Datatilsynet

Cloud computing – en veileder i bruk av nettskytjenester

En vurdering av nettskytjenester opp mot kravene i personopplysningsloven
1. april 2011

Innledning

Cloud Computing, heretter kalt Nettskyen, er en samlebetegnelse for alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett. Serverparkene i Nettskyen kjennetegnes ved at de er laget for såkalt dynamisk skalering. Det betyr at datakraft kan tilpasses kapasitetsbehov, og ved at det som regel betales for faktisk bruk ut ifra behov. Mange eksterne serverparkene står utenfor Norges grenser og utfordringen for virksomhetene er å sørge for at avtalene er i henhold til norsk lovgivning. Det finnes ulike typer Nettsky-tjenester tilgjengelig, alt fra Infrastructure as a Service (IaaS) til Software as a Service (SaaS)[1].

Datatilsynet vil i denne veilederen foreta en overordnet vurdering av Nettskyen opp mot de krav som stilles av personopplysningsloven og helseregisterloven. Det er i tillegg en god del utfordringer i forhold til inngåelse av SLA (Service Level Agreement) avtaler med leverandørene. Da dette faller utenfor Datatilsynets forvaltningsområde. De ulike leverandørene vil heller ikke bli vurdert, da veilederen er generisk og prinsipiell.

Veiledren har følgende fokusområder:

- Personopplysningslovens virkeområde
- Identifisering av behandlingsansvarlig og ansvar
- Akseptkriterier
- Klarlegge juridisk ansvar for leverandør av nettsky-tjenester
- Risikovurdering og informasjonssikkerhet
- Informasjonsplikt
- Særlige problemstillinger
    - Sikkerhetskopiering/Speiling
    - Segmentering
    - Tilgangsstyring
    - Autorisert og uautorisert bruk
    - Dokumentasjon
    - Utlevering til tredjeland

Personopplysningslovens virkeområde

Personopplysningsloven får anvendelse så fremt den behandlingsansvarlige har oppfylt etableringskravet[2] i Norge og at det behandles personopplysninger i tjenesten som definert i personopplysningsloven § 2 nr. 1.

Behandlingsansvar

Plasseringen av behandlingsansvar er ikke noe annerledes enn hvis man velger lokal leverandør av servertjenester som ikke er Internettbasert. Det er den virksomheten som kjøper tjenesten for sin behandling av personopplysninger som er behandlingsansvarlig, jf. Personopplysningsloven § 2 nr. 4.

[1] http://no.wikipedia.org/wiki/Nettskyen

[2] Etableringskravet reguleres i personopplysningslovens § 4. Et sentralt forhold er hvorvidt "..den behandlingsansvarlig benytter hjelpemidler i Norge…"

Akseptkriterier for risiko

Akseptkriterier er nivå for akseptabel risiko forbundet med behandling av personopplysninger, jf. personopplysningsforskriften §§ 2 nr. 4 første ledd og 2 nr. 2. Det skal henvises til akseptabel risiko ved gjennomføring av risikovurderinger og skal gjennomføres før elektronisk behandling av personopplysninger starter, jf. personopplysningsforksriften §§ 2 nr. 1 og 2 nr. 4 siste ledd.

Ansvar for Nettsky-leverandør

Sett i sammenheng med punktet om plassering av behandlingsansvar, faller det naturlig at leverandører av elektroniske tjenester for behandling av personopplysninger på Internett ikke stiller seg annerledes enn hvilken som helst annen tradisjonell lokal leverandør for behandling av personopplysninger. I behandling legges definisjonen i personopplysningsloven § 2 nr. 2 til grunn.

Det leveres altså en tjeneste som man kan velge å ta i bruk som behandlingsansvarlig, hvis denne tjenesten gjennomfører en behandling på vegne av den behandlingsansvarlige er de å anse som en databehandler, jf. Personopplysningsloven § 2 nr. 5.

En databehandler kan ikke behandle personopplysninger på annen måte enn det som er avtalt med den behandlingsansvarlige, jf. personopplysningsloven § 15. Databehandleren plikter i tillegg å gjennomføre sikringstiltak som følger av personopplysningsloven § 13 og forksriftens kapittel 2. En databehandleravtale fritar ikke behandlingsansvarlig for lovfestet juridisk ansvar.

Datatilsynet har laget en veileder og eksempel på avtaleskisser for en slik databehandleravtale. I avtaleskissen og veilederen finner man minimumskravene som det forventes at en slik avtale innholder. Det kan være andre punkter som tilkommer selve avtalen, men det er avhengig av internkontrollen til den behandlingssansvarlige som kjøper tjenesten. Noen slike punkter kan være; sikkerhetskopiering, sletting, tilgangstyring, segmentering av databaser med videre.

Databehandleravtalen skal også til enhver tid gjenspeile hvor personopplysningene blir behandlet. Dette innebærer i praksis informasjon til enhver tid om hvilken leverandør som fysisk besitter de aktuelle opplysningene i det aktuelle landet. Dette kan også være en underleverandør til den som selve tjenesten er levert av.

I tillegg kan det være nødvendig med andre avtaler for regulering av behandlingen, som eksempelvis Safe Harbor. En Safe Harbor[3] avtale vil typisk være aktuelt når tjenesteleverandøren juridisk sett befinner seg utenfor EU og EØS-området. Det er anbefalt å gå igjennom Datatilsynets veiledning om overføring av personopplysninger til utlandet, mer informasjon om det finnes her: http://www.datatilsynet.no/templates/article____2620.aspx.

