Store data – store spørsmål

Bruk av statens store datamengder

NOKIOS Sesjon 3C Big Data i offentlig sektor

Trondheim 3. november 2016

Helge Veum, Avdelingsdirektør

Datatilsynet

Hva er personvern

- Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger.

- Alle mennesker har en ukrenkelig egenverdi. Som enkeltmenneske har du derfor rett på en privat sfære som du selv kontrollerer, hvor du kan handle fritt uten tvang eller innblanding fra staten eller andre mennesker.

EMK artikkel 8 / Grunnloven § 102

EMK artikkel 8

- "Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse."

Paragraf 102 i Grunnloven:

- "Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. **Statens myndigheter skal sikre et vern om den personlige integritet.**"

Personvernprinsippene

- Samtykke eller annet rettslig gr.lag
- Proporsjonalitet
- Formålsbestemthet
- Relevans og minimalitet
- Fullstendighet og kvalitet
- Informasjon og innsyn
- Informasjonssikkerhet
- Særlig vern for sensitive oppl.
- Anonymitet og sporfri ferdsel

Det offentliges behandling av data

- Betydelige mengder data
  - Stat, kommune, direktorater, helseforetak, politiet, lånekassa, skatt
- Ofte av sensitiv eller følsom karakter
  - Helse, kriminelle handlinger, spesielle behov, inntekt, arbeidsforhold, trygdeytelser, sosialhjelp
- Ofte liten grad av selvbestemmelse hos borgeren
  - Lovbestemt behandling, ingen valgfrihet

Bedre kunnskap om borgeren – dag for dag…

Det offentlige behandling av data

- Politisk styrt av mange gode formål
  - Kriminalitetsbekjempelse
  - En bedre skole
  - Bedre helsetilbud
  - En mer effektiv skatteinndriving
  - Bedre tjenester for innbyggerne

- En tendens til å behandle alle offentlige data som et statlig felleseie

- Digitalisering åpner for storstilt deling av data

Samme data – nye formål

Vi er negative til…

At dere ukritisk ruller dere rundt i statens personopplysninger som om det var et stort felleseie

Men…

Men…

- Digitalisering og personvern er ikke motsatte størrelser
- Datatilsynet er ikke motstander av å utvikle gode tjenester til innbyggerne
  - Inklusive gjenbruk av offentlige data
- Riktig bruk av teknologi kan også gi bedre personvern

Men… …

- Data kan deles i samspill med innbyggeren
  - Og det kan i noen tilfeller gi bedre personvern
- Innbyggeren kan
  - Bli informert på nett
    (det er ingen unnskyldning til å ikke informere lengre)
  - Utøve sine rettigheter på nett
- Åpenhet og informasjon er en selvfølge for god (e-)forvaltning

Respekt for innbyggeren

- Data innsamlet til et formål blir brukt til det formålet
- Gjenbruk til nye formål?
  - Godt rettslig grunnlag
  - Bygge interaksjon slik at innbyggeren er med i prosessen
- Bidra til kontroll med «egne» data
  - Varsling, innsyn og administrasjon, samtykke, reservasjon
- Dataminimalisering

Er det for vanskelig å spille på lag med innbyggeren?

