Bak skyen:
Behandling av personopplysninger

Tommy Tranvik, Senter for rettsinformatikk

NOIKOS, 28.10.10

Utfordringer for sky-kunder

1. Manglende styring og kontroll
2. Etterleve lover og regler
3. Endring av jurisdiksjon

- Gjelder særlig i forhold til personvern og informasjonssikkerhet

Se bl.a. ENISA (2009): Cloud Computing. Benefits, Risks and Recommendations for Information Security.

”The patchwork of worldwide data protection laws has become increasingly difficult to navigate” (John Vassallo, Microsoft)

”Governments have serious hurdles to overcome in terms of public perception of the secure processing of citizens’ personal information in cloud computing infrastructures” (ENISA 2009)

”There are restrictions on cloud computing in Europe. It isn’t killing the business, but it is slowing its evolution” (Bob Lindsay, HP)

Agenda

- Skissere viktige og generiske personvernrettslige utfordringer
  - uavhengig av tjenestemodell (SaaS, PaaS, IaaS, etc.)
  - uavhengig av distribusjonsmodell (offentlig sky, virtuell privat sky, partner- eller bransjesky, etc.)
- Spørsmål som bør stilles til leverandører av skytjenester

Sky-scenario

1. Offentlig virksomhet ønsker å bruke leverandør av skytjenester
2. Innebærer overføring av personopplysninger fra virksomheten til leverandøren

NB: Vurderingene kan bli noe annerledes i andre scenarioer (for eksempel individers bruk av skytjenester)

Direktiv 95/46/EC

- Felles regler for elektronisk behandling av personopplysninger i EU-EØS-området
- Ivareta grunnleggende personvernhensyn (bl.a. privatlivets fred, personlig integritet og opplysningskvalitet)
- Norges implementering av direktivet – personopplysningsloven med forskrift

Definisjoner og aktører

- **Personopplysninger**
  - vid definisjon
  - sensitive versus alminnelige
- **Den registrerte**
  - kontroll med og innflytelse over bruken av egne opplysninger
- **Den behandlingsansvarlige (BA)**
  - rettslig ansvarlig for bruken av den registrertes opplysninger
- **Databehandler (DB)**
  - behandler personopplysninger på oppdrag fra behandlingsansvarlig
- **Tredjeland**
  - overføring av personopplysninger til BA eller DB utenfor EU/EØS
  - kan skje under visse betingelser
- **Tilsynsmyndighet (Datatilsynet)**
  - vurdere beskyttelsesnivået i tredjeland
  - meldeplikt eller konsesjonsplikt

Aktører i skyen

- **Den registrerte**
  - bruker av offentlige tjenester (sluttbruker)
  - vite om og påvirke hva som skjer med egne opplysninger
- **Den behandlingsansvarlige**
  - offentlig virksomhet som benytter skytjenester
  - ansvarlig for hva leverandøren av skytjenesten gjør med den registrertes opplysninger
- **Databehandler**
  - leverandør av skytjenesten
  - instrueres av BA om hvordan opplysningene skal brukes (databehandleravtale)
  - fremlegge dokumentasjon overfor BA
- **Leverandør av tjenester til databehandler**
  - behandler personopplysninger som DBs underleverandør
  - kan være flere nivåer med underleverandører

DB kan i enkelte tilfeller være BA

Plikter i skyen

- Ivareta den registrertes rettigheter når opplysninger overlates til aktører i skyen:
  - sikre at sky-aktøren(e) ikke bruker opplysningene til egne formål uten samtykke fra den registrerte
  - gi den registrerte informasjon om hva som skjer med opplysningene
  - gi den registrerte innsyn i egne opplysninger
  - ivareta den registrertes rett til å kreve endring, sperring eller sletting av egne opplysninger

Fordeler med skytjenester

- Store kommersielle aktører
  - ressurser og kompetanse til å vite om rettslige regler
  - ressurser og kompetanse til å holde seg orientert om endringer i lovgivningen
  - ressurser og kompetanse til å ivareta rettslige regler i tekniske og organisatoriske løsninger
  - opptatt av å unngå omdømmetap (negativ publisitet)

Gjelder enkelte store kommersielle aktører mer enn andre

Nøkkelspørsmål 1

- Hvor befinner leverandøren av skytjenesten seg?
  - innenfor EU/EØS-området?
  - i ett eller flere tredjeland?
- I hvilke(t) tredjeland er leverandøren eventuelt lokalisert?
  - tilstrekkelig beskyttelsesnivå?
  - BCR?
- Hvor behandler leverandøren personopplysninger?
  - i ett eller flere tredjeland?
  - hvis ja, hvilke regler gjelder for lokale myndigheters tilgang til opplysningene?
  - kan behandlingsansvarlig påvirke hvor opplysningene lagres?

Nøkkelspørsmål 2

- Benytter leverandøren seg av underleverandører?
- Hvis ja, hvor befinner underleverandørene seg?
  - innenfor EU/EØS-området?
  - i ett eller flere tredjeland?
  - beskyttelsesnivå og lokale myndigheters tilgang?
- Hvilke garantier gir leverandøren i forhold til underleverandørers behandling av personopplysninger?
  - standard kontraktsbestemmelser (2002/16/EC)
- Hva skjer med opplysningene ved utløp av kontrakttiden?
  - stipuleres i databehandleravtale eller SLA?
- Hva hvis leverandøren går konkurs eller blir kjøpt opp?

Nøkkelspørsmål 3

- Hvordan er arbeidsdelingen mellom behandlingsansvarlig og leverandøren av skytjenester?
  - hvem kan den registrerte henvende seg til for bl.a. å kreve innsyn, retting, sperring eller sletting?
  - vil leverandøren benytte opplysningene til egne formål eller utlevere dem til andre?
- Har behandlingsansvarlig garantier for at opplysningene virkelig slettes?
- Hvordan sikrer leverandøren at opplysninger fra mange behandlingsansvarlige isoleres fra hverandre?
  - løsninger for identifisering og autentisering av brukere?
- Hva med behandling av sensitive personopplysninger?
  - kryptert lagring og overføring?
  - rutiner for sikker sletting?

Oppsummering

- Europeisk lovgivning for behandling av personopplysninger beskrives som den største utfordringen
- For behandlingsansvarlig – et styrings- og kontrollproblem
  - sette ut hele eller deler av behandlingen, men beholder det rettslige ansvaret
- Dette forutsetter (i henhold til lovgivningen)
  - garantier fra databehandler (leverandøren av skytjenester)
  - spesielt utfordrende hvis leverandøren benytter underleverandører
  - geografisk plassering av leverandør/underleverandører viktig
- Kvaliteten på informasjonen fra leverandøren avgjørende
- Mulighet for å inngå bindende avtaler og forhandle innholdet i avtalene?