Jeg vil se mappa mi!

Individets rett til kontroll med eget personvern.
-Hvilke konsekvenser gir dette for teknologivalgene?

Ragni Ryvold Arnesen
Seniorforsker, Norsk Regnesentral
Ragni.Ryvold.Arnesen@nr.no

Hva skiller personvern fra ”vanlig sikkerhet”?

- Betydningen av *formålet* med informasjons-behandlingen
- Behandling av personinformasjon kan utløse spesielle *forpliktelser*, f.eks.
  - gi beskjed til personen om at informasjon er utlevert til tredjepart
  - sletting av data etter en viss tid
- Krav til datakvalitet
- Forbud mot å lagre unødvendige opplysninger
- Rett til innsyn

Trender

- Kundeorientering
- Individuelle valg
- One-stop-shop
- Selvbetjening

Forutsetninger:

- Personalisering av tjenester
- Informasjonsdeling
- Tillit til organisasjon/etat og datasystemene

Dagens situasjon (1)

- Datasystemer gir få muligheter for individuell tilpasning
  - Oftest bare to valg: Godta alt, eller la være å bruke tjenesten
  - Individuelle valg i form av samtykke eller reservasjon er lite utbredt
  - Generell praksis må gjelde alle, og dermed være strengere enn mange ønsker
  - Mange nyttige, personaliserte tjenester er umulig å tilby
- Innsyn
  - Innsynsbegjæringer håndteres manuelt og er svært ressurskrevende
  - Retten til innsyn er hittil lite brukt

Dagens situasjon (2)

- Teknologiske løsninger:
  - P3P
  - IBMs Tivoli Privacy Manager
- Stor forskningsaktivitet
- EU-landene
  - Samme lovgivning som Norge, situasjonen nokså lik
  - Det Nederlandske datatilsynet har gjort mye arbeid, bl.a. ”identity protector”-konseptet
- Canada
  - Lovgivning snart på linje med EU
  - ”Privacy Impact Assessment” obligatorisk ved nyanskaffelser eller endringer av det offentliges systemer

Hva bør teknologien tilby?

- Minimere mengden innsamlet informasjon
  - Anonymisering, pseudonymisering, la være å samle inn
- Individuelle valg
  - Spesifisere hva man ønsker
  - Håndheving av hvert enkelt individs ønsker
  - Kontroll av at håndhevingen fungerer
- One-stop-shop-tjenester
  - Åpne, standard grensesnitt mellom systemer for informasjonsutveksling
- Selvbetjening
  - Grensesnitt for individet inn mot systemet

Personvern policy

- Samtykke skal være uttrykkelig og informert
- Policy må defineres i stringent, maskin-tolkbart språk
  - F. eks. EPAL laget av IBM
  - ”Hvem kan gjøre hva med hvilken type informasjon, med hvilket formål, under hvilke betingelser og med hvilke påfølgende forpliktelser”
- Trenger verktøy for å kunne gjøre det gjennomførbart for folk flest

Overføring av policy

- Personlig policy må gjøres tilgjengelig for de som skal etterleve den
  - Dvs. bedrifter, organisasjoner, etater osv., som eier og bruker databaser med personinformasjon
- Standardisering er nødvendig
  - Overføringsmetoder
  - Vokabular

Håndheving av personvern

- Automatisering
  - Trenger systemer som kan lese en policy og avgjøre forespørsler om tilgang til data
- Oppfyllelse av forpliktelser
- Integrasjon med saksbehandlingssystemet
- Utvidet adgang til data krever gode sikkerhetstiltak
  - Autentisering
  - Konfidensialitet
  - Integritet

Deteksjon av brudd på personvern

- Innsyn i data, hvor de kommer fra, hva de blir brukt til
  - Mest mulig automatisert
  - Helst (delvis) selvbetjent
  - Fordeler:
    - Bedre datakvalitet
    - Deteksjon av personvernbrudd
- Automatisk deteksjon av unormal oppførsel i systemet
  - Anomalideteksjon med statistiske metoder som ”lærer” hva som er normal oppførsel
  - Sammenholde ulike datakilder: aksesshistorie, policyer, logger

Advarsel

- En personvern policy kan i seg selv være meget sensitiv
  - Sier mye om personens liv, ønsker og behov
- Muligheten til å gjøre individuelle valg kan også lede til ”valgpress”
  - Mistenkeliggjøring (”hva har du å skjule?”)
  - Gruppepress
  - Aggressiv markedsføring

Oppsummering

- Systemer som gir individet muligheten til kontroll med eget personvern kan gi mange nye muligheter:
  - Enkel informasjonsdeling
  - Selvbetjente tjenester
  - Nye, personaliserte tjenester
- Effekter:
  - Effektivisering, målt i antall arbeidstimer
  - Kortere behandlingstid (kalendertid)
  - Brukervennlighet
  - Bedre kontroll med personvernet