RAPPORT

Nr. 2006:4

Arbeid med informasjonssikkerhet; fra juss til styring og rutiner

Skrevet på oppdrag fra Fornyings- og administrasjonsdepartementet

Rapport

Statskonsult

Forord

Statskonsult videreførte i 2005 sitt flerårige arbeid med informasjonssikkerhet på oppdrag for Fornyings- og administrasjonsdepartementet. Denne rapporten drøfter to ulike tilnærminger til informasjonssikkerhetsarbeidet; "top-down" i form av styringssystem for informasjonssikkerhet og "bottom-up" i form av bruk av regelverket på operativt nivå i saksbehandlingsrutiner.

Arbeidet bygger på intervjuer, seminarer, gjennomgang av regelverket og konkrete forsøk. Intervjuer og rapport har vært distribuert bidragsyterne for kommentarer.

Statskonsult takker alle som har deltatt i arbeidet gjennom å la seg intervjue, delta på seminarer eller bidratt med dokumentasjon! En spesiell takk til Fredrikstad kommune som ga oss gode eksempler og god hjelp, og til Foreningen Kommunal Informasjonssikkerhet (KINS) som besørget invitasjoner til seminarer og som bidro til verdifulle kontakter til informanter.

Fra Statskonsult har seniorrådgiverne Amund Eriksen, Margaret Hagevik, Heidi Høiskar og Kirsti Berg (prosjektleder) deltatt. Fung. avdelingsdirektør Mari Vestre har vært prosjektansvarlig.

Oslo, mars 2006

Mari Vestre
fung. avdelingsdirektør

Innhold

1 Sammendrag

Bakgrunn
Prosjektet som beskrives i rapporten er gjennomført på oppdrag fra Fornyings- og administrasjonsdepartementet og har sin bakgrunn i Nasjonal strategi for informasjonssikkerhet.

Mål og arbeidsmåte
Arbeidet har vært konsentrert om alminnelig informasjonssikkerhet i offentlig og (til dels) privat virksomhet. Prosjektet har hatt to perspektiver på informasjonssikkerhet; styringsperspektivet og saksbehandlingsperspektivet. Målet har blant annet vært å fremskaffe eksempler på hvordan virksomheter arbeider med styring av informasjonssikkerheten, herunder med bruk av BS 7799 Britisk standard for styring av informasjonssikkerhet[1] og hvordan de arbeider med implementering av informasjonssikkerhet på operativt nivå i saksbehandlingsrutinene.

Arbeidet er gjennomført i form av intervjuer, nærmere studier av sentrale deler av regelverket for informasjonssikkerhet samt gjennomføring av et konkret forsøk med å kople regelverket direkte til arbeidstrinn i en saksbehandlings-prosess. Se nærmere i kapittel 2.

Funn og betraktninger
Prosjektets gjennomgang av regelverk for informasjonssikkerhet er nærmere beskrevet i kapittel 3. Prosjektet har forsøkt å skille ut bestemmelser knyttet til styring av informasjonssikkerhet og bestemmelser som kan etterleves på operativt nivå, for eksempel i saksbehandlingsrutiner. Dette er nærmere dokumentert i vedlegg 2. Det er et konglomerat av rettslige krav til informasjonssikkerhet. Noen lover og forskrifter handler spesielt om informasjonssikkerhet, men det er også en rekke lover og forskrifter som omhandler informasjonssikkerhet i forbindelse med andre temaer. Vårt formål har vært å illustrere hva man må forholde seg til både som leder og saks-behandler og etterleve i det daglige arbeidet. Prosjektet har gjennomgått taushetsbestemmelsene spesielt, og peker på at det er mange overlappende regler om taushetsplikt. Beskyttelsesinstruksen, som gjelder for offentlig sektor, er spesielt kompliserende.

Prosjektet har også gjennomgått regelverkets dokumentasjonskrav når det gjelder tiltak og peker på at regelverket kun gir bestemmelser om formåls-avgrenset dokumentasjon når det gjelder saksbehandlingsrutiner. Statskonsult peker på at man derved bare får fragmenterte fremstillinger av hvordan informasjonssikkerheten ivaretas i saksbehandlingsrutiner.

Videre, i kapittel 4, pekes det på at både personopplysningsforskriften og eForvaltningsforskriften delvis støtter seg på en internasjonal standard for administrasjon av informasjonssikkerhet, BS 7799/ NS 7799. Internasjonale

[1] Se kapittel 3 og vedlegg 2 for nærmere omtale og oversikt. Det er flere standarder og varianter av til dels samme standard, med et sentralt utgangspunkt i en britisk standard BS 7799. Vi angir ikke alltid disse ulike versjonene med helt korrekte navn og nummer i rapportteksten – det er ikke nødvendig i rapportens sammenheng. I bilag 2 har vi imidlertid for ordens skyld forsøkt å gjengi standardene med så riktige navn og nummer som mulig.

kvalitetssystemstandarder skiller tradisjonelt mellom styringsprosesser og virksomhetens prosesser på operativt nivå, og det forutsettes at både styrings-prosesser og prosessene på operativt nivå er dokumenterte. Statskonsult tror at noe av usikkerheten i offentlige virksomheter når det gjelder å implementere regelverket på operativt nivå, dels kommer av at regelverket ikke skiller tydelig på styring og saksbehandlingsprosesser, dels at det ikke er krav om at saksbehandlingsprosessene skal dokumenteres som grunnlag for arbeidet med informasjonssikkerhet på operativt nivå.

Kapittel 5 gir en oppsummering av intervjuene. Virksomhetene som ble intervjuet har først og fremst brukt ressurser på å innføre styringssystem for arbeidet med informasjonssikkerhet. Noen har benyttet NS 7799 eller andre tilsvarende internasjonale standarder og noen har bygget direkte på regelverket, særlig personopplysningsforskriften.

Rapporten gir et bidrag til arbeidet med informasjonssikkerhet ved å vise hvordan det går an å jobbe med informasjonssikkerhet som én av flere typer krav som skal ivaretas på operativt nivå, i virksomheters saksbehandlings-prosesser. Dette er beskrevet i kapittel 6.

Arbeidet ble gjort i samarbeid med Sosialtjenesten i Fredrikstad kommune. Her ble det foretatt en prosesskartlegging av saksbehandlingsrutinen for behandling av stønad til livsopphold, og deretter ble de relevante delene av regelverket forsøkt knyttet opp til de enkelte arbeidstrinnene. Eksemplet viser at en rekke krav i regelverket kan knyttes direkte til trinn i saksbehandlingen. Slike krav bør identifiseres og knyttes til prosessbeskrivelser for saksbehandling på sentrale områder. Slike fremstillinger er aktuelle for blant annet analyse- og opplæringsformål, og bør være et innarbeidet fellesgrunnlag for saksbehandlingen, lett tilgjengelig for konsultasjon ved tvil i den operative hverdagen.

Forslag

I kapittel 7 beskrives forslag til tiltak og videre prosess samt hvem Statskonsult mener er adressat for de ulike forslagene. Forslagene beskrives her i kortform:

1. Det foreslås at det utarbeides modeller og veiledninger for arbeidet med informasjonssikkerhet som skiller tydeligere på arbeidet med styring og arbeidet på operativt nivå.
2. Det foreslås at det etableres et praksisfellesskap for arbeid med informasjonssikkerhet i virksomheter, hvor virksomhetene selv kan bidra med erfaringer og hvor regelverksforvaltere kan bidra med tolkninger av regelverket. Praksisfellesskapet bør omfatte møter, seminarer samt et felles nettsted for diskusjon og dokumentasjon. Deltakelse i nettverksarbeid og bruk av eksempler og veiledningsstoff bør være gratis.
3. Det bør vurderes om det kan gis et generelt krav om dokumentasjon av saksbehandlingsprosesser i offentlig sektor. Personopplysningsforskriften og eForvaltningsforskriften bør bli mer tydelige på dokumentasjonskrav og mer eksplisitte når det gjelder kravene til dokumentasjon av styringssystem og kravene til dokumentasjon av saksbehandlingsprosessene.

4. Det bør utarbeides gode eksempelprosesser som innspill til vurdering ved videreutvikling av regelverket. Eksemplene må vise hvordan bestemmelser i sentrale regelverk gjelder for ulike trinn i saksbehandlingsprosessene. Eksemplene bør hentes fra sentrale saksbehandlingsområder i offentlig sektor.
5. Regelverket om behandling av fortrolig/taushetsbelagt informasjon bør forenkles.

2 Bakgrunn

2.1 Nasjonal strategi for informasjonssikkerhet

Arbeidet har sin bakgrunn i Nasjonal strategi for informasjonssikkerhet og er gjennomført på oppdrag for Moderniseringsdepartementet, nå Fornyings- og administrasjonsdepartementet, som en del av departementets oppfølging av eget ansvarsområde i forhold til Nasjonal strategi. Departementet har definert sitt ansvar til å omfatte tiltak både i statlig og kommunal sektor, da det er avgjørende viktig å etablere tillit til informasjonssikkerhet i hele offentlig sektor for å nå målene om eForvaltning.

Statskonsult har bidratt med planarbeid i forhold til departementets oppfølging av Nasjonal strategi og med gjennomføring av konkrete prosjekter. Prosjektene har dels hatt fokus på regelverket for informasjonssikkerhet, dels på forvaltning av regelverket og dels på etterlevelse av regelverket i virksomheter. I forbindelse med innhenting av informasjon om etterlevelse av regelverket, er det også innhentet informasjon fra noen få private virksomheter.

2.2 Tidligere arbeid for departementet i 2005

En kort gjennomgang av Statskonsults oppdrag i 2005 er tatt med i Vedlegg 1, for å vise sammenhengen i oppdragene. Det var et prosjekt i regi av koordineringsutvalget for informasjonssikkerhet (KIS) som gjennomgikk regelverket for informasjonssikkerhet[2] og forvaltningen av regelverket, samt et prosjekt for Moderniseringsdepartementet som viser eksempler på brukererfaringer med regelverket.

KIS-prosjektet viste til at det er behov for bedre empiri som grunnlag for videre utvikling av regelverket, og at det bør ses på hvordan regelverket samordnes. Det ble også pekt på en mulighet for at bruk av norsk standard for styring av informasjonssikkerhet NS 7799, kanskje kan gjøre etterlevelse av regelverket lettere. Virksomheter som har erfaring med ISO 9000-serien av standarder for kvalitetssystemer og /eller NS 7799, mener selv å ha god kontroll i informasjonssikkerhetsarbeidet. Mange virksomheter har arbeidet lenge med informasjonssikkerhet på et overordnet nivå/styringsnivå i virksomhetene, men arbeidet er ikke kommet like langt når det gjelder implementering på operativt nivå.

Brukererfaringer som ble innhentet viste blant annet eksempler på at virksomheter har problemer med å skaffe seg oversikt over regelverket, og at det oppleves at det er et stort gap mellom rettslige normer og den operative hverdagen i virksomhetene. Reglene sier noe om hva som skal gjøres, men det sies lite om hvordan.

