

# Krav til informasjonssikkerhet

DRI1010 – forelesning 15.03.2012

Jon Berge Holden – [jobe@holden.no](mailto:jobe@holden.no)

# Sikkerhet - hva skal beskyttes?

- Informasjonssikkerhet (def. ISO 27001, 3.4)
  - Bevare konfidensialitet, integritet og tilgjengelighet. Dessuten kan andre egenskaper, som autensitet, ansvarlighet, uavviselighet og pålitelighet, omfattes.
- Konfidensialitet
  - Vern mot uautorisert innsyn
- Integritet
  - Vern mot uautorisert endring/tap
- Tilgjengelighet
  - Tilgjengelig på behov

# Regelverk for sikkerhet og etterlevelse (internkontroll)

- Personopplysningsloven §§ 13 og 14
  - Forskriften kapittel 2 og 3
- eforvaltningsforskriften, § 13 m.fl.
- Taushetsplikt, eks. fvl §13
- Andre generelle regelverk
  - Sikkerhetsloven & informasjonssikkerhetsforskriften
  - Beskyttelsesinstruksen, for statlig sektor
  - Økonomiregelverket
- Andre spesielle regelverk
  - Helseregisterloven, ikt-forskriften

# Direktivet

- Behandlingssikkerhed, artikel 17:
  - 1. Medlemsstaterne fastsætter bestemmelser om, at den **registeransvarlige** skal iværksætte de **fornødne tekniske og organisatoriske foranstaltninger** til at beskytte personoplysninger **mod hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang**, navnlig hvis behandlingen omfatter fremsendelser af oplysninger i et net, samt mod enhver anden form for **ulovlig behandling**.
  - <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DA:NOT#texte>

# Informasjonssikkerhet, pol § 13

- **§ 13. Informasjonssikkerhet**
- Den behandlingsansvarlige og databehandleren skal gjennom **planlagte og systematiske** tiltak sørge for **tilfredsstillende informasjonssikkerhet** med hensyn til **konfidensialitet, integritet og tilgjengelighet** ved behandling av personopplysninger.
- For å oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige og databehandleren **dokumentere** informasjonssystemet og sikkerhetstiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernemnda.
- En behandlingsansvarlig som lar **andre** få tilgang til personopplysninger, **f.eks. en databehandler eller andre som utfører oppdrag** i tilknytning til informasjonssystemet, skal **påse at disse oppfyller kravene** i første og annet ledd.
- Kongen kan gi **forskrift** om informasjonssikkerhet ved behandling av personopplysninger, herunder nærmere regler om organisatoriske og tekniske sikkerhetstiltak.

# Personopplysningsloven

- "Tilfredsstillende informasjonssikkerhet", § 13
  - Tiltakene skal "stå i forhold til sannsynlighet for og konsekvens av sikkerhetsbrudd", pof [§2-1](#)
  - Tiltak pålegges hvis "er nødvendig", pof §§2-11 til 2-13, dog: fnr i særstilling pof [§10-2](#)
- Internkontroll som "er nødvendig", § 14
  - "tilpasses virksomhetens størrelse", pof § 3-1
- Prosesskrav - planmessig, systematisk
  - Risikovurdering, [§2-4](#), sikkerhetsrevisjon, §2-5
- Dokumentert
  - Sikkerhetsmål, -strategi, §2-3, rutiner, §2-16 mfl

# Risikovurdering

- Tiltak skal stå i stil med risiko, pof §2-1
- Risiko er
  - sannsynlighet x konsekvens
- Sannsynlighet: Letthet, motivasjon, frekvens
- Konsekvenser
- [Datatilsynets veileder i risikovurdering](#) (TV-506:2002, opptrykt 06.03.09)
- Generelt om risikostyring i staten (SSØ)
- [Veileder fra Difi](#)

K4				R4
K3			R3	
K2		R2		
K1	R1			
Konsekvens (K)/ Sannsynlighet (S)	S1	S2	S3	S4

# Internkontroll, pol § 14

- **§ 14. Internkontroll**
- Den behandlingsansvarlige skal etablere og holde vedlike **planlagte og systematiske** tiltak **som er nødvendige** for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes **kvalitet**.
- Den behandlingsansvarlige skal **dokumentere** tiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernemnda.
- Kongen kan gi **forskrift** med nærmere regler om internkontroll.



# Full kontroll

- Pol § 14 – internkontroll
  - Etterlevelse av pliktene
  - Inkl. sikkerhet
- Pol § 15 – databehandleravtale
  - Bestemmelsesrett
  - Informasjonssikkerhet
- § 14
  - Den behandlingsansvarlige skal etablere og holde vedlike **planlagte og systematiske tiltak som er nødvendige** for å oppfylle kravene i eller i medhold av denne loven, herunder sikre personopplysningenes **kvalitet**.
  - Den behandlingsansvarlige skal **dokumentere** tiltakene. ...
  - Kongen kan gi **forskrift** med nærmere regler om internkontroll.

