Juridiske utfordringer:

Bruken av nettskytjenester

Artikkelen er forfattet av:

Sivilingeniør
Martin Bryn
Partner Deloitte

Advokat
Bjørn Ofstad
Deloitte Advokatfirma

Artikkelen på 15 sekunder

Bruk av nettskytjenester reiser flere juridiske problemstillinger og stiller krav til virksomhetens håndtering av slike ordninger. Den enkelte virksomhet må forsikre seg om at bruken av nettskytjenesten har en tilfredsstillende informasjonssikkerhet, og blant annet foreta en risikoanalyse når det gjelder behandlingen av personopplysninger. Det kreves at virksomheten inngår en databehandleravtale som regulerer hva databehandleren kan bruke opplysningene til, og hvordan opplysningene skal sikres teknisk og fysisk. Bruk av nettskytjenester vil også kunne påvirke informasjonsplikten til virksomheten som er den behandlingsansvarlige.

I artikkelen beskrives noen sider ved samspillet mellom virksomheten (den behandlingsansvarlige), tilbyder av nettskytjenesten (databehandler) og de kravene som stilles i lovverket til bruk av nettskytjenester.

Nettskytjenester

Nettskytjenester – eller Cloud Computing – er en samlebetegnelse som omfatter alt fra dataprosessering og datalagring til bruk av programvare tilgjengelig på eksterne servere. Flere og flere aktører i privat og offentlig sektor ser de mange fordelene ved bruk av nettskytjenester. Eksempelvis kan det være kostnadsbesparende for en virksomhet å sette bort lagring og håndtering av virksomhetens personalarkiv og kunderegister til en ekstern tilbyder av nettskytjenester. Normalt er det også slik at tilbyder av nettskytjenestene i tillegg garanterer for tilgang til bruk av til en hver tid nyeste programvare. Virksomheten slipper da å holde seg oppdatert i forhold til programvareutvikling ved å betale lisens («abonnement») for bruk av programvaren. En annen fordel ved bruk av nettskytjenester er at virksomheten som benytter tjenesten bare betaler for faktisk bruk, noe som medfører at man ikke trenger å ta stilling til kapasitetsbehov. Stikkordet i denne sammenheng er skalerbarhet og fleksibilitet for virksomheten.

Virksomheten og tilbyder av nettskytjenester må være tilknyttet Internett. Videre er det ofte slik at nettskytjenester tilbys fra utenlandske serverparker. Dette er begge forhold som også medfører noen utfordringer ved bruk av nettskytjenester.

Behandlingsansvar – databehandleravtale

I korte trekk kan man si at bruk av nettskytjenester er en form for arbeidsfordeling mellom en virksomhet og en nettskyleverandør, initiert av virksomheten. Personopplysningsloven stiller krav til slike arbeidsfordelinger. Blant annet slår personopplysningloven fast at en behandlingsansvarlig (virksomheten) som setter ut lagring og håndtering av et elektronisk personellarkiv til en databehandler (leverandør av nettskytjenester), fortsatt vil ha ansvaret for personopplysningene.

Videre står det i personopplysningsloven at det i slike tilfeller skal opprettes en databehandleravtale som regulerer arbeidsfordelingen mellom den behandlingsansvarlige (virksomheten) og databehandler (leverandør av nettskytjenester). Eksempelvis skal det i avtalen reguleres hva databehandleren kan bruke opplysningene til og hvordan opplysningene skal sikres teknisk og fysisk.

> Personopplysningloven slår fast at en virksomhet som setter ut lagring og håndtering av eksempelvis et elektronisk personellarkiv, eller annen behandling av personopplysninger, til en leverandør av nettskytjenester, fortsatt vil ha ansvaret for personopplysningene.

Risikovurdering, informasjonssikkerhet og revisjon

En virksomhet skal foreta en risikoanalyse av hvordan den behandler personopplysninger, og risikoanalysen må ses i sammenheng med etablerte akseptkriterier for risiko. Ved siden av dette må virksomheten sørge for å ha på plass et system som sørger for tilstrekkelig informasjonssikkerhet.

For å forsikre seg om at tilfredsstillende informasjonssikkerhet foreligger, må den enkelte virksomhet forvisse seg om at tjenesten som blir tatt i bruk, tilfredsstiller de kravene som er forankret i virksomhetens risikovurderinger. Datatilsynet har sagt at vurderingen må skjerpes når man går fra egen drift til bruk av nettskybaserte løsninger, siden personopplysningene da vil ligge utenfor virksomhetens direkte kontroll.

En databehandleravtale mellom virksomheten og leverandøren av nettskytjenesten skal regulere informasjonssikkerheten, og virksomheten må kunne stille krav til databehandler om fremleggelse av dokumentasjon for utforming av informasjonssikkerhetssystemet.

Videre har personopplysningslovens kapittel 2 en regulering om sikkerhetsrevisjon:

«Sikkerhetsrevisjon av bruk av informasjonssystemet skal gjennomføres jevnlig. Sikkerhetsrevisjon skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartnere og leverandører. Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemet som ikke er forutsatt, skal dette behandles som avvik, jf. § 2–6. Resultatet fra sikkerhetsrevisjonen skal dokumenteres.»

Informasjonsplikt
Merk også at personopplysningsloven stiller krav til at den registrerte, eksempelvis en ansatt registrert i virksomhetens personellregister, skal ha informasjon fra virksomheten/arbeidsgiver om:

- Navn og adresse på den behandlingsansvarlige
- Formålet med registreringen
- Opplysninger vil bli utlevert, og eventuelt hvem som er mottaker,
- Det er frivillig å gi fra seg opplysningene
- Annet som gjør den registrerte i stand til å bruke sine rettigheter etter personopplysningsloven

Bruk av nettskytjenester vil kunne påvirke informasjonsplikten fra virksomheten. Det kan eksempelvis være plikt til å informere om hvor opplysningene er lagret dersom de er lagret utenfor Norge.