[2] ”Regelverket for informasjonssikkerhet” brukes her som fellesbetegnelse på rettslige krav i lover, forskrifter og instrukser i offentlig og privat sektor som stiller krav om informasjonssikkerhet på en eller annen måte. Tilsvarende brukes betegnelsen ”lovverket”.

2.3 Mandatet og vår forståelse av oppdraget

Basert på de to arbeidene som er referert ovenfor, har Statskonsult på oppdrag fra Fornyings- og administrasjonsdepartementet høsten 2005 gjennomført videre intervjuundersøkelser og drøftinger med virksomheter.

Prosjektarbeidet som er hovedanliggendet for denne rapporten dreier seg hovedsakelig om to tilnærminger til informasjonssikkerhetsarbeidet:

- Arbeidet på overordnet nivå i virksomhetene
- Arbeidet på operativt nivå, dvs. saksbehandlingsnivå.

Mandatet er gitt i prosjektplanen for prosjektet:

"Målet med prosjektet er å fremskaffe eksempler på hvordan virksomheter har arbeidet for å etablere styringssystem for informasjonssikkerhet, herunder ved bruk av standarden NS 7799/BS 7799 Styringssystem for informasjonssikkerhet, samt eksempler på implementering av regelverket på operativt nivå i offentlige virksomheters daglige rutiner. Som et resultat av forsøkene, vil prosjektet gi en første skisse av hvordan man kan jobbe med standarden for styringssystem samt en vurdering av sammenhengen mellom styringssystem og den konkrete hensyntagen til regelverket på operativt nivå. Videre vil prosjektet vurdere om det bør utarbeides en veiledning for bruk av standarden for offentlig sektor, eventuelt en for stat og en for kommuner."

Ganske snart ble det klart, at av de vi fikk kontakt med, var det relativt få virksomheter som hadde benyttet BS 7799/NS 7799. Noen hadde benyttet ISO 9001 og noen hadde gått ut fra personopplysningsforskriften. Det ble derfor gjennomført intervjuer for å få frem erfaringer med ulike tilnærminger til styringssystem for informasjonssikkerhet.

Prosjektgruppen har videre sett på hvordan deler av regelverket kan identifiseres og brukes direkte ned på de operative saksbehandlingsrutinene. Det er gjennomført ett eksempel på dette, og eksemplet beskrives nærmere i denne rapporten.

Basert på de erfaringene som kom frem gjennom prosjektet, ble det også naturlig å vurdere deler av regelverket med tanke på hvordan det støtter arbeidet med informasjonssikkerhet på henholdsvis overordnet og operativt nivå.

2.4 Prosjektarbeidet

Prosjektarbeidet har konkret bestått av

- Intervjuer med kommuner, statlige virksomheter samt to private virksomheter vedrørende arbeidet med styring av informasjonssikkerhet
- Deltakelse på seminar i Nord-Odal og Sør-Odal kommuner, der deres arbeid med styringssystem for informasjonssikkerhet ble presentert
- Gjennomføring av forsøk med å anvende regelverket direkte på saksbehandlingsrutiner. Dette ble gjennomført i samarbeid med Fredrikstad kommune, Sosialtjenesten. Det ble etablert

arbeidsflytbeskrivelse og deler av regelverket for informasjonssikkerhet ble forsøkt anvendt direkte på de ulike stegene i saksbehandlingen

- Gjennomgang av regelverket med formål å anvende det i saksbehandlingsrutinene
- Gjennomgang av regelverket med tanke på hvordan det støtter arbeidet med informasjonssikkerhet på henholdsvis overordnet og operativt nivå
- Gjennomføring av to seminarer i Statskonsults regi. Delvis ble det gitt foredrag fra virksomheter i privat og offentlig sektor, og delvis ble prosjektresultater presentert og drøftet.

Statskonsult takker alle som har deltatt i arbeidet gjennom å la seg intervjue, delta på seminarer eller bidratt med dokumentasjon! En spesiell takk til Fredrikstad kommune som ga oss gode eksempler og god hjelp og Foreningen Kommunal Informasjonssikkerhet (KINS) som besørget invitasjoner til seminarene og som bidro med verdifulle kontakter til informanter i arbeidet.

Rapporten ble distribuert bidragsyterne for kommentarer 5. januar 2006. Den foreligger i endelig versjon medio mars 2006.

Fra Statskonsult har seniorrådgiverne Amund Eriksen, Margaret Hagevik, Heidi Høiskar og Kirsti Berg (prosjektleder) deltatt i det faglige arbeidet.

3 Hva i regelverket er rettet mot henholdsvis overordnet nivå og operativt nivå?

I dette prosjektet har vi gjennomgått noen av de antatt sentrale kravene i regelverk som angår informasjonssikkerhet. Hensikten var å finne ut hvilke krav som angår styringsprosesser og hvilke krav som må ivaretas i den operative saksbehandlingen.

Vi fant at de fleste og mest synlige bestemmelsene er de som angår de overordnede styringsprosessene. Det er imidlertid også en flora av bestemmelser som angår ulike faser i saksbehandlingen, og som er av en slik karakter at de i større eller mindre grad egner seg for implementering i de operative prosessene.

Vi fant videre at det er et antall rettslige krav fra ulike regelverk som er parallelle, de gjelder samme forhold. Hver for seg gir ikke de enkelte regelverk hjelp til å oppdage disse parallelle kravene.

3.1 Et mangfold av rettslige krav til informasjonssikkerhet

I denne rapporten har vi fokus på alminnelig informasjonssikkerhet i offentlig og (til dels) privat virksomhet.[3] Vi har også valgt å fokusere på de to regelverkene som oppdragsgiver Fornyings- og administrasjonsdepartementet har ansvar for.[4] Men disse to regelverkene kan ikke ses på isolert, derfor nevnes også andre, relevante regler i prosjektets konkrete sammenhenger.

Rettsregler som stiller krav om informasjonssikkerhet finnes i mange lover, forskrifter og instrukser. I tillegg kan det være krav i kontrakter. Kravene kan være klare og direkte, men også mindre presise, indirekte og nærmest usynlige. Generelt er det ingen regelverk eller kontrakter som i sin helhet *bare* handler om informasjonssikkerhet.[5] Kravene kommer i tilknytning til andre temaer, for å støtte funksjoner og handlinger der det er viktig å ha tillit til informasjonens konfidensialitet, integritet og tilgjengelighet (informasjonssikkerhet).

---

[3] I Nasjonal strategi for informasjonssikkerhet fra juni 2003 skilles det mellom tre områder for sikkerhetstenkning, av hensyn til henholdsvis 1) rikets sikkerhet og andre vitale nasjonale sikkerhetsinteresser, 2) kritiske samfunnsfunksjoner og 3) alminnelig informasjonssikkerhet i samfunnet for øvrig. Strategien har først og fremst som mål å redusere sårbarhet ved det som kalles alminnelig bruk av IT og i kritisk IT-infrastruktur, samt legge til rette for trygge elektroniske tjenester/ytelser fra offentlig og privat virksomhet. IT-sikkerhet og informasjonssikkerhet brukes nærmest synonymt.

[4] Forskrift om personopplysninger (personopplysningsforskriften) (av 15.12.00, nr 1265) og forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) (av 25.06.04, nr 988).

[5] Heller ikke Sikkerhetsloven med forskrifter gjør det, med unntak av den tilhørende forskriften om informasjonssikkerhet. Men sikkerhetsloven med forskrifter handler som kjent om rikets sikkerhet og andre vitale nasjonale sikkerhetsinteresser, hvor informasjonssikkerhet inngår som en viktig delstørrelse. Lovens område er ikke tema i denne rapporten.

Noen lover og forskrifter handler spesielt om informasjonssikkerhet, men det er også en rekke lover og forskrifter som omhandler informasjonssikkerhet i forbindelse med andre temaer.

Aktuelle rettslige krav til informasjonssikkerhet finner vi blant annet i forvaltningsloven – med forskrift om elektronisk kommunikasjon (eForvaltningsforskriften), offentlighetsloven, personopplysningsloven med forskrift og i beskyttelsesinstruksen. Dette er *generelle* regler knyttet til alle typer saksbehandling. Noen regler gjelder i hele den offentlige sektoren (stat, fylkeskommune, kommune), noen bare i statlig sektor. Andre regler gjelder (også) i privat sektor, eller bare i privat sektor (dog ingen av de nevnte er i siste kategori).

I tillegg kommer *spesielle* regler på enkeltområder, som for eksempel i helseregisterloven, helsepersonelloven, lov om sosiale tjenester, kredittilsynsloven med IKT-forskriften osv. Der det finnes særlovgivning med forskrifter, går disse foran de generelle lovene, eller de generelle gjelder som utfyllende til de spesielle. Av og til vises det fra særloven til regler i et generelt regelverk, og sies uttrykkelig at den eller de reglene også gjelder på dette området, i tillegg til særlovens regler.[6]

Ledere, saksbehandlere og andre medarbeidere må rette seg etter et ”lappeteppe” av regler og regelverk. Ledelsen har et spesielt ansvar for å sørge for at reglene er kjent og innarbeidet på en helhetlig og effektiv måte.

Siden det er mange regler om informasjonssikkerhet, har vi valgt å fokusere på noen få, for eksemplenes skyld. Når det nedenfor fremstilles en del detaljer på noen utvalgte områder, er hensikten ikke å gi (full) oversikt over reglene som sådan. Vårt formål er å illustrere mer konkret hva en må forholde seg til, både som leder og saksbehandler og etterleve i det daglige arbeidet. Regler gjengis for å illustrere at det er mye å ha kunnskap om, mye å huske på. Vi forsøker samtidig å se om regelverket gir anvisning på fremgangsmåter til å følge de rettslige normene og rutinene på en god måte.

3.1.1 Noen krav fra personopplysningsloven

Personopplysninger kan bare behandles elektronisk hvis de ansvarlige i virksomheten har gitt melding til Datatilsynet på forhånd.[7] Meldingen skal inneholde visse standardopplysninger, blant annet om hvilke sikkerhetstiltak som er knyttet til behandlingen.[8]

Personopplysninger kan bare behandles hvis den opplysningene gjelder (i loven kalt den registrerte) har *samtykket*, eller det *står i en (sær)lov* at slik behandling kan gjøres, eller av en av de *seks andre særlige grunnene* som er nevnt i loven.[9]

---

[6] Se for eksempel lov om sosiale tjenester (sosialtjenesteloven) (Lov 1991-12-13 nr 81), som i § 8-1 sier at ”Forvaltningsloven gjelder med de særregler som er fastsatt i loven her”. Flere andre eksempler kommer senere.