# Eforvaltningsforskriften

- Forankret i forvaltningsloven § 15a (og esignl)
- Formål, § 1:
  - legge til rette for **sikker og effektiv bruk** av elektronisk kommunikasjon med og i forvaltningen
  - legge til rette for at enhver på en **enkel måte** kan utøve sine rettigheter og oppfylle sine plikter i forhold til det offentlige

# Eforvaltningsforskriften, 2

- Sikkerhetsstrategi og sikkerhetsmål skal ligge til grunn for beslutninger om s.-tjenester m.v., § 13
- Kan enhver bruke e-kommunikasjon til organet?
  - Utgangspunkt: fritt fram, § 3 nr 2
  - Sikkerhetspålegg må være rimelige, § 4 nr 1-3
    - Dog nødvendig hvis taushetsplikt, § 5 nr 1
  - Organet må tilby eller peke på løsninger, § 4 nr 4
  - Veiledningsplikt om restrisiko, § 5 nr 2
- Underretning, § 8 – særlige varslingsregler
- Grundig veileder

## Eforvaltningsforskriften, 3

- “Sikkerhetsstrategien skal danne grunnlaget for forvaltningsorganets beslutninger om innføring og bruk av sikkerhetstjenester og -produkter på en helhetlig, planlagt, systematisk og dokumentert måte. Sikkerhetsstrategien skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.” (§13 nr 1)

# Forvaltningsloven

- § 13 – taushetsplikt: enhver ... hindre ... andre .. adgang ... kjennskap ... det han ... får vite om ... personlige forhold.../konkurransmessig betydning
  - § 13c – oppbevares på betryggende måte
- § 15a – hjemler e-forskrifter
  - Eforvaltningsforskriften, 2004/0988
  - Koef-vedtaket, 2005/1117, jf. efvf § 27
  - Forskrift om it-standarder, 2009/1222

# Kort om sikkerhetsloven

- Formål, jf. § 1
  - ”motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser...”
- Gradering, § 11 – STRENGT HEMMELIG/ HEMMELIG/ KONFIDENSIELT/ BEGRENSET
  - Skade hvis informasjonen kommer på avveie (ref. § 1)
- Streng need-to-know, § 12
- NSM-godkjenning av informasjonssystemer, § 13, m.v.
- Forskrifter
  - Informasjonssikkerhetsforskrift m.v. med detaljerte sikringsregler
    - [Objektsikkerhetsforskriften](#)

# Kort om beskyttelsesinstruksen

- Instruks for statsforvaltningen
- Gradering (§ 2)
  - STRENGT FORTROLIG eller FORTROLIG
- Vurderingstema (§ 4)– skade/betydelig skade mht.
  - offentlige interesser, en bedrift, en institusjon eller en enkeltperson at dokumentets innhold blir kjent for uvedkommende
- Konsekvenser
  - Strengt need-to-know-prinsipp, § 7 – personlig ansvar
- Elektronisk behandling ”så langt det passer” ihht. deler av informasjonssikkerhetsforskriften etter sikkerhetsloven, jf. § 12

# Klassifisering av informasjonsaktiva

- Før risikovurdering, anbefales en kartlegging av informasjonsverdier
  - Personopplysningsloven
    - Vanlig personopplysning, sensitiv personopplysning
  - Offentlighetsloven
    - Offentlig, kan unntas, vurdert meroffentlig
  - Taushetsplikt
    - Forvaltningsloven,
    - Beskyttelsesinstruksen
    - Sikkerhetsloven
- Rapport - klassifisering og beskyttelse av informasjon (KOBI), KIS 2008.
  - 4 klasser for konfidensialitet, integritet, tilgjengelighet, kap 7.2
- Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor
  - 4 risikoklasser, se veiledning



# Kort om elektronisk signatur

- [Esignaturloven § 3](#) definerer tre typer e-signaturer
  - Nr 1: (vanlige)
  - Nr 2: Avanserte
  - Nr 3: Kvalifiserte
- Hva kreves?
  - Prosessrettslig, privatrettslig, forvaltningsrettslig utgpkt
    - Fri bevisbedømmelse, formfrihet, forsvarlig saksbehandling
  - Regelverket gir tidvis avklaring
  - Risikovurdering!
- Merk [efvf § 26](#) nr 2 – langtidslagring
  - arkivet vil kunne bryte signaturen, må da gå god for bindingen

# Økonomiregelverket (ikke pensum)



- Formål, § 1: ... sikre at ...
  - b) fastsatte **mål og resultatkrav oppnås**
  - c) statlige midler brukes **effektivt** ...
- Grunnleggende styringsprinsipper, § 4:
  - b) sikre at fastsatte mål og resultatkrav oppnås, ressursbruken er effektiv og at virksomheten **drives i samsvar med gjeldende lover og regler**,
  - Styring, oppfølging, kontroll og forvaltning må tilpasses virksomhetens **egenart samt risiko og vesentlighet**
- Krav om internkontroll, § 14:
  - Alle virksomheter skal etablere systemer og rutiner som har innebygd **intern kontroll** for å sikre at: ...
    - b) måloppnåelse og resultater står i et tilfredsstillende forhold til fastsatte mål og resultatkrav, og at eventuelle vesentlige avvik forebygges, avdekkes og korrigeres i nødvendig utstrekning
- [Veiledning](#) hos DFØ

