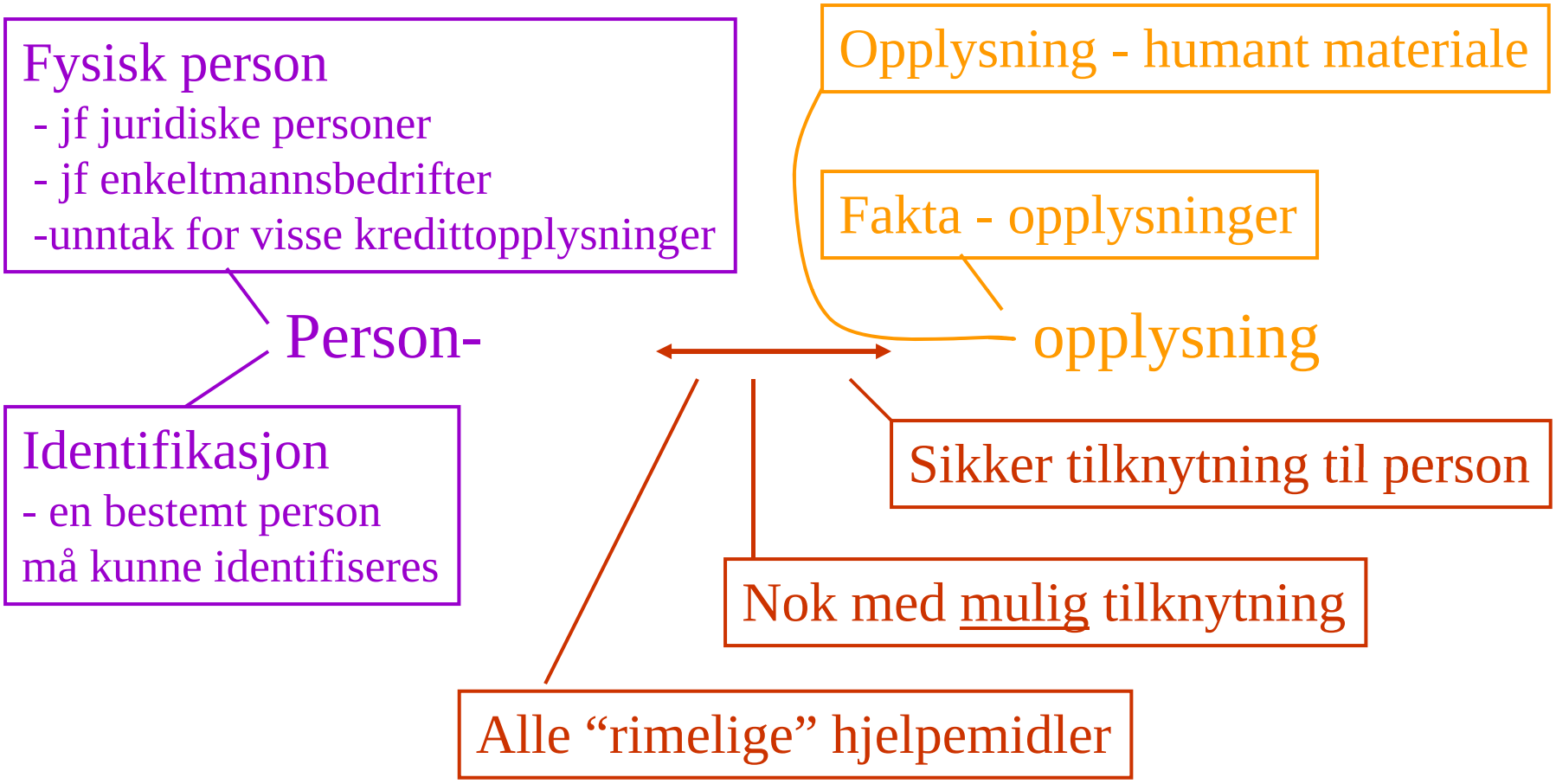
Om personopplysningslovens betydning for systemutvikling