[7] Senest 30 dager før behandlingen starter, personopplysningsloven § 31

[8] Personopplysningsloven § 32, 1. ledd i)

[9] Personopplysningsloven § 8

Hvis det er aktuelt å behandle sensitive personopplysninger, må det søkes konsesjon/tillatelse fra Datatilsynet, med mindre behandlingen har hjemmel i egen lov.[10]

En virksomhet kan bare behandle personopplysninger hvis det fra ledelsens side sørges for det loven kaller "tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet…". Dette skal skje gjennom "planlagte og systematiske tiltak", som skal dokumenteres, og dokumentasjonen skal være tilgjengelig for medarbeidere, Datatilsynet og Personvernnemda. Med andre ord lovkrav om tiltak for å styrke tilliten til at saksbehandlingen skjer på trygg måte, og at tiltakene kan kontrolleres via dokumentasjonen.[11]

Slik dokumentasjon er ikke nødvendigvis tilstrekkelig "bevis" for at sikkerheten i praksis er god; det er avhengig av hvordan den konkrete etterlevelsen/implementeringen faktisk er i dagliglivet. Tidligere prosjekter på dette området har vist at det kan være relativt lang avstand fra de rettslige normene/kravene til styringssystemene i virksomhetene og etterlevelsen/ saksbehandlingen (med eller uten dokumenterte rutiner for de ulike typer saksbehandling). Tilsvarende erfaring kan man lese ut av Datatilsynets tilsynsrapporter.[12] Personopplysningsloven stiller også krav til at det etableres et system for internkontroll for hele loven.[13]

3.1.2 Noen krav fra personopplysningsforskriften

I *personopplysningsforskriftens kapittel 2* finner vi fyldigere krav til særlig ledelsens ivaretakelse av *informasjonssikkerhet*. Det vil føre for langt å ta med alle kravene her, men noen skal nevnes. Forskriften slår fast at det er den daglige ledelsen som har ansvaret for å påse at reglene etterleves. Dette innebærer krav om klar fordeling og dokumentasjon av ansvar og myndighet for bruk av det forskriften kaller informasjonssystemet.

Ledelsen må initielt sørge for at det formuleres sikkerhetsmål og sikkerhetsstrategi, der formålet med behandlingen av personopplysningene skal fremgå, og hvilke valg og prioriteringer som skal gjøres for å nå formålet. Det skal jevnlig undersøkes om bruken av informasjonssystem er god i forhold til virksomhetens behov, og om sikkerhetsstrategien gir god nok informasjonssikkerhet som resultat! Det er grunn til å sette utropstegn bak dette, fordi slike konkrete kartlegginger og vurderinger av egen praksis med jevne mellomrom understreker at arbeidet med informasjonssikkerhet er en prosess, som det må arbeides med på kontinuerlig basis, med etterkontroll av om

---

[10] Personopplysningsloven § 33. Hva som er sensitive personopplysninger er definert presist i § 2 nr 8), a-e, som omfatter bl.a. opplysninger om helseforhold.

[11] Datatilsynet har flere veiledninger om bl.a. hvordan sikkerhetsbestemmelsene skal tolkes, om hvordan risikovurderinger skal gjøres, om tynne klienter, og veiledning for kommuner og fylker, alle ajourført pr 2005 http://www.datatilsynet.no/templates/Temaforside____105.aspx

[12] Se nærmere her: http://www.datatilsynet.no/templates/article____206.aspx

[13] Personopplysningsloven § 14, som utfylles av personopplysningsforskriftens kapittel 3 Internkontroll

tiltakene virker. Forskriften krever at resultatet av gjennomgangen skal dokumenteres og brukes til forbedringer.

Kriterier for akseptabel risiko skal bestemmes, risikovurderinger skal gjennomføres, som grunnlag for revurdering av om kriteriene er hensiktsmessige. Resultatene skal dokumenteres. Det skal også jevnlig gjennomføres sikkerhetsrevisjon, med krav om dokumentasjon av resultatet.

Ved sikkerhetsbrudd/avvik skal disse fanges opp og gi grunnlag for forbedring, og resultatet skal dokumenteres. Til slutt er det grunn til å merke seg at forskriftens kapittel 2 har egne paragrafer/regler for sikring av henholdsvis konfidensialitet, tilgjengelighet og integritet, altså kjernebegrepene for informasjonssikkerhet.

Når det utveksles informasjon med andre virksomheter, skal ledelsen etablere klare ansvars- og myndighetsforhold overfor kommunikasjonspartnere og leverandører. Dette skal nedfelles i egne avtaler. Det kreves også at slike andre virksomheter skal ha tilfredsstillende sikkerhet i henhold til forskriften, at ledelsen kjenner de andres strategi for informasjonssikkerhet, og at ledelsen jevnlig forsikrer seg om at strategien til de andre virksomhetene faktisk gir tilfredsstillende resultat!

3.1.3 Noen krav fra eForvaltningsforskriften

Også i *eForvaltningsforskriften* stilles det krav til informasjonssikkerhet, for å støtte eller bidra til at forskriftens formål nås. Som i personopplysningsforskriftens kapittel 2 er sikkerhetsmål og sikkerhetsstrategi valgt som sentrale krav, med bruk av de samme begrepene. Forvaltningsorgan som benytter elektronisk kommunikasjon *skal* ha beskrevet det som kalles sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i virksomheten (eForvaltningsforskriften § 13 nr 1).

Virksomhetens mål for informasjonssikkerhet ved bruk av elektronisk kommunikasjon skal være formulert i *sikkerhetsmål*, og de nærmere valg og prioriteringer for å nå målene skal være beskrevet i en *sikkerhetsstrategi*. Her er det en sammenheng til formålsparagrafen (§ 1), som sier at det skal legges til rette for sikker og effektiv bruk av elektronisk kommunikasjon. Sikkerhetsmål og -strategi skal bidra til dette, på en samordnet og enkel måte, – både for de som skal kommunisere med forvaltningen (borgere og næringsliv), og for forvaltningen selv.

Forskriftens krav innebærer at det er en *plikt* å lage sikkerhetsmål og sikkerhetsstrategi, og dokumentere det. Dette må være gjort *før* man setter i gang med elektronisk kommunikasjon. I praksis betyr dette at ledelsen/virksomheten ikke kan utvikle og ta i bruk et nytt IKT-system, uten at mål og strategi for informasjonssikkerheten er utarbeidet, og danner et viktig grunnlag for utvikling og bruk av systemet. I forhold til etablerte systemer betyr dette et krav om så fort som mulig å lage sikkerhetsmål og -strategi, - hvis virksomheten ikke skulle ha det. Dette kan føre til oppdagelse av endringsbehov – som alltid er mer kostbart å dekke i etterkant.

Sikkerhetsstrategien skal ikke bare danne grunnlag for valg av det som kalles sikkerhetstjenester og det nærmere nivået på sikkerheten, men også danne

grunnlag for *eventuelt å velge bort* sikkerhetstiltak der de ut fra nærmere vurderinger ikke anses nødvendige. Ofte tas elektroniske løsninger i bruk uten nærmere sikkerhetstenkning; for eksempel e-post. Dette er det et mål å komme bort fra. Forskriften krever at dette i så fall skal være en bevisst og gjennomtenkt handling, med basis i sikkerhetsstrategien.

eForvaltningsforskriften understreker videre at sikkerhetsstrategien skal danne grunnlaget for forvaltningsorganets beslutninger om innføring og bruk av sikkerhetstjenester og -produkter, og at dette skal skje *på en helhetlig, planlagt, systematisk og dokumentert måte.* Dette kravet gir også assosiasjoner til tilsvarende regler for personvernet, se personopplysningslovens (POL) § 13, som krever planlagte og systematiske tiltak for informasjonssikkerhet for personopplysninger, med dokumentasjon. Se også POL § 14 om internkontroll med tilsvarende krav.

Til slutt i eForvaltningsforskriften § 13 (1) slås det fast at sikkerhetsstrategien skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.

Krav til informasjonssikkerhet forekommer som nevnt tidligere i flere lover, forskrifter og instrukser. Denne regelen peker på nødvendigheten av å se slike krav i sammenheng, og gjennomføre tenkning og tiltak for informasjonssikkerhet på en helhetlig måte i den enkelte virksomhet. Kravene i andre regelverk gjelder selvfølgelig uansett, men dette er en slags påminnelse i forskrifts form om å legge opp til en helhetlig etterlevelse. Det er en betimelig påminnelse, som gir betydelige utfordringer å gjennomføre i praksis.[14]

I eForvaltningsforskriften § 13 (2) kommer følgende interessante regel for dette prosjektet (og selvfølgelig generelt): *Sikkerhetsstrategien skal være utarbeidet i henhold til anerkjente prinsipper for informasjonssystemers sikkerhet*.

I forskriften har en bevisst latt være å peke på et bestemt prinsipp eller standard på dette området; de finnes det flere av, og de kan leve uavhengige liv i forhold til forskriften. Anerkjente prinsipper er for eksempel nedfelt i standarder, hvorav den aktuelle her er NS 7799, se kapittel 4.

Sikkerhetsmål og -strategi anses som viktige virkemidler for at det enkelte forvaltningsorgan skal klare å gjennomføre arbeidet med informasjonssikkerhet på en trygg og effektiv måte, som grunnlag for at borgere og næringsliv kan ha tillit til forvaltningen.

Sikkerhetstenkningen skal være en integrert del av virksomhetens øvrige planarbeid (virksomhetsstrategi, inkludert strategi for IKT og informasjonssikkerhet), slik at styring av videre valg og bruk skjer ut fra en helhetlig tenkning.

[14] For noen av regelverkene er kravene til informasjonssikkerhet mer eller mindre harmonisert, men ikke i alle. Se for eksempel krav til sikkerhet også i helseregisterloven (av 18. mai 2001, nr 24), §§ 16 og 17, lov om Schengen informasjonssystem (SIS-loven av 16. juli 1999, nr 66) § 3, samt tilhørende SIS-forskrift kapittel 7, som i stor grad gir politiet tilsvarende regler som i personopplysningsforskriftens kapittel 2. Et annet og kanskje mer praktisk eksempel kan være beskyttelsesinstruksen i statlig sektor som forvaltes av Statsministerens kontor, se nærmere omtale nedenfor.

3.2 Mange overlappende regler om taushetsplikt

Hvis de opplysningene som skal behandles tilsier at det er nødvendig med *konfidensialitet* (skjerming mot uvedkommendes innsyn/tilgang), er det flere sett med regler som er aktuelle i hele offentlig sektor:

- reglene i forvaltningsloven om taushetsplikt for opplysninger om noens personlige forhold eller om konkurranseutsatte opplysninger (§ 13 flg)
- reglene i særlovgivningen som er grunnlag for saksbehandlingen på det enkelte område, for eksempel sosialtjenesten (sosialtjenesteloven § 8-8 om taushetsplikt)
- reglene i personopplysningsloven om at medarbeidere skal pålegges taushetsplikt for personopplysninger hvor konfidensialitet er nødvendig (§ 2-9 om taushetsplikt)
- reglene i eForvaltningsforskriften om behandling av taushetsbelagt informasjon og opplysningsplikt (§ 5 (1) – (3).

I tillegg, men bare på statlig sektor:

- reglene i beskyttelsesinstruksen, som er alene om å gi konkrete regler for behandling av taushetsbelagt informasjon, og som ved elektronisk behandling kobler til tunge, upraktiske regler fra området for rikets sikkerhet, på det sivile området.