# Hvor svikter det?

- Riksrevisjonens undersøkelse av informasjonssikkerheten i alle departementene og 34 virksomheter
- Merknader til
  - 11 departement – manglende styring
  - 10 virksomheter – vesentlige mangler
- [Dokument 1 \(2010-2011\)](#)
  - Oppsummering del II, kap 3, s 21-22



# Riksrevisjonen november 2011

- **Enkeltområder som Riksrevisjonen er særlig kritisk til:**
- **Informasjonssikkerhet i departementene**
- Riksrevisjonen ser alvorlig på at Fornyings-, administrasjons- og kirke departementet ikke har sikret at infrastrukturen som departementene benytter, har tilfredsstillende sikkerhet. Departementenes servicesenter har fortsatt vesentlige mangler på informasjonssikkerhetsområdet.
  - [Riksrevisjonens pressemelding 22.11.2011](#)
- I Dokument 1 (2010–2011) ble det rapportert om til dels alvorlige svakheter og mangler innenfor informasjonssikkerhetsområdet. Merknadene var blant annet knyttet til **manglende identifisering og klassifisering av informasjonsaktiva, ufullstendige risikoanalyser og mangelfull beskyttelse av ikt-infrastruktur**. Årets revisjon har vist at det er iverksatt tiltak for å bedre informasjonssikkerheten, men at det vil ta tid før disse får ønsket effekt. Riksrevisjonen vil følge opp informasjonssikkerheten i forvaltningen i den løpende revisjonen.
  - [Dokument 1 \(2011-2012\)](#), Riksrevisjonens rapport til Stortinget for året 2010

# Eksempel på mangler

- Revisjonen viser flere svakheter knyttet til informasjonssikkerheten i SPK:
  - Det er ikke utarbeidet en **sikkerhetspolicy**, og SPK har ikke etablert en **sikkerhetsorganisasjon** med **klart definerte roller, oppgaver og ansvar** for informasjonssikkerheten
  - Det er svakheter og mangler i beskyttelse av **ikt-infrastruktur** knyttet til driftsadministrasjon og administrasjon av tilganger
  - Overordnet **kontinuitetsplan** gir **ikke en helhetlig oversikt** over hvilke prosedyrer som vil være aktuelle å benytte ved en krise, og kontinuitetsplanen er ikke **testet**
  - (2.1.1, s 33)

# Eksempel på styringssvikt

- Departementet opplyser at styringen av underliggende virksomheter blant annet baserer seg på at det stilles **krav om dokumentasjon** av internkontrollsystemene. (2.1.1, s 33)
- Riksrevisjonen
  - Riksrevisjonen konstaterer at departementet, ut fra sin oppfatning om **risiko og vesentlighet, ikke har kontrollert** om SPK faktisk har gjennomført tiltak og utarbeidet dokumenter slik departementet har forutsatt.
  - I lys av at departementet har **vurdert pensjonsprosessen som samfunnskritisk**, stiller Riksrevisjonen **spørsmål om oppfølgingen har vært tilstrekkelig**. (4.5, s 47)
  - Riksrevisjonen forutsetter at Arbeidsdepartementet bedre tilpasser styring og oppfølging etter **egenart og risiko** i SPK (6.2.1, s 57)

# Eksempel på mangler, 2

- Revisjonen viser flere svakheter i informasjonssikkerheten i etaten:
  - Det gjennomføres risikovurderinger på forskjellige nivåer i organisasjonen, men det er ikke et tilfredsstillende system for å **samle og strukturere** denne informasjonen
  - Det er enkelte svakheter og mangler knyttet til **driftsadministrasjonen**
  - **Mange saksbehandlere har tilgang** til sensitiv informasjon
  - Etatens **kontinuitetsplan** for å gjenopprette drift av ikt-systemer **dekker ikke alle** systemer, er ikke oppdatert, og **testing** av deler av planen er ikke dokumentert
  - Det er mangler i **kunnskap og bevissthet** om informasjonssikkerhet blant etatens ansatte
  - (2.3.6, s 43)

# Eksempler på mangler, 3

- Husbanken
  - ... ikke har ivaretatt kravet om informasjonssikkerhet godt nok i **avtaler med eksterne partnere**, og avtalene nevner heller ikke at det kan foretas **revisjon av tredjepart eller outsourcingaktør**. (1.3.1 s 180)
- Kunnskapsdepartementet
  - Riksrevisjonen konstaterer at enkelte av virksomhetene underlagt Kunnskapsdepartementet ikke har tilfredsstillende **oversikt over hvilke verdier de besitter**.