
Regelverk og informasjonssikkerhet; eksempler på brukererfaringer

Rapporten er utarbeidet av Statskonsult på oppdrag fra Moderniseringsdepartementet. Arbeidet er basert på intervjuer med næringsliv, kommunale og statlige virksomheter.

Statskonsult, 5. september 2005

Innhold

1	Oppsummering	3
2	Bakgrunn, mandat og gjennomføring.....	5
2.1	Bakgrunn	5
2.2	Mandat.....	5
2.3	Gjennomføring	5
3	Problemstillinger fra intervjuene.....	6
4	Kort fra de enkelte intervjuer	10
4.1.1	Norsk Hydros Pensjonskasse	10
4.1.2	Kommunal landspensjonskasse (KLP).....	10
4.1.3	Erfaringer fra tre kommuner	11
4.1.4	Ullevål universitetssykehus.....	13
4.1.5	Helse Vest IKT AS.....	14
	Vedlegg i separat dokument.....	16

1 Oppsummering

Moderniseringsdepartementet har ønsket å få dokumentert konkrete brukererfaringer med regelverket for informasjonssikkerhet, og ga Statskonsult dette i oppdrag i begynnelsen av juli 2005. Det er gjennomført intervjuer med Norsk Hydros Pensjonskasse, Kommunal landspensjonskasse, Gjøvik, Sør-Odal og Larvik kommuner, Ullevål universitetssykehus og Helse Vest IKT AS, og det er samlet inn eksempler på hhv styringssystem, kvalitetssystem og internkontrollsystem for informasjonssikkerhet.

Oppdraget har vært å finne eksempler på brukererfaringer, uten krav til representativitet.

Intervjuene viser at brukerne har delte oppfatninger om regelverket og hvor enkelt eller vanskelig det er å etterleve. Det fremkommer likevel en del forhold som mange nevner og gir eksempler på:

- **Vanskelig å etablere full oversikt over regelverket**
Virksomhetene gir uttrykk for at det er vanskelig å etablere full oversikt over regelverket. Selv virksomheter som mener de har god oversikt har mangelfull liste over lover og forskrifter i sitt internkontrollsystem. Det ser ut til at det særlig er eForvaltningsforskriften som er lite kjent. I mange virksomheter overlates det til avdelingsnivå å holde oversikt over særlovgivning.
- **Hvilke deler den operative virksomheten berøres av de ulike kravene?**
Det ser ut til å være et problem å relatere de ulike kravene i lov og forskrift til de mer operative delene av virksomheten. Larvik kommune som har tatt utgangspunkt i ISO 9000-basert kvalitetssystem, ser ut til å ha lyktes relativt godt med å implementere regelverket ned på det operative planet.
- **Overdimensjonert fokus på styring?**
Flere av virksomhetene har arbeidet i ett til flere år bare med å etablere styringssystem for informasjonssikkerhet. Selv om styringssystemet er på plass, er det lang vei igjen til at regelverket er implementert og etterleves på det operative planet.
- **Ett eller flere internkontrollsystemer?**
Flere av virksomhetene gir uttrykk for at internkontrollkrav fra ulike myndigheter ikke må forutsette ett kontrollsystem for hvert sett av krav. På operativt nivå, hvor ansatte i næringsliv, kommune og stat skal utføre sine daglige gjøremål, må det etableres arbeidsrutiner som ivaretar summen av de krav som skal etterleves. Det må skje en omforming fra krav til arbeidsrutine. Det må ikke være slik at det blir en arbeidsrutine for hver type krav.

-
- **Vanskelig begrepsbruk**
Flere angir at det brukes et juridisk språk som er vanskelig tilgjengelig, også i veiledninger. Ulike myndigheter benytter ulike begreper på samme sak. Det tydeliggjør et behov for tettere samarbeid mellom de ulike myndighetene. Det pekes også på behovet for mer tverrfaglig innsats (dvs ikke bare juss) når regelverk og veiledninger skal utformes.
 - **Behov for bedre veiledning ved direkte henvendelse**
Det pekes på at man ikke alltid får hjelp når man henvender seg til myndigheter med tolkningsproblemer.
 - **Det oppleves at forholdet mellom ulike regelverk er vanskelig å forstå**
Informantene angir ikke spesielt at det er overlapp mellom regelverk. Det anføres derimot at forholdet mellom taushetspliktsregler, personvernregler, informasjonssikkerhetsregler og samarbeids- og til dels innsynsregler kan by på store praktiske problemer. Det oppleves at juridisk virkelighet er vanskelig å trenge inn i, og at myndighetenes tolkning kan gå på tvers av den operative virkelighet i virksomhetene. Informanter oppgir at de opplever at det er for lite samordning mellom IKT-forskriften, Internkontrollforskriften og personopplysningsloven og –forskrift, samt mellom Kredittilsynet og Datatilsynet. Norsk Hydros Pensjonskasse har laget en illustrerende oversikt over internkontrollkravene og sammenhengen mellom disse for de nevnte regelverkene. Det pekes også på at man ikke har fått noen informasjon eller veiledning om hvordan de ulike regelverkene henger sammen.
 - **Stort gap mellom rettslige normer og operativ hverdag**
Brukerne opplever at det er et svært stort gap mellom de til dels svært juridisk formulerte rettslige normene i regelverkene og brukernes operative hverdag. De opplever at de ikke får noen hjelp fra myndighetene til å fylle dette gapet. Reglene sier mest om *hva* som skal gjøres, lite eller ingenting om *hvordan*. Heller ikke veiledninger, skriftlige eller muntlige, makter dette i nevneverdig grad. Brukerne peker på at det mangler viktige ledd mellom de formulerte kravene i regelverkene, og den operative gjennomføringen eller etterlevelsen av dem. Det pekes også på at det er behov for veiledninger som gir eksempler på bruk av beste praksis. Brukere er kritiske til at de ansvarlige myndighetene ikke i større grad har samarbeidet for å hjelpe brukerne med denne praktiske implementeringen, og at regelverkene (og myndighetene) i for liten grad skiller mellom store og små virksomheter. For de små oppleves det særlig byrdefullt og urimelig å måtte sette seg inn i og følge like mange og like omfattende regler som de store.