Det er flere regler på dette konfidensialitetsområdet, men det vil føre for langt å ta de med her. Det som er nevnt skulle være nok til å illustrere at både ledere på generelt, administrativt nivå og saksbehandlere og arkiv på saksbehandlingsnivået har utfordringer med hensyn til hvordan reglene om taushetsplikt best kan følges i den praktiske hverdagen. Det er mange vurderinger som må tas, på ulike stadier i forhold til saksbehandling; det må tilrettelegges og organiseres fra ledelsens side, og det må være gjennomførbart i forhold til den enkelte saksbehandlingsrutine for medarbeiderne som skal gjennomføre saksbehandlingen. Dette må være på plass både for de generelle regelverkene (som gir ”støtteregler” til den ”alminnelige saksbehandlingen”) og de spesielle regelverkene (som gir hovedreglene for saksbehandlingen på det enkelte livsområde/forvaltningsområde).

Nedenfor gis det noe mer utfyllende opplysninger om de enkelte reglene nevnt i strekpunktene over.

3.2.1 Forvaltningsloven § 13

*Forvaltningsloven § 13 (taushetsplikt), 1. ledd***,** forutsetter tiltak for å ivareta konfidensialitet. Utgangspunktet i regelen om taushetsplikt er formulert slik**:** ”Enhver som utfører tjeneste eller arbeid for et forvaltningsorgan, plikter å hindre at andre får adgang eller kjennskap til det han i forbindelse med tjenesten eller arbeidet får vite om:

1) noens personlige forhold, eller

2) tekniske innretninger og fremgangsmåter samt drifts- eller forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde av hensyn til den som opplysningen angår."

Dette er som sagt bare utgangspunktet. Plikten er både passivt å tie, samt aktivt å hindre at "andre" får tilgang til opplysningene. Plikten gjelder "enhver", altså både ledelse, saksbehandlere, arkiv og for eksempel innleide konsulenter. Hvem er "andre", som ikke skal få tilgang til opplysningene? Det en ofte kaller "uvedkommende"? Hvordan kan en skille mellom vedkommende og uvedkommende? Og hva *er* informasjon eller opplysninger om "personlige forhold"?

Begge disse spørsmålene gir loven svar på gjennom en rekke unntak eller nyanserende regler, både med hensyn til hvilke opplysninger som omfattes av taushetsplikten, og hvem som likevel kan se opplysningene, uten hinder av taushetsplikten.

Fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted er ikke omfattet, med mindre det er fare for å røpe et klientforhold eller andre forhold "som må anses som personlige".[15] Hvis den som har krav på taushet samtykker, kan opplysningene likevel gjøres kjent for dem de direkte gjelder eller andre. Det samme gjelder hvis man ikke kan knytte et enkeltindivid til dem, eller opplysningene er alminnelig kjent eller tilgjengelig andre steder.[16]

Videre slår loven fast at en rekke personer/aktører/roller *likevel* kan få tilgang til opplysningene. Dette gjelder for det første (og kanskje naturligvis) parter i saken og deres representanter.[17] Det gjelder videre hvis opplysningene brukes for å oppnå slike formål som opplysningene er gitt eller innhentet for, for eksempel i forbindelse med saksforberedelse, avgjørelse, gjennomføring av avgjørelsen, oppfølging og kontroll.[18] Taushetsplikten er heller ikke til hinder for at opplysningene er tilgjengelig for andre tjenestemenn innen organet eller etaten, forutsatt at dette er nødvendig for "en hensiktsmessig arbeids- og arkivordning, blant annet til bruk ved veiledning i andre saker".[19] Et forvaltningsorgan kan også gi andre forvaltningsorganer opplysninger om en persons forbindelser med organet og om avgjørelser som er truffet og ellers slike opplysninger som det er nødvendig å gi for å fremme avgiverorganets oppgaver etter lov, instruks eller oppnevningsgrunnlag.[20]

[15] Forvaltningsloven § 13, 2. ledd

[16] Forvaltningslovens § 13a, nr 1 - 3

[17] Forvaltningsloven § 13b, 1. ledd nr 1

[18] Forvaltningsloven § 13b, 1. ledd nr 2

[19] Forvaltningsloven § 13b, 1. ledd nr 3

[20] Forvaltningsloven § 13b, 1. ledd nr 5

3.2.2 Sosialtjenesteloven § 8-8

Et av de mange regelverkene kommunene må håndtere i tillegg er *Lov om sosiale tjenester m.v. (sosialtjenesteloven)*. Lovens formål er blant annet å fremme økonomisk og sosial trygghet, bedre levevilkårene for vanskeligstilte og forebygge sosiale problemer. I denne typen saker krever særregelverket naturlig nok at konfidensialiteten skal ivaretas, av hensyn til den enkelte og tillitsforholdet til sosialtjenesten. For å ivareta dette har sosialtjenesteloven i § 8-8 flere krav om taushetsplikt. Der heter det at enhver som utfører tjeneste eller arbeid for sosialtjenesten eller en institusjon etter denne loven, har taushetsplikt etter forvaltningsloven §§13 til 13e. Det legges til at overtredelse straffes etter straffeloven § 121. Begge disse reglene/regelsettene ville gjelde uansett om de ble nevnt eller ikke. Men det kan være nyttig av pedagogiske grunner å peke på dem i særloven.

Videre i paragrafen gis det noen regler som er vinklet litt annerledes enn forvaltningslovens tilsvarende, men som bygger på de samme temaene. Det sies for eksempel at taushetsplikten også omfatter fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted.[21] I forvaltningsloven var disse opplysningstypene som nevnt uttrykkelig unntatt, med mindre de røper klientforhold mv. Her skal de i utgangspunktet omfattes av taushetsplikten. En klients oppholdssted kan imidlertid gis når det er "klart at det ikke vil skade tilliten til sosialtjenesten eller institusjonen å gi slik opplysning".[22] Utfordringen for de 435 kommunene blir å ha rutiner som ivaretar disse særreglene, samt de supplerende generelle reglene.

3.2.3 eForvaltningsforskriften § 5 (1)-(3)

Regler i *eForvaltningsforskriften* sier at når et forvaltningsorgan legger til rette for elektronisk kommunikasjon av potensielt taushetsbelagt informasjon, eller informasjon som kan være underlagt sikringskrav fra annet regelverk (typisk personopplysningsreglene), da skal risiko for uberettiget innsyn være forebygget på tilfredstillende måte. I tillegg får forvaltningsorganet plikt til å informere brukerne godt om risiko ved eventuell overføring av slike opplysninger, samt generell opplysningsplikt om hvordan taushetsbelagte opplysninger og personopplysninger faktisk sikres under behandling i forvaltningsorganet (§ 5 (1) – (3). Hvordan risiko for uberettiget innsyn skal forebygges rent konkret, sier forskriften lite om.

3.2.4 Beskyttelsesinstruksen § 12

Det gjør derimot *beskyttelsesinstruksen*[23] *i statlig sektor*, som forvaltes av Statsministerens kontor. Den stiller krav til fortrolig behandling av

[21] Sosialtjenesteloven § 8-8, 2. ledd, første setning

[22] Sosialtjenesteloven § 8-8, 2. ledd, siste setning

[23] Den er tilgjengelig her: http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-19720317-3352.html

opplysninger som må beskyttes mot uvedkommendes innsyn eller tilgang (konfidensialitet). Plikten gjelder hvis det *"vil kunne skade*" eller *"vil kunne forårsake betydelig skade"*. *"for offentlige interesser, en bedrift, institusjon eller enkeltperson at dokumentets innhold blir kjent for uvedkommende*." Hvis svaret på dette er ja, må dokumentet merkes med graderingen FORTROLIG eller STRENGT FORTROLIG, og de nærmere behandlingsreglene følges. Denne plikten gjelder all "sivil" taushetsplikt i staten. Hvis det er aktuelt med *elektronisk behandling* av slik taushetsbelagt informasjon, må også en rekke regler av hensyn til rikets sikkerhet følges på dette høyst sivile området i hele staten – sentralt, regionalt og lokalt.[24]

De aktuelle reglene står i sikkerhetslovens forskrift om informasjonssikkerhet.[25] Disse rettsreglene er vanskelige å forstå og etterleve, antakelig også innenfor området rikets sikkerhet. Hvordan blir det da etterlevd på sivil sektor? Siden beskyttelsesinstruksen er en statlig instruks, gjelder den "bare" i statlig sektor, men selvfølgelig ikke i fylkeskommunal eller kommunal sektor.

Følgelig foreligger det til dels helt forskjellige behandlingsregler for taushetsbelagt informasjon i henholdsvis statlig og kommunal sektor, selv om begge områder er underlagt samme generelle taushetsregler i forvaltningsloven (samt reglene nevnt over i dette kapitlet). Reglene i statlig sektor blir svært omfattende, uoversiktlige, ressurskrevende og kompliserte på denne måten, og vi har i prosjektet ikke møtt noen som er klar over og følger reglene, slik som beskrevet.

3.3 Dokumentasjonskrav

Den store utfordringen som regelgiverne overlater til det praktiske liv å finne ut av, er hvordan en ut fra rettsreglene kan lage og ta i bruk styringssystemer, i henhold til anerkjente prinsipper/standarder, og å få til rutinebeskrivelser som på en god nok måte forbinder kravene i rettsreglene med både overordnet styring og praktisk saksbehandling.

Det finnes mange krav om at det skal legges til rette for at sikkerhetstiltak dokumenteres, blant annet i form av prosedyrer eller rutiner. Vi har ikke sett tilsvarende krav for de generiske saksbehandlingsrutinene som informasjons-sikkerheten skal tilpasse seg og fungere sammen med. Dermed har man i beste fall bare en del av kartet, eller ulike biter av løsrevne kartdeler, uten at regelverkene bidrar til å se eller ivareta helheten. Nedenfor viser vi krav om dokumentasjon knyttet til informasjonssikkerhet i noen av de sentrale regelverkene.

---

[24] Se beskyttelsesinstruksens § 12, der det heter: *"Dokumenter gradert etter denne instruksen skal så langt det passer, behandles elektronisk i samsvar med følgende regler i sikkerhetslovens forskrift om informasjonssikkerhet: § 4-36 i kapittel 4 om dokumentsikkerhet, kapittel 5 om informasjonssystemsikkerhet, § 6-9 fjerde ledd første punktum jf. § 6-6 i kapittel 6 om fysisk sikring mot ulovlig inntrenging og kapittel 7 om administrativ kryptosikkerhet. Dokumenter gradert etter instruksen skal i slike tilfeller følge reglene for dokumenter gradert BEGRENSET."*

[25] Se nevnte forskrift om informasjonssikkerhet her: http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20010701-0744.html

3.3.1 Generelle regler om saksbehandling i forvaltningen

Forvaltningsloven har generelle bestemmelser om forvaltningens saksbehandling, blant annet om utredningsplikt, dokumentasjon av innhentede opplysninger (nedtegning av opplysninger). *Offentlighetsloven* regulerer den delen av saksbehandlingen som gjelder innsyn i dokumenter. Hovedregelen er at saksdokumenter skal være offentlige.