…så må dere ha Stortinget i ryggen

- Forsvarlig utredet
- Lovhjemmel
- Demokratisk og transparent

Enkelt oppsummert

Digitaliseringen er en kjempemulighet for forvaltningen og personvernet

Dårlig personvern er dårlig forvaltning
- Det driver vi ikke med

Design morgendagens løsninger med personvern innebygd

Noen ganger (ofte?) må staten begrense sin bruk av data om enkeltindivid

Og en setning om regulering…

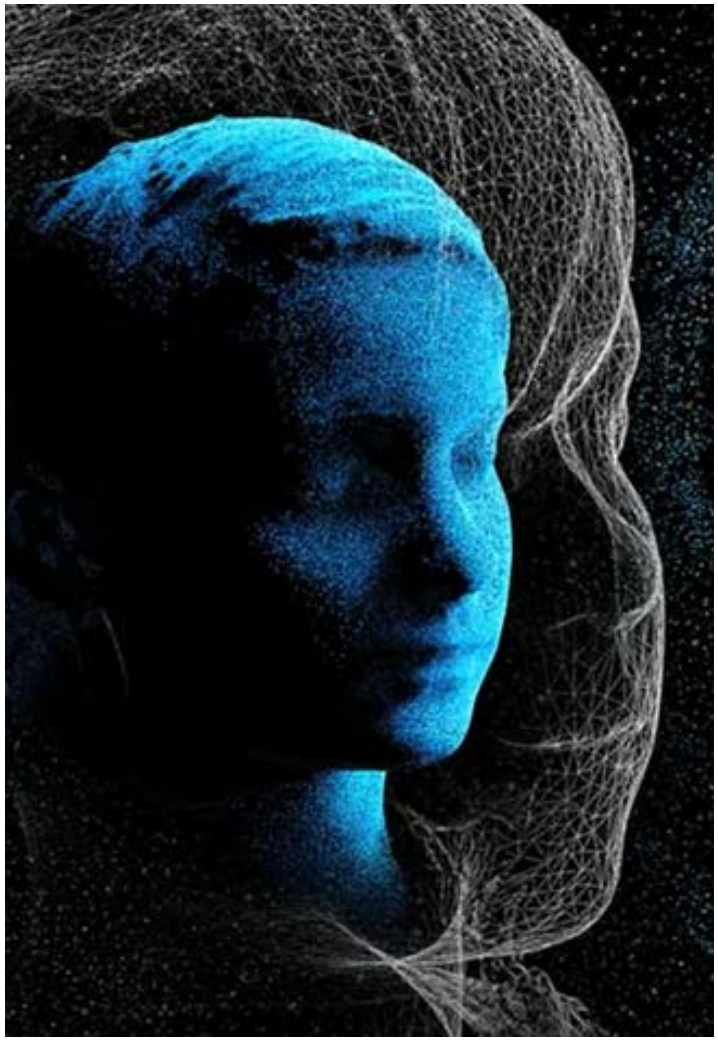
God e-forvaltning trenger god regulering

Når personopplysningsloven ikke gjelder trenger vi robuste regler for sikkerhet og ansvar

Her er vi ikke i mål

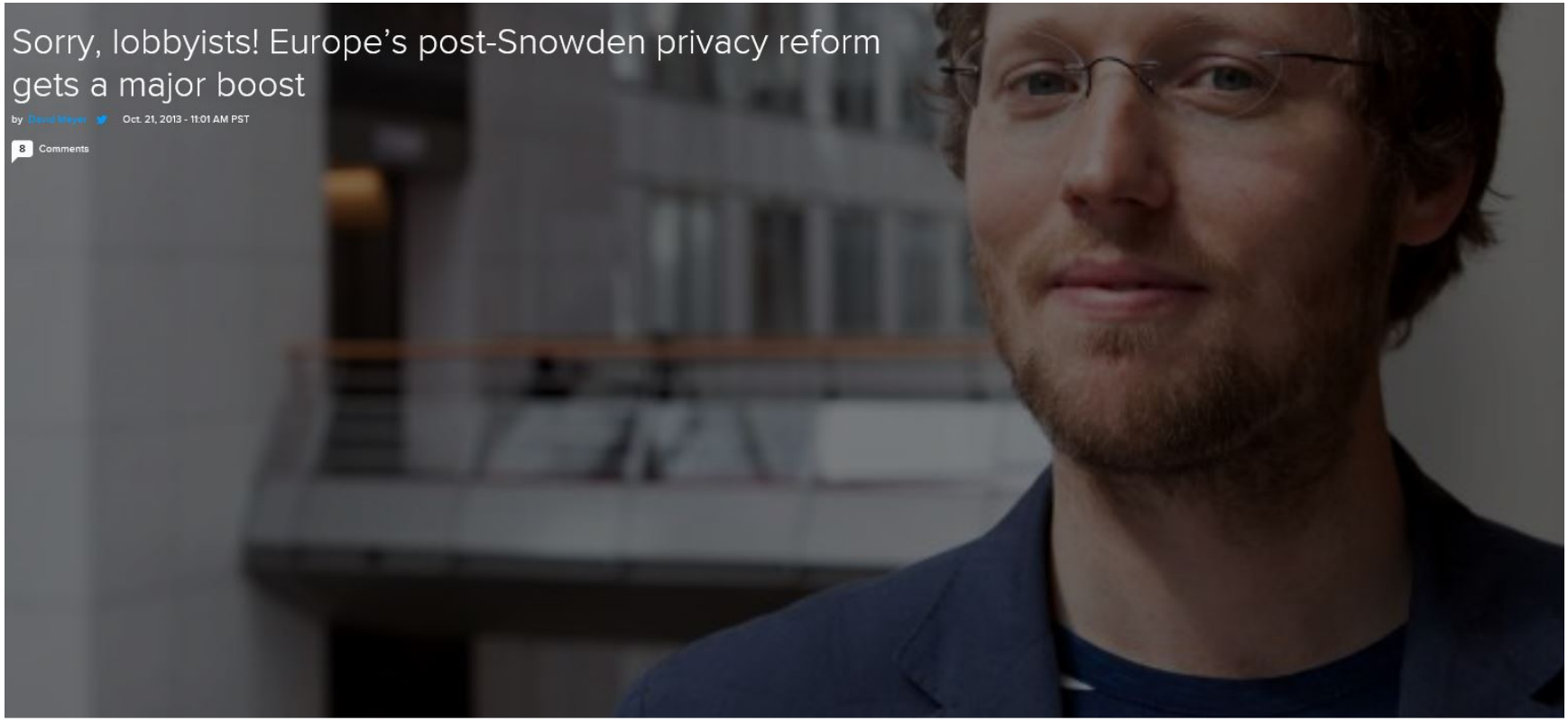
Hvordan utfordrer Big Data personvernet?