2 Bakgrunn, mandat og gjennomføring

2.1 Bakgrunn

Bakgrunnen for rapporten er at Moderniseringsdepartementet ønsket å få frem noen konkrete eksempler på erfaringer og problemer brukerne opplever i forbindelse med regler for informasjonssikkerhet. Oppdraget ble gitt til Statskonsult.

2.2 Mandat

Moderniseringsdepartementet ga som mandat for oppdraget å finne ”frem til eksempler på konkrete problemer som brukerne opplever knyttet til implementering av regelverk for informasjonssikkerhet, og særlig problemer knyttet til overlapp mellom de ulike reguleringene.” Dessuten ville det være ”interessant å se på konkrete eksempler på problemer med uklart, mangelfullt eller overlappende regelverk. Det er ønskelig å få frem minst ett konkret eksempel fra henholdsvis en SMB-bedrift, en kommune og en statlig virksomhet. Eksemplene skal dokumenteres i en rapport og med inntil to sider lesevennlig oppsummering. Rapporten skal foreligge til møte i KIS 13. september, dvs ca 5.september.”

2.3 Gjennomføring

Arbeidet er gjennomført i perioden primo august til og med 5. september, 2005 av seniorrådgiverne Margaret Hagevik, Kirsti Berg og Amund Eriksen, Statskonsult.

For å finne frem til interessante informanter, fikk Statskonsult hjelp fra lederen av en arbeidsgruppe for juss og informasjonssikkerhet under IT-Sikkerhetsforum (ISF)¹. I tillegg tok vi kontakter med flere i kommunesektoren, dels gjennom foreningen KINS (Kommunal Informasjonssikkerhet), samt med Post- og teletilsynet, Nasjonal sikkerhetsmyndighet og Datatilsynet.

Intervjuer er gjennomført med Norsk Hydros Pensjonskasse, KLP (Kommunal Landspensjonskasse), Gjøvik kommune, Sør-Odal kommune, Larvik kommune, Ullevål universitetssykehus og Helse Vest IKT AS. Se de enkelte intervjuene gjengitt i vedlegg 1.

Vi har også mottatt eksempler på en rekke dokumenter fra ulike styringssystem, kvalitetssystem og internkontrollsystem fra henholdsvis Sør-Odal kommune, Larvik kommune og Helse Vest IKT AS. Se nærmere i vedleggene 2, 3 og 4.

Fra Datatilsynet har vi mottatt utdrag fra tilsynsrapporter relatert til sikkerhet 2001 – 2005, Datatilsynet august 2005, som gir konkret oversikt og innblikk over en rekke av de mest erfarte problemene ved gjennomførte tilsyn med informasjonssikkerhet, knyttet til personopplysninger. Se vedlegg 5

¹ *Veiledning lover og regler med betydning for informasjonssikkerhet*, som fantes i opprinnelig versjon 1.0 pr mars 2003, erstattet av versjon 1.1 september 2004. Veiledningen gir en bred oversikt over lover og regler som regulerer informasjonssikkerhet for norske virksomheter. Det sto en arbeidsgruppe bak med representanter fra mange bransjer og sektorer, bl.a. statlig, kommunal, bank, forsikring, industri, shipping, kraft, telekommunikasjon, forsvar mv. Gruppen ble ledet av Lars Erik Fjørtoft, Deloitte & Touche.

I vedlegg 6 har vi gjengitt et svarbrev til Helse Vest fra Sosial- og helsedirektoratet, *Ad tilgang til pasientinformasjon i helseforetak og på tvers av helseforetak*, fra mai 2005.

I vedlegg 7 er enkelte begreper forklart.

Informantene har uttrykt ønske om at den tilsendte systemdokumentasjonen ikke offentliggjøres uten nærmere avtale. Vi mener at heller ikke intervjuene i sin rå form, slik de fremgår av vedlegg 1, bør publiseres. Ved en eventuell publisering, foreslår vi at rapporten og vedleggene 5-7 publiseres.

