



Datatilsynet

# **Om manglende tilgang til helseopplysninger.**

## **Datatilsynet**

**Senioringeniør Johan Braar Larsen, Datatilsynet**

**26.09.2006**



# Innhold

- **Innledning og Datatilsynets rolle**
- **Risikovurdering**
- **Sikkerhetsbestemmelser om tilgjengelighet**
- **Normen og tilgjengelighet**
- **Ansvar**

# Personvernutfordringer i dagens digitale samfunn:

- **Den "sentrale databasen"**

- Trusselen fra "den store datamaskinen" er den klassiske årsak til at personvernlovgivning ble satt på agenden for 30 år siden.

**Fra bank husker vi alle konsekvensene av systemer ute av drift – i år var trussel om benkstreik nok til lønnsnemd.**

**Helsesektoren iverksetter nå stadig større baser og systemer hvor konsekvensene av avbrudd blir "alvorlige". Datatilsynet er urolige og sier ofte i fra om dette.**



# Datatilsynets roller



- **Samfunnspåvirkning**
- **Råd og veiledning**
- **Tilsyn og sanksjon**
- **Saksbehandling**  
(regulering / vilkår)

- **Uavhengig forvaltingsorgan**
- **Klageinstans er personvern-nemnda**
- **Samarbeider med andre forvaltningsorgan**  
(informasjonssikkerhet er Datatilsynets ansvar)
- **Bidrar ved personvernombud og bransjenormer**



# Sikkerhetsdefinisjon

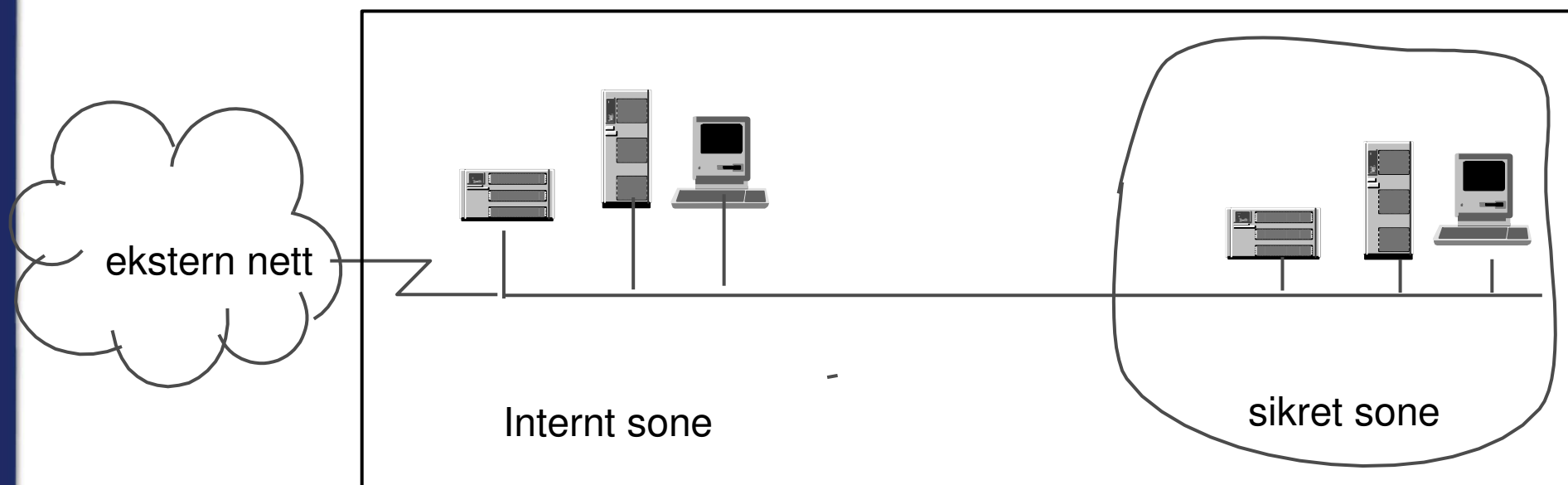
- **Informasjonssikkerhet for å motvirke fare for:**
  - tap av liv og helse,
  - personlig integritet,
  - anseelse, og
  - økonomiske tap
- **Ved slik fare skal planlagte og systematiske tiltak stå i forhold til risiko:**
  - Konfidensialitet
  - Integritet
  - Tilgjengelighet

**Tiltakene består av styringssystem (ansvar og rutiner) og sikkerhetstiltak (teknisk utstyr) som er "risikovurdert" og dokumentert**



# Trusler mot sikkerhet

- Påført av noen fra "utsiden"
- Påført av noen fra "innsiden"
- Andre trusler (feil ved strøm osv.)



