

Informasjonssikkerhet i forvaltningens saksbehandling – hvilke regler gjelder?

Dag Wiese Schartum
Avdeling for forvaltningsinformatikk
UiO

Regler om informasjonssikkerhet (hva er det?)

Krav til internkontroll (pol § 14)

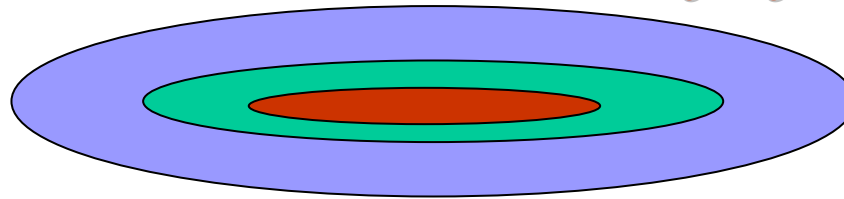
Fvl § 13c, annet ledd:
“oppbevaring på
betryggende måte”

Enkeltstående
regler

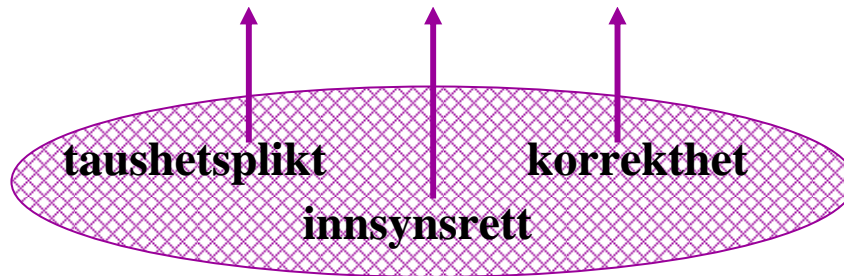
“Kombinasjoner” Prinsippet om forsvarlig saksbehandling

Helhetlige regelverk

- Personoppl.forskr. kap 2
- Eforvaltningsforskriften
- Sikkerhetsloven kap. 4
- Arkivforskriften kap IV



F.eks:



”Grunnregler” vedrørende
informasjonsbehandling

Sikring av personopplysninger er nødvendig i alle virksomheter

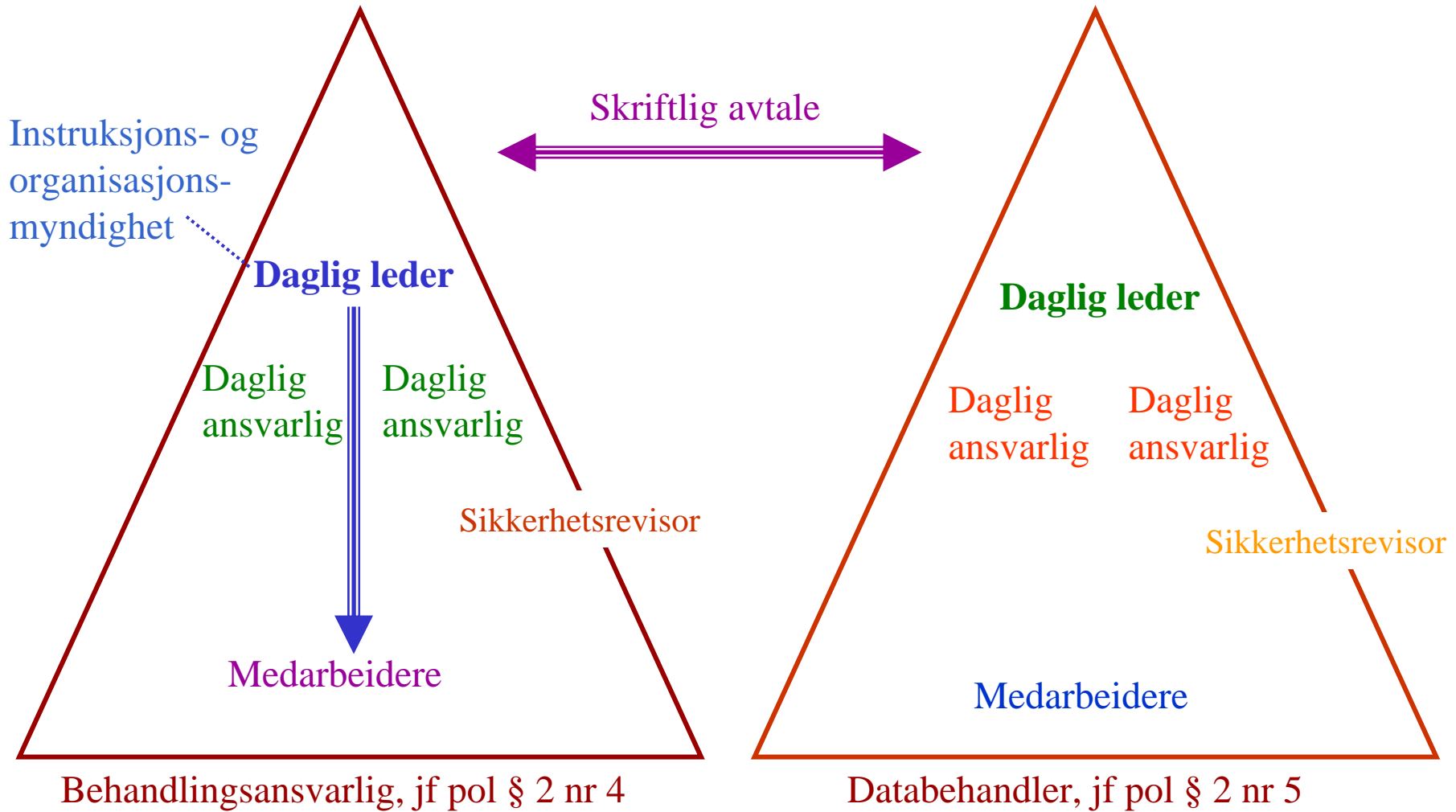
Forholdet mellom kravene i pol til sikring (§ 13) og internkontroll (§ 14)