3 Problemstillinger fra intervjuene

Ikke full oversikt over regelverkene

Flere av informantene angir at det er vanskelig å etablere oversikt over lover og forskrifter som berører informasjonssikkerhet. Når vi ser på eksemplene på internkontrollsystem fra noen av de intervjuende virksomhetene, ser vi at det kun er en del av de aktuelle lover og forskrifter som er nevnt. Man tar gjerne utgangspunkt i lov om personopplysninger. Oversikt over aktuelle særlover er gjerne overlatt til avdelingsnivå. Selv en virksomhet som er sertifisert av Det Norske Veritas etter NS7799, har ikke nevnt alle relevante lover og forskrifter.

Virksomhetene har høyst ulik kjennskap til hvilke regelverk som gjelder for dem mht informasjonssikkerhet, - fra de som sikkert hevdet at de hadde full oversikt (som viste seg å ikke stemme helt), til de som ga uttrykk for at de slett ikke er sikre på om de har full oversikt, eller omvendt: temmelig sikre på at de ikke har full oversikt.

Det regelverket som er minst kjent, er sannsynligvis eForvaltningsforskriften (til forvaltningsloven). Dette er bekymringsfullt, ettersom den utfyller forvaltningsloven, og gir en rekke premisser for hele offentlig sektors måte å tilrettelegge elektronisk kommunikasjon på (stat, fylkeskommune og kommune), med informasjonssikkerhet som et sentralt premiss. I en kvantitativ spørreundersøkelse Statskonsult gjorde våren 2004 på oppdrag fra Moderniseringsdepartementet, kom det frem at av de som svarte var det litt under 30 % i statsforvaltningen som kjente til forskriften, litt under 40 % i fylkeskommunene, og under 10 % av kommunene! Intervjuene gjennomført nå i august 2005 kan indikere at mangelen på kjennskap til eForvaltningsforskriften fremdeles er omfattende. Dette gjelder både store og små virksomheter.

Vi har inntrykk av at personopplysningsloven med forskrift er godt kjent både i offentlig og privat sektor. Tilsvarende at i helsesektoren er de ulike helselovene godt kjent.

På den annen side er kjennskap til eksistensen av regelverket ikke det samme som god kjennskap til innholdet, eller hvordan det skal implementeres.

Enkelte av de intervjuede virksomhetene ønsker bedre veiledning og helst med konkrete eksempler. Statskonsult vil peke på at et slikt arbeid kunne gi stor gevinst for kommunene, i og med at arbeid som gjøres for én kommune vil ha stor overføringsverdi til andre kommuner. For andre typer virksomheter må det større grad av skreddersøm til.

Hvilke deler av regelverket gjelder for de ulike delene av virksomheten?

Manglende oversikt over regelverket er den ene siden av problemet. Like viktig er at det ser ut til å være problemer knyttet til å relatere de ulike lover og forskrifter til det praktiske arbeidet i de ulike deler av virksomheten. Ikke minst ser det ut som det er vanskelig å implementere lover og forskrifter ned på det operative nivået.

For å kunne etablere en god internkontroll, er det en forutsetning at virksomhetene har oversikt over hele regelverket, hvilke deler av regelverket som gjelder de ulike deler av virksomheten, og hvilke arbeidsoperasjoner som må hensynta de ulike krav. Hensikten med et internkontrollsystem er nettopp å dokumentere hvordan de ulike kravene blir ivaretatt. Da må man ned på det operative nivået og vise hvordan ulike regler ivaretas gjennom de faktiske arbeidsprosessene. Larvik, som har tatt utgangspunkt i ISO 9000-basert kvalitetssystem, har lyktes relativt godt med å implementere regelverket ned på det operative planet (for de regelverk som er identifisert).

Forholdet mellom styringssystem og arbeidsrutiner på operativt nivå.

I følge informantene tar det ett til flere år å etablere et overordnet styringssystem for informasjonssikkerhet. Da er kravene ennå ikke implementert i arbeidsprosessene på operativt nivå. Noen gir uttrykk for at det kan være vanskelig å forstå hvilke aktiviteter de ulike internkontrollkravene bør kunne ut i.

Der hvor virksomheten har implementert et kvalitetssystem fra før, tar det kortere tid å implementere nytt regelverk. Dette skyldes at reglene innbakes i eksisterende system.

Statskonsult vil peke på at det ser ut som om styringsdelen av internkontrollvirksomheten har fått overdimensjonert plass i arbeidet i forhold til den praktiske tilnærmingen på operativt nivå.

Det er i det hele tatt en lang vei fra kravene i de enkelte regelverkene til konkret etterlevelse i hverdagens saksbehandling og gjøremål.

Et annet forhold som flere peker på er at regelverkene ikke ser til å skille mellom store og små virksomheter; alle skjæres over en kam og skal tilsynelatende etterleve de samme kravene enten man har to ansatte eller fem hundre. Store regelverk og små virksomheter går ikke alltid så bra sammen. Man blir oppgitt.

Ett eller flere internkontrollsystemer?