Ingen av disse lovene stiller krav om at de ulike trinn i saksbehandlingen skal følge en forhåndsbestemt saksgang og at det skal dokumenteres at denne følges.

Etter *eForvaltningsforskriften § 13* (1) skal en sikkerhetsstrategi danne grunnlaget for forvaltningsorganets beslutninger om innføring og bruk av det som kalles sikkerhetstjenester og -produkter. Dette skal skje *"på en helhetlig, planlagt, systematisk og dokumentert måte"*. Videre sier forskriften at *"sikkerhetsstrategien skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks*". Dette må den enkelte virksomhet ta ansvar for og finne ut av selv. Forskriftskravet er en påminnelse om behovet for å se de ulike rettslige kravene i sammenheng, og at dette må skje på en systematisk og dokumentert måte. Dette er et omfattende krav både til den generelle, overordnede styringen, og til den operative gjennomføringen/saksbehandlingen.

I forskriftens § 13 (2) slås det fast at sikkerhetsstrategien skal være utarbeidet *"i henhold til anerkjente prinsipper for informasjonssystemers sikkerhet"*. Dette er den nærmeste hjelpen man får i forskriften, til å få bedre styring på systemene sine, og etterlevelse av rettsreglene.

3.3.2 Personopplysningsloven og personopplysningsforskriften

Personopplysningslovens § 13 Informasjonssikkerhet lyder*:*

"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 Personvernnemnda."

Begrepet "planlagte og systematiske tiltak" har sin opprinnelse i kvalitetssikring og benyttes i ISO 9000-serien for kvalitetssystemer. Vi kommer tilbake til dokumentasjonskrav i kvalitetssystemer i kapittel 4.

Slik kravene er fremstilt i Personopplysningsloven, kan det være vanskelig å knytte dokumentasjonskravet til selve saksbehandlingsrutinene. Det kan se ut som om sikkerhetstiltakene skal gjelde det elektroniske informasjonssystemet, selv om dette ikke står uttrykkelig. Det fremkommer ikke et utrykkelig krav om dokumenterte saksbehandlingsrutiner, selv om dette kunne vært underforstått.

Personopplysningslovens § 14 Internkontroll har tilsvarende krav som § 13, men også her er et eventuelt krav om dokumentasjon av saksgangen underforstått og lite eksplisitt.

Personopplysningslovens § 15 Databehandlerens råderett over personopplysninger er noe mer eksplisitt: ”En databehandler kan ikke behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige.”

Her forutsettes det at det er avtalt/dokumentert hvordan personopplysninger behandles. Det kan likevel hende at dokumentasjonskravet ikke kan sies å gjelde alle saksbehandlingstrinn, men kun de saksbehandlingstrinn som håndterer personopplysninger.

Personopplysningslovens § 18 Rett til innsyn, inneholder også bestemmelser om dokumentasjon av behandling og sikkerhetstiltak, uten at det eksplisitt nevnes at saksgangen skal være dokumentert. Som bruker vil man antakelig føle seg bedre informert dersom dokumentasjon av alle trinn i saksgangen forelå, og at sikkerhetstiltakene knyttet til de trinn som påvirker informasjonssikkerheten var dokumentert. **Leses regelverket slik at kun de operasjoner som direkte angår personinformasjon skal dokumenteres, vil brukerne eller tilsynsmyndigheter ikke kunne ha full oversikt eller på egen hånd vurdere om også andre trinn i saksbehandlingen kan påvirke informasjonssikkerheten.**

Personopplysningslovens § 22 omhandler retten til redegjørelse om regelinnholdet i datamaskinprogrammer som foretar automatiserte enkeltvedtak. Det vil være særdeles vanskelig å sikre tillit til programmer hvis ikke alle behandlingssekvensene fremgår av en slik dokumentasjon. Det samme kan sies om saksbehandlingsrutiner som bare er delvis automatiserte eller helt manuelle.

Til sammen inneholder personopplysningsloven så mange krav til ulike faser i en saksbehandling og krav til dokumentasjon av disse, at det kan synes underforstått at saksgangen i seg selv skal være dokumentert, men det er liten eksplisitt støtte for dokumentasjon av saksgangen.

Personopplysningsforskriftens kapittel 2 Informasjonssikkerhet og kapittel 3 Internkontroll inneholder en rekke konkrete krav om tiltak for sikring av personopplysninger og om at rutinene for dette skal være dokumentert. I tillegg kreves det at ”*Databehandlere som behandler personopplysninger på oppdrag fra behandlingsansvarlige, skal behandle opplysningene i samsvar med rutiner behandlingsansvarlige har oppstilt*”. Dette medfører at i hvert fall alle behandlingsledd i saksbehandlingskjeden som omfatter håndtering av personopplysninger, skal være dokumentert.

3.3.3 Datatilsynets veiledninger

Datatilsynet har utgitt en rekke veiledninger om informasjonssikkerhet; Veiledning i informasjonssikkerhet for kommuner og fylker, Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer og Risikovurdering av informasjonssystem med utgangspunkt i forskrift til personopplysningsloven.

Veiledning i informasjonssikkerhet for kommuner og fylker har noen kommentarer om dokumentasjon:

Kapittel 12 Administrative og tekniske rutiner:

”Informasjonssystemet skal benyttes i samsvar med fastlagte rutiner. I den grad det er nødvendig for å oppnå tilfredsstillende informasjonssikkerhet, skal rutiner utarbeides for bruk, drift og vedlikehold av det enkelte utstyr eller program.”

Del VI Dokumentasjon gir utfyllende regler om styrende dokumenter og Prosedyrer, og nevner spesielt rutiner for risikoanalyse, egenkontroll, ledelsens gjennomgang, konfigurasjonsendring, beredskapsplaner, avviksbehandling, adgangskontroll, tilgangskontroll, dataoverføring og dokumentsikkerhet. Dette er forhold som dels inngår i ledelsens overordnede ansvar og dels angår drift.

Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer viser til § 2-16 i personopplysningsforskriften, og sier ”Dokumentasjonskravet omfatter i tillegg til beskrivelse av tekniske sikkerhetstiltak, også rutiner for arbeid med informasjonssystemet og registrering av hendelser.” Hendelser er her avvik fra fastlagte prosedyrer og mulige trusler mot informasjonssikkerheten.

Risikovurdering av informasjonssystem med utgangspunkt i forskrift til personopplysningsloven ser informasjonen som en *verdi*, et aktivum for virksomheten og som må vernes på forsvarlig måte. Se særlig *kapittel 4* Kartlegging. Veiledningen bruker begrepet *miljø* om de omgivelsene som verdiene befinner seg i. ”Miljøet omfatter blant annet informasjonssystem, (fysisk) installasjon og organisasjon. Også de prosesser og driftstilstander verdiene inngår i er en del av mijløbeskrivelsen.”

”Forskjellige verktøy og metoder kan tas i bruk for kartlegging av verdier og miljø – også metodikk som ikke direkte er utarbeidet for kartlegging ved risikovurderinger. Resultater fra *prosesskartlegging* forteller om hvor og hvordan verdier bearbeides, og il samtidig gi informasjon om muligheter for tap eller skade.”

Dette siste utdraget er fra kapittel 4.2 Verktøy, og er det eneste stedet vi har funnet som beskriver dokumentasjon av arbeidsprosessene/ saksbehandlingsprosessene som en metode i sikkerhetsarbeidet. Men i kapittel 4.3 Kartlegging av personopplysninger, sies det ”Ved bruk av prosesskartlegging i dette arbeidet er det naturlig å identifisere den formålsavgrensede behandlingen i ”prosessen” – i stedet for å ta utgangspunkt i typiske forretningsprosesser.”

Prosjektgruppen mener likevel at en prosesskartlegging som gir fyldestgjørende oversikt over saksbehandlingsprosessene, i mange tilfeller vil kunne gi et godt grunnlag, både for å sikre at formålet med saksbehandlingen blir ivaretatt, og et grunnlag for å sikre at alle regler som gjelder behandlingen blir identifisert og hensyntatt.

Ikke all offentlig behandling er saksbehandling eller en forhåndsdefinert sammenhengende prosess. Omsorgstjenester i institusjon, vil for eksempel være styrt av blant annet akutte situasjoner som oppstår, og det kan være sterke krav til dokumentasjon av situasjonsbetingede handlinger, og krav til bestemte

handlingsmønstre, uten at disse handlingene inngår i en forhåndsdefinert sammenhengende prosess.

Når det gjelder saksbehandling som først og fremst bygger på informasjon, vil sammenhengende prosessbeskrivelser være av stor verdi. Vårt eksempel fra Fredrikstad kommune går nærmere inn på dette.

4 Litt om standarder for kvalitetssystemer i relasjon til informasjonssikkerhet

Grunnen til at vi tar med noe om kvalitetssystemer her, er at kapittel 2 i personopplysningsforskriften bygger på en versjon av BS 7799, om styring av informasjonssikkerhet i organisasjoner. Denne er en av flere standarder som har sterkt slektskap med ISO 9000-serien av standarder for kvalitetssystemer, hvorav ISO 9001 er den mest omfattende. ISO 9001 er lagt til grunn for standarder for mange ulike områder. **Mens regelverket har hovedfokus på styring og dokumentasjon av styringsprosesser, forutsetter kvalitetssystemene at også de viktigste kjerneprosessene (i offentlig sektor saksbehandlingsprosessene) er dokumenterte.**

Etter hvert vokste det frem et stort marked for kvalitetsrådgivning, og flere ulike skoler eller konsepter for kvalitetsutvikling. Disse skal vi ikke gå inn på her. Vi vil bare nevne at det også ble utviklet en egen standard for kvalitetsledelse eller styring av kvalitet og en standard for revisjon av kvalitet.

Disse standardene har vært gjenstand for flere runder med utvikling. Det kan derfor være nyttig å gå tilbake til hovedprinsippene for kvalitetsutvikling og styring av kvalitet.

For det første baserer kvalitetsutvikling seg på at virksomhetens hovedprosesser er beskrevet. En måte å starte kvalitetsutvikling på er å foreta en prosessanalyse, en beskrivelse av praksis. Denne gjøres deretter til gjenstand for forbedringer, basert på 1) kjennskap til hvordan man arbeider og 2) måling av resultater. Måling av resultater uten kjennskap til hvordan de fremkommer, har ingen mening. Hva skal man da forbedre? I kvalitetsarbeidet er det snakk om systematiske tiltak, ikke tilfeldige.

For det andre holdes kjerneprosesser og styringsprosesser atskilt. Styringsprosessene skal sørge for at det foregår et systematisk og styrt arbeid med forbedring av prosessene på alle nivåer i organisasjonen. Men det forutsettes at hovedprosessene er dokumentert. I kvalitetsarbeidet er det disse som i utgangspunktet skal forbedres, også med tanke på hvordan de ivaretar lovkrav.