- Big Data utfordrer særlig to personvernprinsipper:
  - Formålsbestemthet: Personopplysninger må benyttes kun for bestemte formål
  - Dataminimalisering: Ikke lagre mer data enn nødvendig. Data som ikke lenger er nødvendige for det angitte formål må slettes eller anonymiseres
- *Big Data handler om datamaksimalisering og bruk av data til nye formål*



COMPUTER SAYS NO

Ny personvernlovgivning kommer



Sorry, lobbyists! Europe's post-Snowden privacy reform gets a major boost

by David Meyer Oct. 21, 2013 - 11:01 AM PST

8 Comments

Tough times loom for U.S. cloud companies selling into Europe. On Monday, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs voted overwhelmingly in favor of toughening up the EU's privacy regime.

The EU's new Data Protection Regulation has been crawling through the European legislative process for more than a year and a half now, and it began as quite a strident proposal for boosting Europeans' privacy. Then the U.S. corporate lobbying machine sprang to life, gutting key aspects of the new legislation.

And then Edward Snowden leaked the NSA documents, showing the world how the U.S. is subverting web services from Google to Microsoft in order to

Nye personvernregler fra 2018

Hva betyr det for din virksomhet?

Datatilsynet

Til ledere med ansvar for personvern, sikkerhet og utvikling

Er du klar for nytt regelverk?

I 2018 blir dagens personvernregelverk erstattet av EUs personvernforordning. Norske virksomheter bør derfor begynne å forberede seg på nye personvernregler allerede nå. Før de nye reglene trer i kraft må dere sørge for at dere har:

1

Internkontroll og oversikt over hvordan dere behandler person-opplysninger

Fra 2018 må ikke bare behandlings-ansvarlige, men også databehandlere ha oversikt over behandling av personopplysninger.

2

Systemer, tjenester og løsninger som oppfyller prinsippene om innebygd personvern

Velg den mest personvernvennlige innstillingen som standard. Bygg personvernet inn ved blant annet å begrense mengden informasjon som samles inn, pseudonymisere opplysninger så raskt som mulig, være åpen om innsamling og bruk av opplysninger, og tenke sikkerhet i alle utviklingsfaser (innebygd sikkerhet).

3

Systemer som er tilpasset for dataportabilitet

Alle registrerte skal som hovedregel kunne ta med seg personopplysninger de selv har oppgitt, fra en virksomhet til en annen. Systemene dere bruker må være tilpasset for overføringer og mottak av opplysninger.

4

Tilfredsstillende informasjonssikkerhet

Gjennomfør risikovurderinger og få på plass tekniske og organisatoriske tiltak som pseudonymisering og kryptering. Systemene må sikre konfidensialitet, integritet, tilgjengelighet og robusthet. Sørg for at tilgjengelighet og tilgang til personopplysningene dere behandler gjenopprettes på en sikker måte etter hendelser. I tillegg må dere ha prose-dyrer for å teste, vurdere og evaluere at tiltakene både er effektive og ivaretar sikring av alle personopplysninger virksomheten behandler.

5

Rammeverk og rutiner for å vurdere personvernkonsekvenser

Dersom et tiltak er inngripende, skal dere vurdere personvernkonsekvensene ved tiltaket ved hjelp av en Privacy Impact Assessment (PIA) før det iverksettes. Er risikoen høy og umulig for dere å redusere, skal Datatilsynet involveres i forhåndsdrøftelser.

6

Rutiner for avvikshåndtering

Forordningen stiller strengere krav til avvikshåndtering enn dagens regelverk. Ved brudd på sikkerheten skal dere varsle Datatilsynet innen 72 timer, og vi skal varsles oftere enn før. I tillegg skal dere informere alle som er berørt av sikkerhetsbruddet. Databehandlere skal også varsle behandlingsansvarlig umiddelbart ved avvik.

datatilsynet.no/forordning

Datatilsynet