Flere av informantene gir klart uttrykk for at internkontrollkrav fra ulike myndigheter ikke må forutsette ett internkontrollsystem for hvert sett av krav. På det operative nivået, hvor ansatte i næringsliv, kommune og stat skal utføre sine daglige gjøremål, må det etableres arbeidsrutiner som ivaretar summen av de krav som skal etterleves. Det må skje en omforming fra krav til arbeidsrutine. Noen har pekt på ISO 9000-serien som et godt utgangspunkt for etablering av arbeidsrutiner, og som egner seg som sentralt system hvor de ulike internkontrollkravene kan innarbeides.

Statskonsult vil gjerne peke på at dette er en kjent problemstilling fra HMS-området. Da Internkontrollforskriften (HMS) ble lansert, førte det til at mange virksomheter som hadde et kvalitetssystem fra før, etablerte et HMS-system ved siden av, for å oppfylle de nye kravene. Etter en stund så man at

dette var en uheldig praksis, og mange så fordelene av å implementere Internkontrollforskriftens krav i kvalitetssystemet.

Vanskelig begrepsbruk

Mange har påpekt at vanskelig begrepsbruk i regelverkene skaper uklarheter. Dette oppfattes nok ikke like problematisk av alle – de som er bevisste på dette og gjør en ekstra innsats, har ikke nødvendigvis store problemer. Dermed ikke sagt at de synes dette er en heldig tilstand; den samlede kompleksiteten blir større, og det blir også den tilhørende tids- og ressursbruken.

Ett eksempel på ulike begreper som brukes om tilnærmet samme forhold er henholdsvis ”*behandlingsansvarlig*” (Personopplysningsloven) og ”*databelandlingsansvarlig*” (Helseregisterloven), som i begge lover er ”*den som bestemmer formålet med behandlingen av helseopplysningene og hvilke hjelpemidler som skal brukes*”. Dette er gjort med vilje av regelmakerne. Om det er lurt for brukerne, er en annen sak; ikke alle er fornøyde.

Andre begreper som brukes til dels om hverandre, og til dels med uklart innhold, er sikkerhetsmål og sikkerhetsstrategi, sikkerhetspolicy (alle med informasjons- eller –IT eller –IKT foran), styringssystem, risikoanalyse, risikovurdering, handlingsplan, tiltaksplan, kvalitetsmål, prinsippnotat, mv. Det nærmere hierarkiet i eller mellom de av begrepene som henger sammen, synes også uklart for mange.

I det hele tatt kan vanskelig begrepsbruk virke forvirrende og føre til at brukerne lurer på om det er en eller flere aktiviteter det er snakk om, og hvilken sammenheng det er mellom dem. Se også nedenfor om juridisk språk.

Noen informanter mener at man bør legge seg opp mot begrepsbruken i ISO 9000. Velinnarbeidede begreper fra ISO 9000, som for eksempel ”ledelsens gjennomgang”, bør ikke gis andre ord i de ulike regelverkene.

Overlapp mellom regelverk og myndighetsområder

Informantene har ikke generelt hevdet at det er problem med overlapp mellom regelverk, utover det som kommer frem under andre overskrifter her.

Det er imidlertid understreket at forholdet mellom taushetspliktregler, personvernregler, informasjonssikkerhetsregler og samarbeids- og til dels innsynsregler, kan by på store praktiske vanskeligheter. Da snakker vi om reglene om slike forhold i helseregisterloven, helsepersonelloven, forvaltningsloven, personopplysningsloven, alle med forskrifter, samt reglene om internkontroll i ulike regelverk, og i Internkontrollforskriften. I tillegg om Sosial- og helsedirektoratet, Datatilsynet, samt flere departementer. Dessuten om de veiledninger og råd disse til sammen gir, skriftlig og muntlig. Noen av problemstillingene er tatt opp av Helse Vest IKT AS, i brev til Sosial- og helsedirektoratet, og i deres svarbrev, se vedlegg 6. Det oppleves at juridisk virkelighet er vanskelig å trenge inn i, og at den med myndighetens tolkning er på tvers av det operative livets virkelighet.

I tillegg oppgir informanter at de delvis opplever for lite samordning mellom IKT-forskriften, Internkontrollforskriften og personopplysningslov og – forskrift, samt mellom Kredittilsynet og Datatilsynet. Informanten fra Norsk Hydro Pensjonskasse har laget en illustrerende oversikt over internkontroll rammeverk og sammenhengen mellom disse, fra de nevnte regelverkene. Dette er plassert til slutt i intervjuet med nevnte pensjonskasse, se vedlegg 1, som ett av flere mulige eksempler. Det pekes blant annet på at det ikke er mottatt noe

informasjon fra regelverksforvalterne om hvordan de forskjellige regelverkene henger sammen.

Samarbeid mellom ulike myndigheter, og behovet for tverrfaglighet

Informanter peker på at det i stor grad brukes et for juridisk språk; at reglene virker som de er laget av og for jurister. Denne kritikken rammer også veiledninger, som ikke oppleves tilstrekkelig orientert mot det operative, praktiske, gjennomføringsmessige. Det sies mye om *hva*, men ikke på langt nær nok om *hvordan*. Dette tolkes i retning av at de som lager reglene (jurister og myndigheter) er for alene om å lage dem, og vet for lite om det praktiske livets krav.

De ulike myndighetene har en tendens til å se for isolert på sine egne krav.