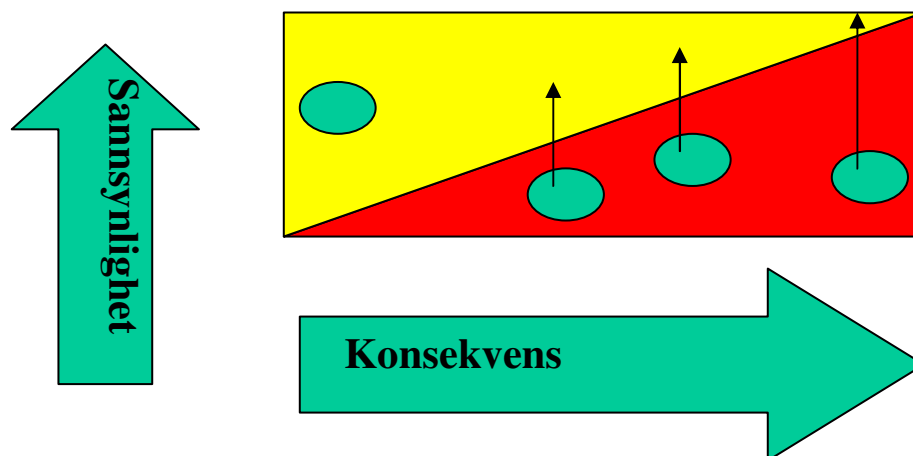
*Selv det med lav sannsynlighet skjer ...*



# Risikovurdering, flere trinn

- Kartlegg og klassifiser alle behandlinger
- Identifiser uønskede hendelser
- Konsekvensvurdering (1-4)
- Sannsynlighetsvurdering (letthet 1-4)

**Sammenlign resultater og iverksett tiltak for å komme innenfor akseptabel risiko (ikke på totalkonsepter, men alle delene)**





# Sikkerhets bestemmelser:

---

## **POF §2-14 om sikkerhetstiltak:**

Sikkerhetstiltak skal omfatte tiltak som ikke kan påvirkes eller omgås av medarbeiderne, og ikke være begrenset til handlinger som den enkelte forutsettes å utføre.

## **POF §2-14 kommentar til tiltak:**

Sikkerhetstiltak bør etableres slik at funksjonen til to uavhengige tiltak må påvirkes før et sikkerhetsbrudd får betydning for konfidensialitet, tilgjengelighet eller integritet for personopplysningene

**Alternativ strømtilførsel, eksterne linjer, databaser er vanlig, men systemer vil ofte ha enkeltkomponenter som ikke dubliseres – disse kan ha begrenset testing av nytt**



# Sikkerhets bestemmelser:

---

## **POF §2-12 om "backup":**

Personopplysninger og annen informasjon som er nødvendig for å gjenopprette normal bruk, skal kopieres.

## **POF §2-12 om "backup":**

.....Kravet til reservekopi gjelder også eksempelvis program og innstillinger til program.....

**I tillegg til å kunne operere når systemet faller ut skal det være mulig å kunne gjenoppta normal bruk av systemet, slik gjenopprettelse vil ha behov for egne planer ....**



# Sikkerhets bestemmelser:

---

## **POF §2-12 om alternativ behandling:**

Alternativ behandling skal forberedes for de tilfeller informasjonssystemet er utilgjengelig for normal bruk.

## **POF §2-12 kommentar til tiltak:**

Alternativ behandling kan gjennomføres ved duplisering av utstyr/program eller ved hjelp av manuelle behandlingsrutiner.