Dag Wiese Schartum,
Avdeling for forvaltningsinformatikk (AFIN), UiO

Generelt

- Personopplysningsloven er (nesten) alltid relevant ved utvikling av informasjonssystemer som skal behandle “personopplysninger”
- Loven er basert på EU-direktiv om personvern som er mønster for lovgivningen i alle EU-/EØS- land
- Kan du hovedtrekkene i personopplysningsloven (pol), kan du hovedtrekkene i “all” europeisk personvernlovgivning (30 land)!
- De delene av regelverket jeg her gjør rede for er slike som primært gjelder systemnivået og som må tas hensyn til tidlig i et systemutviklingsarbeid
- Andre deler av loven (som jeg ikke gjennomgår her) er mer rettet inn mot den enkeltes rettigheter mv. Også disse er relevante for systemutvikling, men frivillig å ta hensyn til (kan for eksempel lage rutiner i systemet for å legge til rette for innsyn, men er ikke forpliktet til dette
- Denne forelesningen hører systematisk hjemme i bolk 2 av emnet (kunde-/leverandør-/brukerforhold)

“Personopplysning” (PO)



Loven skiller ikke mellom opplysningstype og -verdi, men dette skillet kan være nyttig

Sensitive personopplysninger: slike som er listet opp i § 2 nr 8.

Sjekkliste, trinn 1

- Gjelder loven for mitt informasjonssystem?
  - Hvis jeg er etablert i Norge (hovedregel)
  - Hvis PO blir behandlet elektronisk
    - Behandling = alt du kan gjøre med data
    - Helt eller delvis elektronisk behandling
    - Uansett tekst, bilde, lyd mv
    - Spesielle regler gjelder for videoovervåking

Sjekkliste, trinn 2

- Har jeg lovlig adgang til de opplysningene jeg ønsker å behandle (eller kan jeg skaffe det?)
- Mulige rettslige grunnlag
  - Lovhjemmel
  - Samtykke
    - Frivillig
    - Informert
    - Uttrykkelig
  - Nødvendig (slik det er angitt i pol §§ 8 og 9)

Sjekkliste, trinn 3

- Hva skal jeg benytte PO til?
  - All behandling av PO må skje for ett eller flere bestemte *formål*
  - Formålene må være angitt før behandling begynner
  - Formålet spiller en viktig rolle bl.a i forhold til krav til opplysningskvalitet og info.sikkerhet
  - Formålet kan endres, men det er begrensninger

Sjekkliste, trinn 4

- Har opplysningene den nøvendige kvalitet?
  - Kvalitetskravene skal alltid bedømmes ut i fra formålet
  - Kvalitetskrav etter loven:
    - tilstrekkelige
    - relevante
    - korrekte
    - oppdaterte
  - Det skal alltid vurderes om det er behov for tiltak for å fremme opplysningskvaliteten

Sjekkliste, trinn 5

- Er personene tilstrekkelig sikkert identifiserte?
  - Begrensninger i adgang til å benytte “entydige identifikasjonsmidler”:
    - fødselsnummer
    - biometriske identifikasjonsmetoder
  - Må være
    - saklig behov for og
    - nødvendig å benytte slike identifikasjonsmidler
  - Datatilsynet kan gi pålegg om bruk av entydige identifikasjonsmidler

Sjekkliste, trinn 6

- Hva er tilfredsstillende sikkerhetstiltak?
  - Skal sikre
    - konfidensialitet
    - integritet
    - tilgjengelighet
  - Skal vurdere behov for og iverksette tiltak
  - Tiltakene må være
    - planlagte
    - systematiske
    - dokumenterte
  - Tiltakene kan være av et hvilket som helst slag

Sjekkliste, trinn 7

- Hva må jeg gjøre for å være sikker på at loven, forskriften og eventuelle enkeltvedtak blir etterlevet?
  - Internkontroll må gjennomføres for å sikre etterlevelse av krav i:
    - lov og forskrift
    - konsesjoner og andre enkeltvedtak
  - Tiltakene må være
    - planlagte
    - systematiske
    - dokumenterte

Sjekkliste, trinn 8

- Kan jeg starte behandlingen?
  - Melding skal sendes minst 30 dager før hvis meldepliktig
  - Konsesjon må søkes hvis sensitive PO
    - Sensitive opplysningstyper er definert i loven
    - Kan ikke starte behandlingen før konsesjon er gitt og vilkår som stilles i konsesjonen kan etterleves

Videre informasjon

- Personvern.uio.no
- Datatilsynet.no
- Personvernnemnda.no