontakt med oss på telefon 02575

eller salg@maestro.no for mer informasjon og bestilling

maestro.no

revisorer, banker, forsikringsselskaper og advokater o.l. oppbevarer dokumentasjon for lovpålagt kundekontroll i en periode på fem år etter avslutningen av kundeforholdet. Dersom det ikke stilles særskilte krav i den aktuelle bestemmelsen, må utgangspunktet være at oppbevaringsplikten kan oppfylles gjennom å lagre informasjonen i en nettsky.

Tilsvarende spørsmål kan oppstå i forbindelse med lovpålagte eller avtalte *konfidensialitetsforpliktelser*. Spørsmålet blir om oppbevaring av informasjon i nettskyen innebærer en spredning og/eller tilgjengeliggjøring av informasjon i strid med konfidensialitetsplikten. Dette må igjen vurderes konkret, ved å sammenholde de kravene som følger av den konkrete konfidensialitetsplikten med den informasjonsspredningen bruk av nettskyen innebærer. Det avgjørende vil normalt være hvem som får tilgang til informasjonen ved lagringen. Lagring i nettskyen kan imidlertid ikke i seg selv bety at informasjonen anses spredt eller tilgjengeliggjort.

Det kan også foreligge plikter til å sørge for sikring av data mot bl.a. tap og misbruk, eksempelvis som følge av hacking. Et eksempel på dette er forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT), som stiller krav til IKT-virksomheten til bl.a. banker, forsikringsselskap, inkassoforetak og eiendomsmeglerforetak. De regulerte foretakene må bl.a. «utarbeide prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, jf. § 1, mot skader, misbruk, uautorisert adgang og endring, samt hærverk», jf. § 5. Forskriftens § 2 og 12 forutsetter likevel at hele eller deler av IKT-virksomheten til de regulerte virksomhetene kan settes ut. Forskriften er derfor ikke til hinder for bruk av nettskyløsninger. Sikkerhetsnivået den enkelte nettskyløsning tilbyr, må imidlertid oppfylle forskriftens krav. En rapport utgitt av ENISA (European Union Agency for Network and Information Security) i desember 2014, påpeker at en rekke finansielle virksomheter i Europa er tilbakeholdne med anvendelse av nettskyløsninger av frykt for ikke å overholde de regulatoriske kravene for nettskybruk.

Det kontraktsrettslige forholdet til nettskyleverandøren

Kontrakten for nettskytjenestene vil typisk følge leverandørens standardvilkår. Som regel er det lite eller intet forhandlingsrom for å få endret på disse vilkårene. Den virksomhet som velger å akseptere og inngå avtaler på slike standardvilkår, vil bli bundet av disse på de vilkårene som følger av en objektiv tolkning av bestemmelsene. Det skal svært mye til før en avtale mellom to profesjonelle parter kan settes til side, eller at en klar ordlyd bortfortolkes. Det finnes heller ikke ufravikelig lovgivning om nettskyavtaler som kan redde nettskykunden.

Innholdet av avtalen bør på den bakgrunn vurderes nøye forut for avtaleinngåelsen. Dels må det undersøkes om avtalen gir sikkerhet for at tjenestene gjennomføres på en måte som er i samsvar med nettskykundens regulatoriske forpliktelser gjennomgått ovenfor. For eksempel må den virksomheten som ønsker å bruke nettskytilbudet til å lagre personopplysninger, undersøke om avtalen gir sikkerhet for at personopplysningene ikke overføres til andre land på en måte som er i strid med personopplysningsloven.

Av andre forhold som kan være relevant for nettskykunder er:[11]

- Fremgår det tydelig hvilke tjenester som omfattes?
- Er de kvalitative kravene som stilles tilstrekkelig presise, slik at det i praksis vil være mulig å klage dersom ytelsen er dårlig?
- Har leverandøren forpliktet seg til konfidensiell behandling av dataene, og til å avstå fra å bruke dem for egne formål?
- Er sikkerhetsnivået leverandøren tilbyr tilstrekkelig?
- Er det tilfredsstillende oppetid og responstid?
- Hva skjer hvis noe går galt? Har leverandøren fraskrevet seg ansvaret for erstatning ved eventuelt mislighold? Hvem har risikoen for tap av data?
- Hva skjer ved opphør av avtalen med tanke på tilbakeføring av data, og eventuelt migrering til ny leverandør? Er tilbakeføring av data kurant både teknisk sett og etter kontrakten?
- Har leverandøren tatt forbehold om å innføre ensidige endringer av negativ betydning for kunden, enten det gjelder innholdet av avtalevilkårene eller innholdet av selve tjenesten?
- Hvilket lands rett avtalen er underlagt, og hvilket lands domstoler skal behandle eventuelle tvister? Mange nettskyleverandører er utenlandske, og vil i sine standardvilkår utpeke leverandørens hjemland både med tanke på lovvalg og verneting. Dette kan skape praktiske utfordringer for en norsk kunde dersom en tvist først oppstår.

11 Mer omfattende sjekklister for nettskykontrakter er utarbeidet av bl.a. Cloud Sweden (se cloudsweden.se).

Det må understrekes at en kontrakt som gir kunden krav på god ytelse og relevante misligholdsbeføyelser, er en mager trøst dersom tjenesten rent faktisk fungerer dårlig eller ikke er tilgjengelig, eller dersom data går tap. Tilsvarende vil en kvalitativt god og sikker teknisk løsning fra en anerkjent leverandør i noen tilfeller kunne kompensere noe for en dårlig kontrakt der leverandøren fraskriver seg det meste av ansvar.

Avslutning

Gjennomgangen av det rettslige rammeverket for nettskyen har vist at nettskyen medfører flere rettslige utfordringer for bedrifter. For offentlige virksomheter vil eksempelvis arkivloven hindre bruk av utenlandske nettskytjenester som innebærer varig lagring av informasjon. Dette er uheldig sett i lys av fordelene nettskyen kan føre til, og bør endres.

Regjeringen har respondert på de utfordringene dagens lovverk medfører. Kommunal- og moderniseringsdepartementet har nedsatt et interdepartementalt prosjekt som i løpet av første halvår 2015 skal utarbeide en oversikt over hvilke regelverk som kan hindre bruk av nettskyen og deretter vurdere hvorvidt disse reglene mangler en god begrunnelse med dagens teknologi. I tillegg vil departementet lage en policy for bruk av nettskyen, og utarbeide sjekklister og veiledere for virksomheter som vurderer å bruke nettskytjenester.[12] Det er også grunn til å tro at EU vil videreutvikle relevant regelverk som også vil ha betydning for Norge. Et eksempel er rapporten fra ENISA nevnt ovenfor, der det oppfordres til at EBA (European Banking Authority) utarbeider klare retningslinjer for finansnæringens bruk av nettskyen.

12 regjeringen.no/nb/tema/statlig-forvaltning/ikt-politikk/hvor-skal-offentlig-sektor-lagre-og-behandle-data/id2 353 784/?regj_oss=10

Det skal utarbeides en oversikt over hvilke regelverk som kan hindre bruk av nettskyen.