Avvik brukes i kvalitetsutvikling som utgangspunkt for forbedringer, men det er viktig å merke seg, at prosessene *i utgangspunktet* skal være innrettet med tanke på å gi tillit til at krav til prosessene og resultatene vil bli ivaretatt. Dette er et viktig element å ta med seg også i informasjonssikkerhetsarbeidet. Arbeidsprosessene, her for eksempel saksbehandlingsprosessene, bør legges opp med tanke på at man (også tredjepart/en utenforstående) skal kunne ha tillit til at de ulike kravene blir ivaretatt.

Kvalitetssystemenes filosofi ble ikke tatt inn i offentlig sektors forbedringsarbeid i full bredde. Man skilte på krav som er satt i regelverk og krav og behov som brukerne ellers måtte ha. *Internkontroll kom i offentlig sektor til å dreie seg om å dokumentere at krav i medhold av lov og forskrift var oppfylt.* Forutsetningen som ligger til grunn i kvalitetstenkningen, om dokumentasjon av kjerneprosessene ble ikke tatt med i regelverket. Det enkelte

regelverk har formålsavgrensede krav om dokumentasjon, ikke et krav om at kjerneprosessene skal være dokumenterte.

NS 7799, som ligger til grunn for kapittel 2 i personopplysningsforskriften, har med andre ord en annen filosofisk bakgrunn enn det som kommer til uttrykk i regelverket.

Vi tror at noe av usikkerheten i offentlige virksomheter når det gjelder å implementere regelverket på operativt nivå, dels kommer av at regelverket ikke skiller tydelig på styring og kjerneprosesser, dels at det ikke er krav om at (dokumentasjon av) kjerneprosessene skal legges til grunn for arbeidet med informasjonssikkerhet på operativt nivå.

Vi vet fra før at mange virksomheter har gjort et stort arbeid med å beskrive kjerneprosessene. Dette gjelder både statlig og kommunal sektor. Det ligger eksempler på dette på www.kunnskapsnettverk.no, spesielt fra Arendal kommune. I dette prosjektet har vi sett at også Fredrikstad kommune har jobbet med dokumentasjon av saksbehandlingsprosessene, her prosessene i sosialtjenesten. Men disse prosessene har ikke foreløpig vært koplet til arbeidet med informasjonssikkerhet.

Prosjektgruppen mener det er grunn til å se nærmere på mulighetene for å bruke prosessorienterte beskrivelser av saksbehandlingsrutinene også i arbeidet med informasjonssikkerhet.

5 Erfaringer fra arbeid med informasjonssikkerhet i offentlige og private virksomheter

I dette kapitlet omtaler vi erfaringer i forbindelse med gjennomføring av regelverket om informasjonssikkerhet. Vi har intervjuet personer fra offentlige og private virksomheter. Deres erfaringer er knyttet til gjennomføringen på overordnet nivå, ved innføring av styringssystemer, og i noen grad til arbeid med implementering av regelverket på operativt nivå, i saksbehandlingen.

Intervjuene er gjennomført med utgangspunkt i et spørreskjema og finnes som Vedlegg 5 til rapporten.[26]

Følgende personer ble intervjuet:

- Odd Tangen, IT-sikkerhetsrådgiver, Norsk Tipping
- Bent Markussen, kvalitets- og sikkerhetssjef, EDB Business-partner
- Herbjørn Andresen, Gunn Pettersen, Mari Nylund og Trond Laupstad, Rikstrygdeverket
- Raghild Folgerø, sikkerhetsleder, Toll- og avgiftsdirektoratet
- Heidi Thorstensen, sikkerhetsleder og personvernombud, Ullevål universitetssykehus
- Ivar Otto Voll, Turid Johansen og Ingerid Gjølstad, Fredrikstad kommune
- Jim-Arne Hansen og Anders Neerland Soleim, Lotteri- og stiftelsestilsynet
- Frank E. Celius, daglig leder, Norsk Hydro pensjon

Informantene ble blant annet spurt om hvilken støtte de fant i regelverket i forbindelse med etablering av styringssystem og om de eventuelt hadde benyttet standarder for informasjonssikkerhet eller annet verktøy.[27]

> De fleste informantene opplyser at de har støttet seg til regelverket for personvern. De fleste gir inntrykk av at de har god oversikt over hvilke andre regler om informasjonssikkerhet som gjelder for dem. På direkte spørsmål viser det seg imidlertid at flere for eksempel ikke kjenner til eforvaltningsforskriften.
>
> Noen opplyser at de har brukt NS 7799 (Norsk standard Styringssystem for informasjonssikkerhet) i arbeidet med informasjonssikkerhet. Også andre standarder og verktøy er benyttet i arbeidet, blant annet WLA (Norsk Tipping), Cobit (Norsk Hydro pensjon) og ITIL (Norsk Tipping). Nærmere omtale av standarder og verktøy som er benyttet fremgår av Vedlegg 3. RTV

[26] Undersøkelsen ble gjennomført som en kvalitativ undersøkelse, basert på en intervjumal.

Norsk Tipping har reservert seg mot publisering av intervjuet på grunn av dets muntlige form.

[27] Innrykk i teksten viser funn fra intervjuene.

har skjelet til diverse standarder, men har laget sitt styringssystem som et internkontrollsystem tilpasset RTVs behov.[28]

På spørsmål om det er et mål å sertifisere seg etter NS 7799, svarer de fleste at dette ikke er aktuelt.

> Som begrunnelse oppgis det blant annet at sertifisering er en ressurskrevende prosess som ikke står i forhold til nytteverdien for deres virksomhet. Det skal i denne sammenheng nevnes at EDB Business-partner allerede er sertifisert etter Både ISO 9001 og NS 7799 og at Norsk Tipping er sertifisert etter WLA. For EDB Business-partner er det forretningsforhold og kunder som krever sertifisering, og Norsk Tipping må være sertifisert for å kunne samarbeide med lotteriselskaper i andre land.

Informantene ble spurt om opplevde problemer i forbindelse med gjennomføring av regelverket, både på overordnet nivå og på operativt nivå.

> De fleste gir uttrykk for at arbeidet med gjennomføring av regelverket for informasjonssikkerhet på overordnet nivå har vært ressurskrevende. Noen har benyttet ekstern bistand, mens andre utlukkende har brukt interne ressurser. Det understrekes betydningen av å arbeide tverrfaglig. De fleste har opplevd prosessen som krevende, men noen føler nå at de har ”kommet i mål”.
>
> På den annen side gir informantene inntrykk av at det har vært en utfordring å få utnyttet styringssystemene på operativt nivå, *det vil si å få integrert informasjonssikkerhet i de daglige saksbehandlingsrutinene*. Dette oppleves også å være en ressurskrevende prosess. Flere av informantene understreker derfor betydningen av at arbeidet forankres i beslutninger fra ledelsen og at de ansatte får tilstrekkelig opplæring. Ikke minst er det viktig at opplæringen gis med jevne mellomrom for å hindre at de ervervede kunnskapene ikke ”går i glemmeboken”.

Et par informanter trekker frem eksempler på hvordan manglende forståelse for regelverket, enten hos ansvarlig ledelse eller hos ansatte, kan gi noen utfordringer.

> Et av eksemplene gjelder innsyn i pasientjournaler. Hensynet til informasjonssikkerhet tilsier at det gis begrenset tilgang til slike journaler. Dette blir imidlertid ikke alltid møtt med forståelse hos studenter og forskere som ønsker slik tilgang. Et annet eksempel gjelder informasjon på utbetalingsblanketter om hva utbetalingen gjelder. Mottaker av utbetalingen kan ha berettiget ønske og rettslig krav om diskresjon. Her skal hensynet til stønadsmottaker og taushetsplikten gå foran utbetalers eventuelle behov for enkle løsninger.

Informantene ble spurt om hvordan de opplever tilsynsmyndighetenes oppfølging av informasjonssikkerhetsarbeidet.

[28] Deler av styringssystemet er lagt ut på www.kunnskapsnettverk.no, på prosjektrom som krever registrering.

> Noen svarer at de har fått gode innspill, mens andre mener at tilsynet virker sporadisk. Flere nevner imidlertid Datatilsynets hjemmesider som et bra hjelpemiddel for å arbeide med informasjonssikkerhet.

På bakgrunn av vårt forslag om å opprette et "Beste praksis-fellesskap", ble informantene spurt om de kunne tenke seg å delta i en nettverksgruppe for informasjonssikkerhetsarbeid.

> Samtlige stiller seg positivt til et slikt initiativ, blant annet fordi de mener det er mange spørsmål som det er ønskelig å kunne diskutere med andre likesinnede. Erfaringer knyttet til personvernombud blir spesielt nevnt. Både Ullevål sykehus og Toll- og avgiftsdirektoratet har etablert personvernombud, og informantene derfra gir uttrykk for at de gjerne deler sine erfaringer med andre virksomheter på dette området.

Inntrykk fra intervjuene kan oppsummeres slik:

Virksomhetene har først og fremst brukt ressurser på å innføre overordnede systemer for informasjonssikkerhet. Operativt nivå oppleves som en større utfordring. Noen oppga imidlertid at de var godt i gang også med dette. Hovedutfordringen for mange er å få avsatt tilstrekkelige ressurser til opplæring og bevisstgjøring av samtlige ansatte. Mye arbeid er nedlagt i å skaffe oversikt over regelverket og sette reglene i sammenheng med de arbeidsoppgavene som skal utføres i deres virksomhet. Mange opplever at de selv har måttet "finne opp hjulet" og imøteser derfor et forum hvor de kan innhente erfaringer fra andre virksomheter med tilsvarende problemstillinger.

Informasjonen fra intervjuene gjorde at prosjektgruppen gikk nærmere inn i regelverket for å se hvordan dette støtter informasjonssikkerhetsarbeidet på henholdsvis styringsnivå og operativt nivå, se kapittel 2 og vedlegg 2.

6 Lovverket for informasjonssikkerhet anvendt direkte på saksbehandlingsrutinene

I dette kapitlet viser vi til et forsøk med å integrere regelverket for informasjonssikkerhet i etablerte rutiner i Fredrikstad kommunes sosialtjeneste.

Vi fikk her god hjelp av Ann-Christin Aakre Olsen ved sosialtjenesten.

Det viste seg at Sosialtjenesten i Fredrikstad hadde etablert mange rutinebeskrivelser, og at det også var et fast opplegg for å revidere og forbedre rutinene. Vi fant at de etablerte rutinebeskrivelsene var beregnet på saksbehandlere som kjente saksgangen godt, og var derfor lite detaljerte. I rutineblankettene er det referert til Lov om sosiale tjenester, men ikke referert til regler om informasjonssikkerhet. Vi tror at dette er en normal situasjon. Rutinene fungerer sikkert godt i saksbehandlingen i dag. Vi fant at selv om det ikke er referert til regelverket om informasjonssikkerhet, så er det likevel en rekke forhold knyttet til informasjonssikkerhet som blir ivaretatt.