Det bør f.eks. etableres en forståelse hos myndighetene for at det kun kan være ett system på det operative nivået der de daglige gjøremål skal utføres. Man kan ikke ha flere arbeidsrutiner for samme arbeidsoppgave. Det må lages arbeidsrutiner som ivaretar alle de aktuelle krav i lov og forskrift. Dette er et av de vanskeligste punktene for det praktiske liv; hvordan etterleve et antall krav fra flere regelverk, på en måte som er helhetlig, praktisk, forståelig og effektiv.

Dette tilsier tverrfaglig samarbeid i betydelig større grad enn i dag (jurister og andre berørte, med relevante fagkompetanser), samt tilvarende tverrgående samarbeid mellom berørte departementer og direktorater, både når reglene lages, og når de tolkes/gis råd om.

Flere av de nevnte forhold viser til et behov for bedre samarbeid mellom ulike myndigheter. Brukerne oppfatter det som om de ulike myndighetene er redde for å legge seg opp i andre myndigheters saker, men peker på at det er behov for bedre koordinering av krav og begrepsbruk, for å gjøre de mer forståelige og lettere å etterleve på det operative planet.

Bedre veiledning ved direkte henvendelse

Det pekes også på at man ikke alltid får hjelp når man henvender seg til myndigheter med tolkningsproblemer. Datatilsynet var et eksempel som ble nevnt i negativ retning, men også i høyst positiv retning! Her har brukerne åpenbart flere erfaringer, og det er ulike syn som gjør seg gjeldende. Dette kan muligens henge sammen med kompetansen til den som henvender seg til Datatilsynet, eller det kan henge sammen med kompetansen til den som svarer. Det kan også være at spørsmålene krever kompetanse på regelverk som ligger utenfor myndighetsområdet. Eller handle om manglende kompetanse på det praktiske og operative.

Statskonsult vil peke på at det ville være verdifullt for virksomhetene å kunne henvende seg til et sted med tverrfaglig kompetanse og få autoritative råd der.

Synliggjøre kompetansebehovet som er nødvendig

Informanter ønsker at det settes fokus på at det er nødvendig med kompetanse for å jobbe med informasjonssikkerhet i virksomhetene. Dette bør synliggjøres.

Datatilsynets Veiledning i informasjonssikkerhet for kommuner og fylker peker på behovet for kompetanseplanlegging i pkt 16 om personellsikkerhet. Manglende forståelse og prioritering fra ledelsens side kan være en av årsakene

til at kompetanse om juss, informasjonssikkerhet og informasjonssikkerhetsarbeid noen steder synes undervurdert.

4 Kort fra de enkelte intervjuer

Nedenfor følger Statskonsults gjengivelse fra intervjuene, men i kortform. Dette er uttrykk for opplysninger, synspunkter og meninger fra intervjuobjektene, og så godt vi har klart uten noen tillegg eller ”farvelegging” fra vår side. Det henvises til de enkelte intervjuene i *vedlegg 1* for mer detaljert og fullstendig informasjon. Der fremgår det også hvem som er blitt intervjuet.

4.1.1 Norsk Hydros Pensjonskasse

Kredittilsynets informasjonsmøte (for en samling av private pensjonskasser) om regelverket bidro til å skape større klarheter. Tilsynet ga ingen råd om hvordan IKT-regelverket kan tilpasses den enkelte virksomhet. IKT-regelverket synes utarbeidet for store virksomheter med komplekse data og legger opp til at det skal iverksettes store systemer. Mindre virksomheter må bruke mye ressurser på å finne ut om de løsningene som er best egnet hos dem, virkelig tilfredsstillende kravene i regelverket.

Det er mange regler som omhandler samme sak, og det kan være vanskelig for virksomhetene å finne ut hvilke regler som er mest relevante og eventuelt om hvordan reglene henger sammen. Det eneste informanten fikk vite var at hvis man tilfredsstillende kravene i personopplysningsloven, tilfredsstillende man kravene i IKT-forskriften.

Virksomheten har bare hatt kontakt med Kredittilsynet. Man savner et synlig samarbeid myndighetene imellom. Det gjelder både i forbindelse med tilsyn og gjennom den informasjonen som brukerne har behov for. Myndighetene burde også være i bedre dialog med brukerne når reglene skal innføres og når de skal gjennomføres.

Det er også et problem at de mange regelverkene man skal forholde seg til har ulik struktur og begrepsbruk. Ulik struktur gjør at det er vanskelig å finne ut av hvordan reglene henger sammen. Det samme gjelder bruken av ulike begreper, som i tillegg gjør at det oppstår tolkningsproblemer. Også overlappende regler skaper tolkningsproblemer (se vedlagte matrise).

Virksomheten har en informasjonsportal (plussportal) for sine medlemmer. Her ligger blant annet sensitive opplysninger om den enkelte. Tilgangen til portalen skjer gjennom brukernavn og passord. Regler om elektronisk signatur ble ikke fulgt, da man ikke så behov for dette.

Informanten er ukjent med Nasjonal strategi for informasjonssikkerhet.

