

# Informasjonssikkerhet, e-forvaltning og juss – kort oversikt og innledning

Seminar om informasjonssikkerhet i offentlig saksbehandling 01.06. 2007

Amund Eriksen, seniorrådgiver

[amund.eriksen@statskonsult.no](mailto:amund.eriksen@statskonsult.no)

Tlf 2245 1259, mobil 4808 4951

# Hva er ”informasjonssikkerhet”?

- Fokus på informasjon som et aktivum, en verdi, av grunnleggende betydning for organisasjonens virksomhet
- En tilstand (tegn/data/informasjon, produkter, organisasjon, mv)
- En prosess (en kontinuerlig prosess)
- Kjernen er sikring av informasjonens autentisitet, tilgjengelighet, integritet, kvalitet og konfidensialitet

# Tre hovedkilder til sikkerhetskrav:

- Juridiske krav (lover, forskrifter, avtaler - interne og eksterne krav – nasjonale og internasjonale)
- Egen vurdering av virksomhetens risiko og muligheter
- Mål, prinsipper og krav som virksomheten selv utvikler for å støtte sin spesifikke virksomhet

# Organisatoriske utgangspunkter

- Ledelsen har ansvaret
- Planverk som virkemiddel for å ivareta ansvaret
- Gunstig å dele mellom operativt ansvar og kontrollansvar
- Sikkerhetsplan/politikk må samordnes med andre planer/politikker - utgjøre en del av VIRKSOMHETS-PLANEN
- Del av årlige rutiner/budsjett og rapporter – på høyeste nivå

# ”Internkontroll”, ”kvalitetssystem”, ”styringssystem”

- systematiske tiltak må etableres (for å påse at kravene etterleves)
- tiltakene må dokumenteres (både at de er etablert og at de følges)
- den enkelte virksomhet har ansvaret
- gir grunnlag for systemrevisjon og/eller verifikasjon (både tilsyn og egen virksomhet)

# Hvilke regelverk i offentlig sektor krever informasjonssikkerhet? (bl.a.)

## Generelle regler:

- Forvaltningsloven, eForvaltningsforskriften, offentlighetsloven og beskyttelsesinstruksen
- Personopplysningsloven og –forskriften

## Spesielle regler:

- Helseregisterloven, helsepersonelloven, norm for informasjonssikkerhet i helsesektoren (sistnevnte = veiledende)
- Beredskapsforskriften i kraftforsyningen
- Esignaturloven med forskrifter

# Blir regelverkene fulgt?

- Altfor få av *regelverksforvalterne* som prøver å finne ut av dette (unntak: eForvaltningsforskriften (FAD) i 2004, og personvernreglene (JD og FAD) i 2006)
- Nye regler bygger sjelden på innhenting av empiri
- Vanskelig for mange å få full oversikt over alle regelverk/rettslige krav
- Forholdet mellom ulike regelverk oppleves vanskelig å forstå
- Stort opplevd gap mellom de rettslige normene og den operative hverdagen

# Blir regelverkene fulgt? (2)

- FAD kartla (ved SK-oppdrag) om eForvaltningsforskriften = ok?, og omarbeidet den og ga den ut i forbedret stand!
- Kartleggingen tilsa at den var lite kjent (i 2003-4); gjelder ennå!
- En fornyet og tredelt veiledning **er laget** og skal publiseres NÅ (juni 2007)
- Dagens ønskedrøm: ingen får gi regler uten også å lage nettbaserte eksempler på hvordan de kan etterleves (konkrete rutiner for typiske områder for saksbehandling)



# Noen dokumenter om informasjonssikkerhet og juss:

- *Nasjonal strategi for informasjonssikkerhet (2003-06): eksisterende regler må komme i bedre praktisk bruk*
- *Forprosjektrapport fra en arbeidsgruppe til Koordineringsutvalget for informasjonssikkerhet (KIS); Regelverk og informasjonssikkerhet, juni 2005*
- *Regelverk og informasjonssikkerhet; eksempler på brukererfaringer, rapport fra Statskonsult til MOD (nå FAD), september 2005*
- *Arbeid med informasjonssikkerhet; fra juss til styring og rutiner, rapport fra Statskonsult til FAD, mars 2006*

# Typisk tilnærming i dagens regelverk:

- Gir støtte til **ledelsens** ansvar for ivaretagelse av informasjonssikkerhet, og til dokumentasjon av ledelsesprosesser
- Gir liten støtte til **saksbehandlernes** mulighet for å etterleve kravene til informasjonssikkerhet i den operative saksbehandlingen
- Gir få eller **ingen krav til** at en virksomhet **dokumenterer** etterlevelse av informasjonssikkerhet i saksbehandlingen/**rutiner** for saksbehandlingen

# Ovenfra og ned, - eller nedenfra og opp?

- Overordnede normer i lover og forskrifter mv
- Styringssystemer
- Det operative plan/saksbehandling/produksjon; ofte styrt av en blanding av særregelverk og generelt regelverk, hvor ingen har tenkt på hvordan en i praksis skal klare å både oppdage og deretter etterleve alle kravene

# Statskonsult har mange jordnære forslag til forbedringer....

- Lage modeller og veiledninger for bedre å skille mellom informasjonssikkerhet på styrings- og operativt nivå
- Etablere praksisfellesskap – deling – gratis utveksling av eksempler! F.eks ta i bruk Kunnskapsnettverket
- Finne og vise frem eksempelprosesser – vise sammenheng regelkrav og rutiner for etterlevelse i praksis

– *Og mange, mange, mange andre gode forslag. Bare se i de nevnte rapportene.*