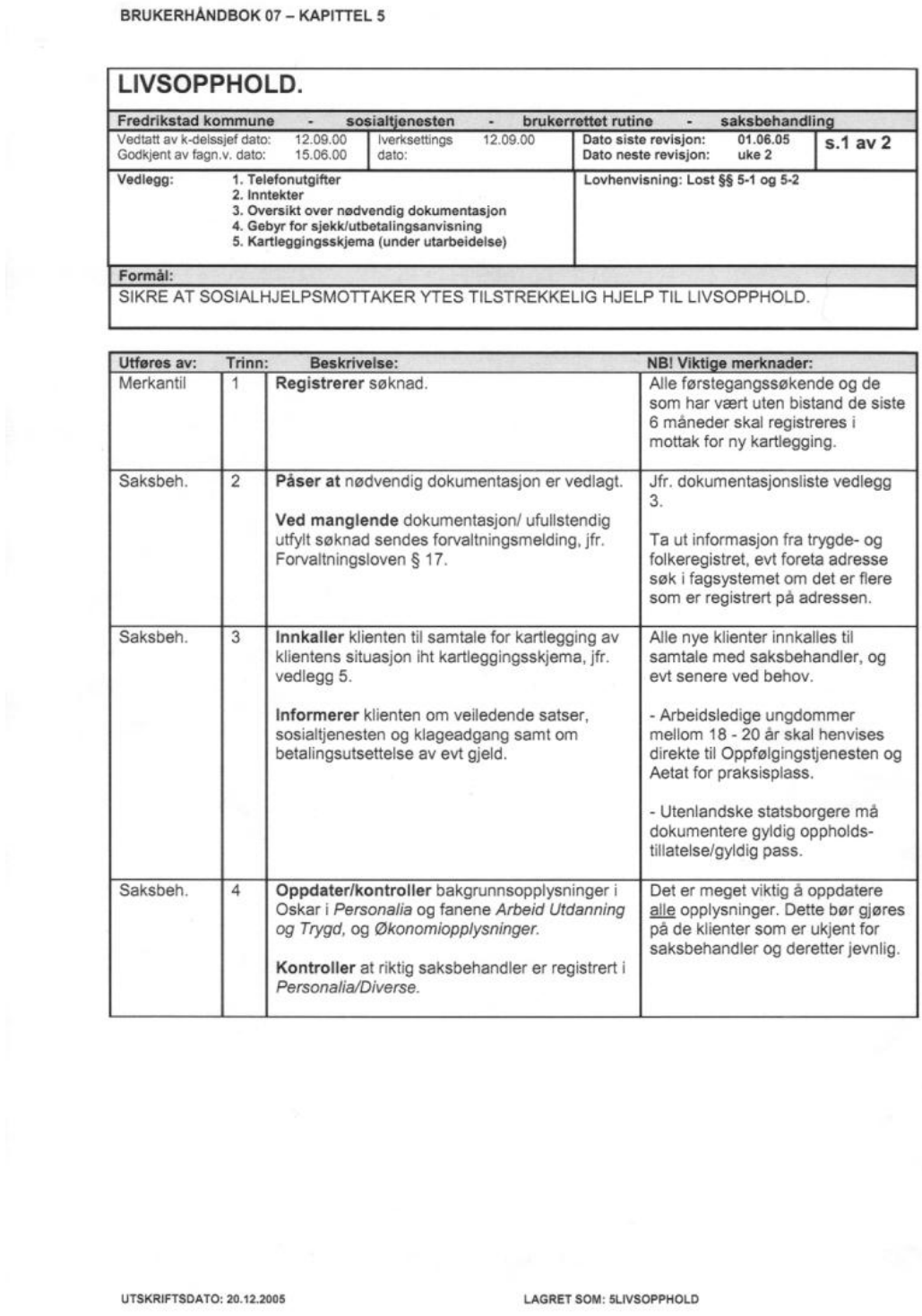
Hensikten med forsøket på å lage rutiner som også viser til regelverket om informasjonssikkerhet, var å prøve ut om regelverket kan implementeres på en dokumentert måte på operativt nivå, det vil si i saksbehandlingsrutinene. Det ble derfor nødvendig å etablere en mer detaljert prosessbeskrivelse.

6.1 Forutsetninger

For å lage et mest mulig realistisk eksempel har vi tatt utgangspunkt i rutiner i Fredrikstad kommune. Vi har gjennomført intervju med saksbehandler i Sosialtjenesten for å få et overblikk over saksgangen, og det er denne saksgangen vi har brukt som utgangspunkt for å implementere regelverket for informasjonssikkerhet. Men fremstillingen av saksgangen er likevel kun ment som et eksempel. I virkeligheten må man jobbe i flere omganger med å beskrive saksgang og detaljerte rutiner. En overordnet fremstilling av rutinene bør vise hvilke ulike typer saker som kan forekomme, og den enkelte rutine (for en bestemt type sak) bør bearbeides slik at alle viktige forhold som regelverket prøver å regulere, synliggjøres. Arbeid med å implementere regelverket på rutinenivå vil være en iterativ prosess, både med hensyn til dokumentasjon og de reelle handlingene som utføres.

6.2 Eksempel med bakgrunn i Fredrikstad kommune

Sosialetaten i Fredrikstad kommune har som nevnt, organisert arbeidet med dokumentasjon av saksbehandlingsrutinene. Blant annet er det et eget rutineutvalg som jevnlig gjennomgår rutinene og kommer med forslag til forbedringer. Dette var et godt utgangspunkt for forsøket i dette prosjektet. Figur 1 viser et eksempel på rutinedokumentasjon fra Sosialtjenesten i Fredrikstad. Rutinen er navngitt, det er informasjon om godkjenning og revisjon, samt henvisning til lov om sosiale tjenester.



BRUKERHÅNDBOK 07 – KAPITTEL 5

LIVSOPPHOLD.

Fredrikstad kommune - sosialtjenesten - brukerrettet rutine - saksbehandling

Vedtatt av k-delssjef dato: 12.09.00 Godkjent av fagn.v. dato: 15.06.00	Iverksettings dato: 12.09.00	Dato siste revisjon: 01.06.05 Dato neste revisjon: uke 2	s.1 av 2

Vedlegg:
1. Telefonutgifter
2. Inntekter
3. Oversikt over nødvendig dokumentasjon
4. Gebyr for sjekk/utbetalingsanvisning
5. Kartleggingsskjema (under utarbeidelse)

Lovhenvisning: Lost §§ 5-1 og 5-2

Formål:

SIKRE AT SOSIALHJELPSMOTTAKER YTES TILSTREKKELIG HJELP TIL LIVSOPPHOLD.

Utføres av:	Trinn:	Beskrivelse:	NB! Viktige merknader:
Merkantil	1	**Registrerer** søknad.	Alle førstegangssøkende og de som har vært uten bistand de siste 6 måneder skal registreres i mottak for ny kartlegging.
Saksbeh.	2	**Påser at** nødvendig dokumentasjon er vedlagt. **Ved manglende** dokumentasjon/ ufullstendig utfylt søknad sendes forvaltningsmelding, jfr. Forvaltningsloven § 17.	Jfr. dokumentasjonsliste vedlegg 3. Ta ut informasjon fra trygde- og folkeregistret, evt foreta adresse søk i fagsystemet om det er flere som er registrert på adressen.
Saksbeh.	3	**Innkaller** klienten til samtale for kartlegging av klientens situasjon iht kartleggingsskjema, jfr. vedlegg 5. **Informerer** klienten om veiledende satser, sosialtjenesten og klageadgang samt om betalingsutsettelse av evt gjeld.	Alle nye klienter innkalles til samtale med saksbehandler, og evt senere ved behov. - Arbeidsledige ungdommer mellom 18 - 20 år skal henvises direkte til Oppfølgingstjenesten og Aetat for praksisplass. - Utenlandske statsborgere må dokumentere gyldig oppholds-tillatelse/gyldig pass.
Saksbeh.	4	**Oppdater/kontroller** bakgrunnsopplysninger i Oskar i *Personalia* og fanene *Arbeid Utdanning og Trygd*, og *Økonomiopplysninger*. **Kontroller** at riktig saksbehandler er registrert i *Personalia/Diverse*.	Det er meget viktig å oppdatere alle opplysninger. Dette bør gjøres på de klienter som er ukjent for saksbehandler og deretter jevnlig.

UTSKRIFTSDATO: 20.12.2005 LAGRET SOM: 5LIVSOPPHOLD

Fig 1: Utdrag fra eksempel på rutinebeskrivelse i Fredrikstad kommune, Sosialtjenesten. Utdraget viser 4 av til sammen 8 trinn.

En gjennomgang av rutinedokumentasjonen viste at den først og fremst forholder seg til Lov om sosiale tjenester og at detaljeringsnivået forutsetter god faglig oversikt. Det er mange forhold som er underforståtte, og de trinn som er beskrevet er valgt fordi de kan relateres til Lov om sosiale tjenester.

Vi ønsket å se på om regelverket for informasjonssikkerhet kunne refereres for de enkelte trinn i saksbehandlingsflyten. For å få frem et mer detaljert bilde, ble det laget en oversikt over saksbehandlingsflyten i samarbeid med saksbehandler fra Sosialtjenesten. Denne oversikten er vist i Figur 2. Flytskjemaet viser flere detaljer/trinn i arbeidsprosessen enn den opprinnelige rutinebeskrivelsen. Da vi etterpå arbeidet med å kople regelverket for informasjonssikkerhet til de enkelte trinn i arbeidsprosessen, ble det klart at detaljeringsnivå og hvordan man fremstiller arbeidsprosessen har betydning for arbeidet med å vurdere hvordan informasjonssikkerheten blir berørt og hvor regelverket kommer til anvendelse. Det kan godt tenkes at man i det daglige kan greie seg med en mer summarisk fremstilling, men for en analyse av arbeidsprosessen og for opplæringsformål i forhold til regelverket for informasjonssikkerhet, bør fremstillingen være relativt detaljert. Man bør sørge for å få med seg alle arbeidstrinn hvor personinformasjon utveksles muntlig, nedtegnes skriftlig eller registreres i et datasystem, transporteres, mellomlagres i posthyller, skrives ut på printere, sendes med post, overføres elektronisk til andre og lagres i arkiv.

En slik arbeidsflytbeskrivelse vil kunne være et godt grunnlag for en risikoanalyse knyttet til saksbehandlernes og administrative funksjoners håndtering av saksinformasjon og det fysiske miljøet rundt dette, samt analyse av risikoen for manglende eller mangelfull etterlevelse av regelverket. Dette kan også gi grunnlag for interne og eksterne revisjoner i forhold til om og i hvilken grad regelverket etterleves.