**Alternativ behandling skal testes og kunne gjøres tilgjengelig i forhold til akseptabel "nedetid"....**



# Sikkerhets bestemmelser:

---

## **POF §2-6 om avvik:**

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

## **POF §2-6 om avvik:**

Avviksbehandlingen vil normalt omfatte rapportering, strakstiltak, permanent korrigering...

**Kun avvik som gjelder utlevering av personopplysninger er meldepliktige til Datatilsynet – vi har likevel fått informasjon om enkelte driftsavvik som vi ser alvorlig på og har fulgt opp med saksbehandling og vurderer tilsyn.**



# Sikkerhets bestemmelser:

---

## **POF §2-15 om leverandører:**

Den behandlingsansvarlige skal ha kunnskap om sikkerhetsstrategien hos ”*databehandlere / leverandører – som gjennomfører sikkerhetstiltak*” og jevnlig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet.

## **POF §2-15 om leverandører:**

Dette kan oppnås ved at behandlingsansvarlige meddeles resultater fra ledelsesgjennomganger, sikkerhetsrevisjoner og avviksbehandling som er relevant....

**Tilgang til tjenester er så sentralt at det er naturlig med spesiell krav og oppfølginger – kompetanseforhold er utfordrende i slike avtaler og oppfølging.**



# Normen for sikkerhet.

## **Kartlegging kritikalitet i "systemer":**

- Klassifisere kritisk for pasient / virksomhet
- Klassifisere alvorlige konsekvenser
- Klassifisere svekket tillit og lavprioriterte

## **Fastlegge akseptabel risiko:**

- Minimum inneholde maksimal avbruddstid

## **Etablere tilpassede testede nødprosedyrer:**

- Drift med delvis systemstøtte
- Drift uten bruk av systemene

**Bransjenormen skal medvirke til styrket fokus på tilgjengelighet / nedetid og at ledelsen beslutter konkrete valg på akseptkriteriene.**



# Den behandlingsansvarlige

- **Ansvarlig (fengsel, mulkt, erstatning)**
- **Bestemmer formål og hjelpemidler**
- **Har sikkerhetsansvar i egen virksomhet og ansvar leverandører og databehandlere**
- **Avtale om hva databehandlere mv. gjør**
- **Pliktregler overfor den registrerte**
- **Internkontroll er prinsipløsningen**

**Ledelsen har ansvar for hvilke behandlinger som gjøres og hvilke datasystem som brukes internt og eksternt – samt sikkerhet med "oppetider".**



# Ansvar i ulike virksomheter

## Behandlingsansvarlig

- Har konkret **ansvaret** for at loven etterleves hos seg

## Databehandler

- Den som behandler personopplysninger på vegne av Behandlingsansvarlig. (datasentral må, følge pof 2)

## Leverandør av program ol

- Intet direkte ansvar for loven, men kan være "seriøs" ved å kjenne lovens krav og løsningsmuligheter (mange får nå direkte råd og veiledning om dette fra Datatilsynet)

## •Leverandør / part med IT-tilgang

- Her har behandlingsansvarlig alene ansvar for parten og pof 2) Sertifisering BS7799 eller NS/ISO17799 ?

**Kontrakter er behandlingsansvarliges styringsverktøy!!**



# Personvernombud

**Datatilsynet har intensivert sitt arbeid med å etablere ombud.**

- Dette kan bidra til styrket personvern
- Virksomheten bestemmer selv om eget ombud eller om dette settes ut til andre.

- **Ombudets oppgaver**

- Skal sikre at virksomheten følger loven
- føre meldingsoversikt

- **Virksomhets "fordel"**

- Unntak fra meldeplikt–nær kontakt Datatilsynet



# Ytterligere informasjon

## **WWW.DATATILSYNET.NO**

- Helseregisterloven
- Personopplysningsloven
- Sikkerhetsforskriften med kommentarer
- Veiledning i risikovurdering
- Veiledning for kommuner
- Bransjenorm i sikkerhet for helsesektoren

## **EPOST**

- Postkasse@Datatilsynet.no
- Sikkerhet@Datatilsynet.no

**Ny veiledning i internkontroll utvikles nå**