4.1.2 Kommunal landspensjonskasse (KLP)

IKT-forskriften (forskrift om bruk av informasjonsteknologi) gir ikke anvisning på eksakte metoder for å utarbeide risikoanalyser. Det er liten hjelp å få fra myndighetene. Virksomheten har enda ikke utviklet slik metode, men arbeider med det nå, blant annet med hjelp fra eksterne konsulenter.

KLP bruker testdata for å utvikle og teste systemene. Det hentes ikke-anonymisert informasjon fra 40-40000 kunder. Personene som behandler dataene har vanlig taushetsplikt. I henhold til personopplysningsreglene gis

konsesjon for bruk av data i samsvar med virksomhetens formål. Det er fra juridisk hold blitt hevdet at KLP's bruk av testdata ikke har noe med selskapets formål å gjøre, og at deres konsesjon derfor ikke dekker denne datainnsamlingen. Datatilsynet har ikke kunnet gi svar, men har oppfordret KLP til å selv foreslå en løsning som tilsynet senere vil vurdere på et prinsipielt grunnlag. På bakgrunn av dette tolkningsproblemet som har oppstått for KLP, mener de at det er behov for å gjøre formålsbestemmelsene i personopplysningsreglene klarere.

KLP har måttet investere i nye maskiner for å tilfredsstille reglens krav til soneinndeling. De gamle maskinene hadde ikke mulighet for å oppnå to nivåer. Kravet om soneinndeling gjelder for alle typer virksomheter. KLP antar at en del mindre virksomheter ikke vil se seg råd til å skifte ut utstyr for å kunne skille data.

Implementering av regelverket har vært både tids- og ressurskrevende.

KLP har ikke selv opplevd at Kredittilsynet og Datatilsynet samarbeider, men har lest at det er et samarbeid i forbindelse med innføringen av IKT-forskriftene. KLP har ikke hatt besøk av Datatilsynet. De har heller ikke fått hjelp når de har henvendt seg til tilsynet med et konkret problem (bruk av testdata). De opplever at Datatilsynet og Kredittilsynet legger ulik vekt på informasjonssiden. For eksempel har Datatilsynet en informativ hjemmeside. Kredittilsynets hjemmeside er ikke så informativ.

4.1.3 Erfaringer fra tre kommuner

Tre kommuner er intervjuet: Gjøvik, Sør-Odal og Larvik. Alle de tre kommunene har arbeidet med etablering av et internkontrollsystem for informasjonssikkerhet slik personopplysningsloven krever, men er kommet ulikt langt i prosessen.

Gjøvik kommune har etablert et overordnet styringssystem for informasjonssikkerhet, Sør-Odal har etablert det overordnede styringssystemet og har implementert en del rutiner på operativt nivå og Larvik har implementert internkontroll for hele kommunen ned på operativt nivå, og er sertifisert av Det Norske Veritas etter standarden NS 7799 som gjelder styringssystem for informasjonssikkerhet.

Nærmere om Gjøvik kommunes erfaringer

Se også intervjuet.

Informasjonssikkerhetsarbeidet er først prioritert i inneværende år. Det arbeides med å sette seg inn i lover og regler og med å etablere en arbeidsmetodikk for informasjonssikkerhetsarbeidet.

I tillegg til at det oppleves som tidkrevende og vanskelig å sette seg inn i regelverket, oppleves det også som vanskelig å få oversikt over det. Ledelsen vet for lite, med blant annet for liten forståelse for at informasjonssikkerhet er mer enn IT-sikkerhet.

Foreløpig jobbes det på overordnet nivå. Det operative sikkerhetsarbeidet er delegert ut til de ulike kommunale virksomhetene, men det er usikkert hvordan dette arbeidet drives i dag.

Nærmere om Sør-Odal kommunes erfaringer

Se også intervjuet og vedlagt styringssystem².

Sør-Odal arbeider med et internkontrollsystem for kommunen. Foreløpig er systemet på overordnet nivå, dvs. har fokus på styringsmekanismene, ikke på de operative rutinene i utførende ledd. Ambisjonen er å lage et felles internkontrollsystem for kommunen etter modell av ISO 9000-serien. Har hele tiden jobbet ut fra personopplysningsforskriften.

Kommunen erfarer at de ulike regelverkene benytter begreper og beskrivelser på aktiviteter som er forskjellig fra regelverk til regelverk, mens de velkjente begrepene fra kvalitetssystem-standardene i ISO 9000-serien heller kunne ha vært brukt. Det er et sterkt ønske at de ulike regelverkene innrettes på en standardisert måte og med felles begrepsbruk. Det ville være en stor fordel om man la seg tett opp til ISO-9000.

Et av problemene er språket i regelverket. Det erfares som juridisk og ikke enkelt å forstå. Datatilsynets veiledning vedrørende informasjonssikkerhet oppleves heller ikke som lett å forstå. Selv ved konsultasjon med Datatilsynet og bruk av leverandør for å etablere ”systemoversikt”, ble ikke resultatet bra nok (for Datatilsynet) og det er vanskelig å forstå hva kravene egentlig er. Det er generelt vanskelig å forstå hvilke aktiviteter de ulike kravene bør munne ut i.