- Mulig å se informasjonssikkerhet som et særskilt område av internkontrollen
- Felles krav til informasjonssikkerhet og internkontroll, pol §§ 13 og 14
 - Tiltak skal være
 - Planlagte
 - Systematiske
 - Dokumenterte
 - Dokumentasjonen skal være tilgjengelig for
 - Alle aktuelle medarbeidere
 - Tilsynsmyndigheter

Krav til informasjonssikkerhet etter pol § 13

- Bestemmelsen i § 13 gjelder både *behandlingansvarlig* og *data-behandler* og utgjør ramme for hva som kan bestemmes i forskrift
- Arbeidet med informasjonssikkerhet skal omfatte
 - Konfidensialitet
 - Integritet
 - Tilgjengelighet
- Informasjonssikkerheten skal være “tilfredsstillende”, jf pol § 13
 - Vurderingen gjelder hvor ekstensive (omfattende) tiltakene skal være
 - og hvor intensive/strengt tiltakene skal være
- § 13 innebærer krav om konkret vurdering av hver behandling
 - Forskriften stiller opp krav til **organisering** mv av sikkerhetsarbeidet
 - Forskriften stiller opp krav til **framgangsmåter** for sikkerhetsarbeidet
 - Forskriften stiller opp noen **materielle minstekrav** mv
- Datatilsynet kan gi pålegg om sikring (§ 2-2, jf pol §§ 46 og 47)

Krav til organisering av sikkerhetsarbeidet



Både behandlingsansvarlige og databehandler har selvstendig ansvar for informasjonssikkerheten

Krav til fremgangsmåter

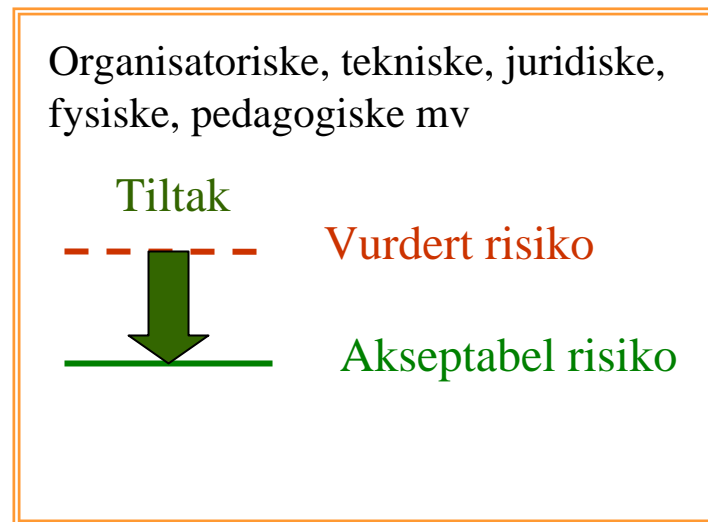
Det skal føres oversikt over hvilke personopplystyper som behandles

Det skal gjennomføres risikovurdering for behandlingen av disse opplysnings-typerne:

Sansynlighet for ... sikkerhetsbrudd
Konsekvensene av...

Tiltak skal være

- Planlagte
- Systematiske
- Dokumenterte



Stor
+

÷
Liten

Risiko

Avvikshåndtering

All behandling av personopplysninger skal skje i henhold til på forhånd fastlagte rutiner.

Behandling i strid med fastlagte rutiner og sikkerhetsbrudd skal behandles som avvik.

Avviksbehandlingen skal ha som formål å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentakelse.

Materielle krav til informasjonssikkerhet i pof

- Tiltakene skal stå i forhold til sannsynligheten for og konsekvenser av “sikkerhetsbrudd” (§ 2-1, 2), jf krav til risikovurdering (§ 2-4)
- Konkretiserer krav til:
 - Fysisk sikring (§ 2-10)
 - Konfidensialitet (§ 2-11)
 - Tilgjengelighet (§ 2-12)
 - Integritet (§ 2-13)
 - Sporbarhet, ikke-manipulering og automatisering (§ 2-14)
 - Krav til kvalitet ved overføring av personopplysninger (§ 2-15)

Anbefalt lesing:

Informasjonssikkerhet. Rettslige krav til sikker IKT

Jansen og Schartum (red) (Fagbokforlaget 2005)

Boken er skrevet for å formidle innholdet av reglene på en måte som ikke krever spesiell juridisk kompetanse. Dessuten formidler den generell kunnskap om sikkerhetstenkning, -metodikk og -teknikker, noe som gjør det lettere å forstå de teknologiske implikasjonene.

Boken omfatter regelverk vedrørende:

- * Sikring av personopplysninger
- * Sikker kommunikasjon med og i offentlig forvaltning
- * Elektroniske signaturer (jf. lov om elektroniske signaturer)
- * Krav til informasjonssikkerhet i finansnæringen
- * Sikkerhetsloven og forskrift om informasjonssikkerhet
- * Opphavsrettslige regler vedrørende informasjonssikkerhet
- * Straffelovens bestemmelser vedrørende datakriminalitet