Adskillelse av opplysninger lagret i nettskyen
En nettskyleverandør vil normalt tilby sine tjenester til flere brukere, noe som betyr at det i en nettsky ofte vil være lagret informasjon fra flere virksomheter og/eller offentlige institusjoner. Avhengig av nettskyleverandør, kan dette enten bety at data lagres i én felles database («multi-tenant»), eller at de lagres i egne dedikerte databaser («single-tenant»). Datatilsynet har utalt at en virksomhets personopplysninger ikke skal blandes med personopplysninger fra en annen virksomhet. Dette er forhold som må reguleres i databehandleravtalen, og nettskyleverandøren må dokumentere hvordan dette håndteres.

Overføring til utlandet
Ofte vil bruk av nettskytjenester medføre at opplysningene overføres/lagres i utlandet. Overføring av personopplysninger til land utenfor EU/EØS (tredjeland) krever et særlig behandlingsgrunnlag. Dette kan eksempelvis være «skreddersydde» avtaler utarbeidet av EU-kommisjonen hvor mottaker garanterer for en viss sikkerhet for personopplysningene. Overføring av personopplysninger til USA kan være forankret i Safe Harbour-avtalen, gitt at nettskyleverandøren har valgt å signere Safe Harbour-avtalen. Det finnes også enkelte tredjeland som av Datatilsynet er klassifisert som «trygge» mottakerland hvor en overføring behandles som om overføringen var foretatt innenfor EU/EØS.

Kontroll med databehandleren
Etter personopplysningsloven følger det at virksomheten skal etablere planlagte og systematiske tiltak for å sikre at lovens krav følges. Det er verdt å merke seg at virksomheten er ansvarlig for at denne kontrollen gjennomføres.

Det bør da reguleres i databehandleravtalen hvordan opplysningene skal lagres, hvilke rutiner som skal følges og hvordan etterlevelsen skal kontrolleres. Internkontrollen må også gjelde for andre plikter enn informasjonssikkerhet, f.eks. at opplysningene ikke skal behandles til andre formål enn det som er avtalt om sletting, bruk og overføring til tredjeland.

Autorisert og uautorisert bruk
Personopplysningsforskriften stiller krav til at uautorisert bruk av opplysninger, og forsøk på uautorisert bruk av informasjonssystemet skal registreres. Avtalen mellom virksomheten og nettskyleverandøren må ta høyde for slik registrering. Teoretisk sett er det opp til partene hvem som skal foreta slike registreringer. Det er imidlertid vanlig at dette reguleres i databehandleravtalen, slik at dette i praksis løses ved at databehandleren registrerer hvem som tar ut opplysninger fra informasjonssystemet, at dette lagres og kan kontrolleres i ettertid.

Opplysninger om registrering av databruk må ses i sammenheng med tilgangsstyringer. En tilgangsstyring kan bestå i at gitte personer vil få tilgang gjennom personlige brukernavn og passord. De personene som skal innvilges en tilgang, bør i tillegg være underlagt et autentiserings- og autorisasjonssystem, hvor det undersøkes om personen er egnet til å få tilgang til opplysningene. En slik vurdering må da foretas opp mot personell hos databehandleren, altså de personene som arbeider i virksomheten som leverer nettskytjenesten. Arbeidstakerne hos databehandleren bør også underlegges den samme taushetsplikten som de ansatte i virksomheten til enhver tid har, når disse behandler personopplysninger m.m.

Den behandlingsansvarlige virksomheten må forsikre seg om at tilgangsstyringen er tilfredsstillende og i samsvar med lovpålagte krav om egen internkontroll. Dette løses gjennom risikovurderinger hvor man ser hen til opplysningene som skal lagres og de tilgangs- og sikkerhetssystemer som databehandleren har satt i verk.

Som vi har vist ovenfor vil samspillet mellom virksomheten (den behandlingsansvarlige), tilbyder av nettskytjenesten (databehandler) og de kravene som stilles i lovverket til bruk av nettskytjenester, kreve inngående kunnskap innenfor både jus og informasjonsteknologi.

Virksomheters bruk av nettskytjenester

Blant annet som et ledd i virksomheters effektiviseringstiltak ser vi at flere virksomheter outsourcer ulike oppgaver til eksterne tjenesteleverandører. En tjeneste som i økende grad etterspørres av virksomheter i Norge, er bruken av nettskytjenester (eller Cloudløsninger/ SaaS: Software-as-a-Service). Bruk av slike tjenester reiser flere juridiske problemstillinger, og stiller strenge krav til sikkerhet og gode rutiner hos tilbydere av nettskytjenester.

Datatilsynet mottok i 2011 en klage på Narvik kommunes bruk av nettskytjenester, mens Moss kommune selv kontaktet Datatilsynet for veiledning om sin bruk av nettskytjenester. Datatilsynet varslet i første omgang et vedtak om at kommunenes bruk av tjenestene måtte opphøre. I 2012 valgte Datatilsynet ikke å fatte vedtak likevel, men lot Narvik kommune fortsette å bruke tjenesten. Moss kommune har fått veiledning fra Datatilsynet i bruken av nettsky.

«Dette er ingen blancofullmakt til å benytte nettskytjenester, men hvis en del forutsetninger er på plass, og en virksomhet gjennomgår en grundig og god risikoanalyse, vil det kunne være en akseptabel løsning», sier direktør i Datatilsynet, Bjørn Erik Thon.