Et annet problem for kommunen er at de ulike regelverkene stiller opp krav som om kommunen skal etablere et eget system for hvert regelverk. Slik vil det ikke være i praksis. Det må være ett system i kommunen, slik at alle relevante krav hensyntas i så vel styringssystem som arbeidsgangen/rutinene/prosedyrene på operativt nivå.

På overordnet nivå bør det være et felles internkontrollsystem for kommunene, og deretter kan det implementeres lokalt. Det er ingen grunn til at alle skal begynne på bar bakke. Det bør legges føringer i form av standarder, for eksempel for taushetserklæringer. Det burde være unødvendig med flere sett med taushetserklæringer eller at taushetserklæringene skal se ulike ut fra kommune til kommune.

Det ville være nyttig med konkrete eksempler på operativt nivå.

Det er viktig at en kommune først etablerer det overordnede styringssystemet sentralt, før den enkelte virksomhet starter arbeidet med lokal implementering.

Det bør være en bevisstgjøring omkring behovet for kompetanse på informasjonssikkerhetsområdet. Sør-Odal har opparbeidet en viss kompetanse gjennom prosjektet, men den sitter spredt.

Proessen har pågått et år, og man regner med ytterligere to år før alle rutiner på operativt nivå er dekket inn.

Nærmere om Larvik kommunes erfaringer

Se også intervjuet og eksempler hentet fra internkontrollsystemet.

Larvik kommune har etablert et styringssystem for informasjonssikkerhet i tråd med kravene i standarder NS 7799 og er sertifisert av Det Norske Veritas i forhold til denne. (KB: Standarden stiller bl. a. krav om at virksomheten skal ha oversikt over alle lover og forskrifter som gjelder informasjonssikkerhet og som er aktuelle for virksomheten.)

² Det er Nord-Odals system som er vedlagt. Kommunene har samarbeidet om etablering av systemet.

Larvik har ikke hatt de samme negative erfaringene med regelverket som Sør-Odal rapporterer å ha. De mener selv dette kommer av at de på forhånd har innført et kvalitetssystem for kommunen i tråd med ISO 9000. De har også implementert miljøkravene (ISO 1401) ved å implementere dem i kvalitetssystemet. Dette har de også gjort når det gjelder kravene i NS 7799. Det er mao ikke etablert mange ulike systemer i kommunen, men et felles kvalitetssystem som hensyntar de ulike internkontrollkravene.

En erfaring som er verdt å merke seg, er at de ulike tilsynsmyndighetene har en tendens til å forvente at det skal være et eget system med fokus på "deres" krav. Slik kan det ikke være i kommunene. Det må være ett felles system som sørger for at de ulike kravene blir oppfylt i det ytterste operative ledd.

Kommunen har god erfaring med at det etablerte systemet virker. Det gjennomføres jevnlig sårbarhetsanalyser, og disse gjennomgås med tanke på felles tiltak for sentrale trussebilder.

Systemet er implementert i ytterste ledd på operativt nivå.

Det er vedlagt eksempler fra styringssystemet og fra operative prosedyrer.

Statskonsult vil påpeke at selv om Larvik har etablert et styringssystem og operative prosedyrer med stor dyktighet, er det fremdeles aktuelle lover som ikke er nevnt, for eksempel eforvaltningsforskriften. Vi regner med at mange kommuner avventer en felles løsning på esignatur.

4.1.4 Ullevål universitetssykehus

Ut fra opplysningstyper, systemer og andre forhold ved sykehuset er det en utfordring å ta tilstrekkelig hensyn til regler om informasjonssikkerhet. I mange sammenhenger er man fornøyd, i andre er en klar over at reglene ikke tas tilstrekkelig hensyn til, uten at det er lett å gjøre noe med det.

Ett eksempel er tilgang til opplysninger, som styres ut fra et opplegg/system med tre nivåer. Gruppe en har tilgang på alt – mens gruppe tre har svært begrenset tilgang. Tekniske tilgangsrettigheter blir dermed gjerne større enn det er juridisk adgang til. Dette reguleres bl.a. av taushetsplikter i helsepersonelloven, helseregisterloven samt personvernregler i personopplysningsloven, alle med innslag av supplerende regler om informasjonssikkerhet. I tillegg utfylles det med ansatte-avtaler mv. De mer finmaskede nevnte rettsreglene tas neppe nok hensyn til dagliglivets tilgang til f.eks. journaler. Tre-nivåsystemet blir for grovmasket. Bl.a. er det grunn til å tro at sniklesing av journalopplysninger mv forekommer i atskillig omfang; neppe brudd på taushetsplikt, men heller ikke rettmessig tilgang!

Det stilles spørsmålstegn ved om Helsennett-utviklingen har tatt tilstrekkelig hensyn til taushetsplikt og andre juridiske behandlingsregler for elektronisk informasjon; en kan ikke se at dette blir tilstrekkelig problematisert av direktoratet. Vanskelig å bygge bro mellom juridiske, tekniske og organisatoriske forhold. Ullevål universitetssykehus lager IK-system sentralt som sendes de lokale enhetene/avdelingene, men klarer ikke sentralt å sjekke om etterlevelsen lokalt er tilfredsstillende.