Datatilsynet anser av den grunn en leverandør av Nettsky-tjenester som en databehandler, uavhengig av hvilken tjeneste som leveres, så fremt personopplysningsloven med forskrift har anvendelse.

Risikovurdering og informasjonssikkerhet

Den behandlingsansvarlige skal, som nevnt tidligere, gjennomføre en risikovurdering for behandling av personopplysninger, jf. personopplysningsforksriften § 2 nr. 4. Risikovurderingen skal deretter sammenlignes med akseptkriteriene som ble laget først. På bakgrunn av dette skal det treffes

[3] Datatilsynet om Safe Harbor: http://www.datatilsynet.no/templates/article____2626.aspx

adekvate tiltak for å oppnå en tilfredsstillende informasjonssikkerhet for behandling av personopplysningene.

For å oppnå tilfredsstillende informasjonssikkerhet må den behandlingsansvarlige kunne forvisse seg om at tjenesten som blir tatt i bruk møter de kriterier som er fastlagt under arbeidet med akseptkriteriene og risikovurderingen. Vurderingen må tillegges større vekt når man eksempelvis går fra egen drift av e-post løsninger eller lagring av opplysninger til nettskybaserte løsninger som oppnår samme formål. Det blir faktisk enda viktigere. Spørsmålet blir; Hvordan skal den behandlingsansvarlige forvisse seg at informasjonssikkerheten faktisk er tilfredsstillende?

Ettersom nettskybaserte løsninger benytter Internett som hovedkanal for kommunikasjon er det ofte slik at leverandøren kommer med en avtale som kjøper skal signere på. Avtalen innholder vanligvis en del som omhandler informasjonssikkerhet.

Det er ikke gitt at en slik avtaler god nok for å forvisse seg om en tilfredsstillende informasjonssikkerhet. Erfaringer fra Danmark viser at leverandører ikke alltid innfrir rimelige forventninger. I en konkret og prinsipiell viktig sak har det danske Datatilsynet tatt stilling i en sak mot en dansk kommune for lagring av sensitive personopplysninger i Nettskyen. Kommunen kunne ikke legge en avtale fra leverandøren til grunn for å si at informasjonssikkerheten var god nok. Tilsynsmyndigheten mente at kommunen med rimelighet måtte forvisse seg om at så var tilfelle.

Personopplysningsforksriftens kapittel 2 om informasjonssikkerhet har i tillegg en særlig bestemmelse vedrørende sikkerhetsrevisjon;

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

Datatilsynet er derfor av den oppfatning at:

- Databehandler må kunne legge frem dokumentasjon for informasjonssystemets utforming og sikkerhetsløsninger slik at behandlingssansvarlig kan forvisse seg om at løsningen har tilfredsstillende informasjonssikkerhet sett opp mot risikovurdering og akseptkriterier.
- Databehandler kan ikke endre informasjonssikkerhetstiltak uten at den behandlingsansvarlig er blitt informert skriftlig og har godkjent endringen, jf. risikovurdering og akseptkriterier.

Informasjonsplikt

Det følger av personopplysningsloven § 19 at den registrerte skal ha informasjon fra den behandlingsansvarlige om blant annet navn og adresse på den behandlingsansvarlige og dennes eventuelle representant, jf § 18 om rett til innsyn. Den behandlingsansvarlige må kunne håndtere de rettigheter den registrerte har etter nevnte bestemmelser.

Særlige problemstillinger

Nettskyen har i utgangspunktet fordeler i forhold til tradisjonelle leverandører av servertjenester kan Nettskyen tilby mer fleksible og interoperative løsninger. Men slike fordeler fører også med seg noen særlige problemstillinger som kan være nødvendig å adressere hvis man velger en nettsky-basert løsning.

- **Sikkerhetskopiering/Speiling** – Hvordan fungerer dette? Overføres personopplysningene til et annet land for redundans, eksempelvis fra Irland til USA eller fra Tyskland til India. Er en slik redundans i henhold til de avtaler som er inngått, er det nødvendig med en Safe Harbor avtale? Hvordan behandles personopplysningene på det andre stedet?
- **Segmentering** – Datatilsynet har uttalt ved tidligere anledninger at en behandlingsansvarliges personopplysninger ikke skal sammenblandes med en annen behandlingsansvarliges personopplysninger. Dette fordi de betraktes som to separate juridiske enheter. Hvordan vil dette bli håndtert?
- **Tilgangsstyring –** Hvem hos leverandøren har tilgang til personopplysningene som behandles? Er tilgangstyring i henhold til lovpålagte krav, egen internkontroll eller andre aktuelle forhold? Se særlig avsnittet over om risikovurdering og informasjonssikkerhet.
- **Autorisert og uautorisert bruk –** Tar løsningen høyde for registrering av autorisert og uautorisert bruk i henhold til personopplysningsforskriften §§ 2-14 og 2-16 siste ledd.
- **Dokumentasjon** – Er løsningen tilstrekkelig dokumentert med hensyn på kontroll fra offentlig myndighet, se særlig personopplysningsforskriftens § 2-16 første og annet ledd.
- **Utlevering til tredjeland** – Personopplysninger kan ikke uten videre overføres til land utenfor EØS-sonen. Reguleringen i slike tredjeland kan være en helt annen enn i Norge og dermed kreve forholdsregler. Det vises spesielt til personopplysningslovens § 29.