Jussen er laget i for stor grad av og for jurister. På den annen side settes store omstillinger i gang, med stor tro på juss som virkemiddel, - men foretakene overlates til selv å finne ut av hva som skal gjøres og hvordan. Strategisk kompetanse på juss burde vært koplet bedre til. Flere fagkompetanser

burde ha samarbeidet sterkere i forbindelse med de sentrale initiativene. En del av de sentrale initiativene kan vanskelig realiseres inne i et sykehusnett, og noen av initiativene spriker: Sikkerhetsnorm skal være i samsvar med personvernreglene, samtidig skal sikkerhetsportal brukes av borgerne på Internett, og i tillegg internt i sykehuset. Det siste antas å være i konflikt med personvernreglene, og er neppe løst ved overordnet bransjenorm.

Et annet opplevd problem er ulike tolkninger av reglene om informasjonssikkerhet. Dette kan være leverandører av IT-systemer (ulik tolkning av kravspesifikasjon), departementet (HOD) og direktoratet (Shdir) ikke alltid er samkjørte, de tolker ikke nødvendigvis likt. Det gir sprikende resultater, uklarhet og merarbeid.

Det er dyrt og ressurskrevende å etterleve regelverket og pålagte krav, som bl.a. setter tekniske og organisatoriske begrensninger/premisser. Kompetansekrevene å se slike sammenhenger, og å forfølge dem/ta konsekvensen av dem i praksis. Blir ikke nødvendigvis gjort godt nok; til dels kan det hoppes over bevisst eller ubevisst. Tolkning av reglene om sikkerhet, tilgang og taushetsplikt mv kan være vanskelig i seg selv, og vanskelig å praktisere likt – og det er lite praksis tilgjengelig. Her trengs bedre hjelp fra sentralt hold.

På den ene siden kan det oppleves som imponerende mye konsistens i lov- og forskriftsverket. På den annen side finnes det klare problemer i tolkningen og praktiske konsekvenser av ulike tolkninger av regler i helselovgivningen og personvernlovgivningen. Shdir har skrevet utredning om tilgang til pasientinformasjon i helseforetak og på tvers av helseforetak nå i 2005;³ jussen tolkes annerledes enn det mange helseforetak har gjort, og har implementert i praksis. Utredningen burde vært gjort i 2001, som premiss for utviklingsarbeid og systemarbeid, ikke i etterkant: dette er fordyrende og frustrerende.

God nok kvalitet i journal-løsningene er vanskelig å oppnå. Blanding av juss og praksis, tekniske løsninger mv. Det finnes en høyesterettsdom som ga foretaksstraff for uforsvarlig kvalitet i journalsystem. Dette er en aktuell problemstilling både i forhold til eksisterende systemer og i videreutviklingen av de elektroniske systemene.

Det oppleves som problematisk uklare forhold mellom Datatilsynet og Statens Helsetilsyn; neppe utviklet god, samordnet tilsynsmetodikk og tolkning av regelverk. Det framgår av intervjuet at eForvaltningsforskriften var ukjent.

4.1.5 Helse Vest IKT AS

Personopplysningsreglene og helseregisterreglene bruker ulike ansvarsbegreper. Dette er uheldig og egnet til å skape misforståelser. Begrepet

”behandlingsansvarlig” (pol) henspiller i helsefaglig sammenheng på den som har et medisinsk behandlingsansvar. Helseregisterloven bruker derfor begrepet ”databehandlingsansvarlig”.

Myndighetenes strenge fortolkning av helseregisterlovene og personopplysningsreglene skaper praktiske gjennomføringsproblemer. Konkret gjelder det spørsmål om utveksling av pasientjournaler mellom helseforetak, og hvem som skal være databehandlingsansvarlig i denne sammenheng. Ettersom

³ Ad tilgang til pasientinformasjon i helseforetak og på tvers av helseforetak, Sosial- og helsedirektoratet, mai 2005, svarbrev til Helse Vest, som stilte spørsmål våren 2004. Gjengitt i vedlegg 6.

både Datatilsynet og Sosial- og helsedirektoratet er av den oppfatning at det er de lokale helseforetakene - og ikke de regionale helseforetakene - som må være databehandlingsansvarlig, mener Helse Vest IKT at myndighetene legger opp til at det i praksis blir vanskelig å utveksle nødvendig informasjon mellom foretakene.

Det er vanskelig å følge opp regelverket på individnivå (130 ansatte og 25 000 brukere). Det har medført at ikke alle har fått tilstrekkelig opplæring. Opplæring er imidlertid en del av det etablerte styringssystemet og avdelingsleder har ansvaret for oppfølging.

Prosesen med å implementere reglene har vært meget tids- og ressurskrevende.

Informanten har hørt navnet Nasjonal strategi for informasjonssikkerhet, men kjenner ikke til hva denne inneholder. eForvaltningsforskriften var ukjent.

Vedlegg i separat dokument

Intervjuene, utdrag fra kvalitetssystemer, internkontrollsystemer mv, ligger i eget vedleggsdokument. Vedleggene 2, 3 og 4 (systemeksempler) samt vedlegg 5 og 6 er i form av frittstående filer som er tilgjengelig i elektronisk form. Det vises til det separate vedleggsdokumentet.