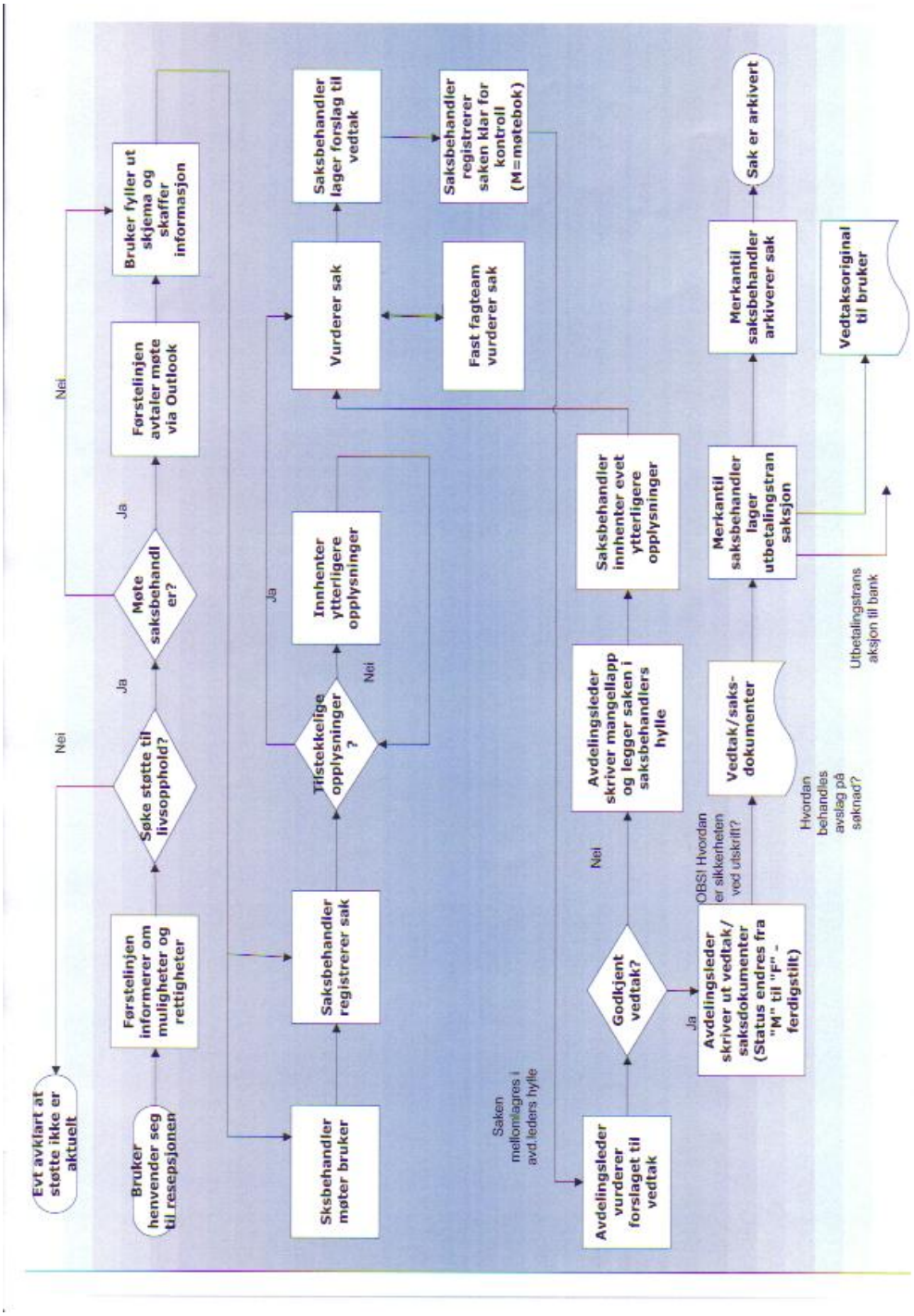
(I tillegg kommer selvsagt sårbarhetsanalyse som gjelder elektronisk infrastruktur, fagsystemet og driftsmiljøet.)

På bakgrunn av den beskrevne saksflyten, ble det i prosjektet laget en ny tekstbasert rutinebeskrivelse over samme lest som Sosialtjenesten benytter, men nå også med en kolonne for henvisning til regelverket for informasjonssikkerhet. Denne er vist i figur 3. Vi gjør oppmerksom på at dette er gjennomført som en prøve på om det er mulig å lage direkte koplinger mellom saksbehandlingsrutiner og regelverket for informasjonssikkerhet. Den nye rutinen er ikke godkjent for bruk i Sosialetaten i den formen den har på nåværende stadium.

Se figur 2 og 3 på de neste sidene.

Når det foreligger instrukser, forvaltnings- eller domsavgjørelser av betydning for tolkning og saksbehandling, kan slik informasjon også kobles til aktuelle arbeidstrinn i saksbehandlingsprosessen.

Det finnes mange IT-verktøy som kan håndtere dette, og som kan gi førstelinjen betydelig bedre støtte i saksbehandlingen enn de har i dag.



Figur 2: Flytskjema. (Obs at dette kun er et eksempel og at flytskjemaet trenger bearbeiding for å avspeile den faktiske rutinen på en tilfredsstillende måte.) Flytskjemaet er mer detaljert enn den opprinnelige rutinen for å vise arbeidstrinn som berøres av regelverket for informasjonssikkerhet.

Den ”nye” rutinebeskrivelsen viser flere arbeidstrinn og viser til Lov om sosiale tjenester, Forvaltningsloven og regelverket for personopplysninger.[29]

LIVSOPPHOLD.

Fredrikstad kommune - sosialtjenesten - brukerrettet rutine - saksbehandling

Vedtatt av k-delssjef dato:	12.09.00	Iverksettings	12.09.00	**Dato siste revisjon:**	**01.06.05**
Godkjent av fagn.v. dato:	15.06.00	dato:		**Dato neste revisjon:**	**uke 2**

s.1 av 2

Vedlegg:	**Lovhenvisning:**
1. Telefonutgifter	**Lost §§ 5-1 og 5-2**
2. Inntekter	**POF Personopplysningsloven**
3. Oversikt over nødvendig dokumentasjon	**POL Personopplysningsforskriften**
4. Gebyr for sjekk/utbetalingsanvisning	**Fvl Forvaltningsloven**
5. Kartleggingsskjema (under utarbeidelse)	**eF eForvaltningsforskriften**

Formål:

SIKRE AT SOSIALHJELPSMOTTAKER YTES TILSTREKKELIG HJELP TIL LIVSOPPHOLD.

(Rutinen er tilpasset for å vise regelverk for informasjonssikkerhet og er ikke kontorets virkelige rutine.)

Utføres av:	**Trinn:**	**Beskrivelse:**	**NB! Viktige merknader:**	**Eksempler på rettsregler, bl.a. om informasjons-sikkerhet**
Resepsjon (1.-linjen)	1	**Informér** bruker om muligheter og rettigheter	Hvis stønad er aktuelt, gi bruker 4-siders blått søknadskjema og informasjon om utfylling	**Fvl § 11** (veiledningsplikt) og **§ 13** (Taushetsplikt) **LoST § 4-1** (Opplysning, råd og veiledning) og **§8-8** (Taushetsplikt) Hvis elektr søknad: **eF §§ 3** (Bruk av elektronisk kommunikasjon ved henvendelser til forvaltningen), **4** (Krav til bruk av sikkerhetstjenester og – produkter mv. ved henvendelser til forvaltningsorgan), **5** (Formidlling av taushetsbelagte opplysninger og personopplysninger til forvaltningen), **6** (Bekreftelse på et en henvendelse er mottatt) og **7** (Henvendelser som ikke tilfredsstiller aktuelle krav)

[29] OBS! Rutinen er ikke helt i samsvar med flytskjemaet og trenger en bearbeiding før den kan fremstå i en mer korrekt form.

Merkantil	2	For aktuelle søkere: **Vurder om møte med saksbehandler er nødvendig**		
Merkantil	3	**Avtal møte** med saksbehandler Tidspunkt og navn registreres i Outlook- kalender for aktuell saksbehandler		
Merkantil	4	**Informer om** erklæring om riktige opplysninger og om informert samtykke til innhenting av opplysninger. Bruker må skrive under på dette på søknadskjemaet.		**POL §§** **8** (Vilkår for å behandle personopplysninger), **9** (Behandling av sensitive personopplysninger), **11** (Grunnkrav til behandling av personopplysninger) **POF kap 2** (Informasjonssikkerhet)
Saks-behandler	5	**Saksbehandler møter bruker** Kartlegg livssituasjon og behov. Påse at nødvendige opplysninger er vedlagt. **Informerer** klienten om veiledende satser, sosialtjenesten og klageadgang samt om betalingsutsettelse av evt gjeld.		**Fvl § 13** flg **LoST § 8-8** Hvis søknad elektr: **eF §§3,4,5,6 og 7** Hvis søknad manuell: **eF § 1 (2)** (Forskriften gjelder elektronisk kommunikasjon og elektronisk saksbehandling. Dvs. gjelder selv om søknad sendes manuelt, da man benytter elektronisk saksbehandlingssystem)
Saks-behandler	6	**Saksbehandler vurderer tilsendt søknad.** **Påser at** nødvendig dokumentasjon er vedlagt. **Ved manglende** dokumentasjon/ufullstendig utfylt søknad sendes forvaltningsmelding, jfr. Forvaltningsloven § 17.	Jfr. dokumentasjonsliste vedlegg 3. Ta ut informasjon fra trygde- og folkeregistret, evt foreta adresse søk i fagsystemet om det er flere som er registrert på adressen.	

Saks-behandler	7	**Saksbehandler registrerer sak i fagsystemet** Fagsystemet Oscar. Brukers navn og personnummer registreres og systemet gir saken en saks-id. Saks-id føres på søknadsskjema.		**POL §§ 8, 9, 11**, **12** (Bruk av fødselsnummer m.v.), **13** (Informasjonssikkerhet), **14** (Internkontroll), jf **POF kap 2 og** **3** (Internkontroll) **Arkivforskr kap 3 A** (Behandling av post og saksdokumenter)
Forts. se vedlegg				

Figur 3: Figuren, som går over flere sider, viser en arbeidsversjon av saksbehandlingsflyt ved Fredrikstad kommune, Sosialtjenesten. I høyre kolonne er det lagt inn referanser til aktuelle rettskilder. Rutinen må bearbeides videre med hensyn til en korrekt gjengivelse av saksflyt mv. Hele rutinen er gjengitt i Vedlegg 4.

6.3 Erfaringer

Det vi fant gjennom forsøket, var at det går an å kople regelverket for informasjonssikkerhet direkte til saksbehandlingsrutinene, men at dette krever god innsikt i regelverket. Arbeidet med rutinebeskrivelser og å knytte regelverket opp mot de ulike trinn i arbeidsflyten, må gjennomføres som en iterativ/gjentakende prosess. Etter hvert som man trenger inn i regelverket, vil man lettere se hvilke sider av saksbehandlingen som blir berørt og derved bør beskrives.

I det videre praktiske arbeidet med regelverk knyttet til arbeidsprosessene, vil vi foreslå en analysefase der prosessene beskrives relativt detaljert, og hvor det aktuelle regelverket skrives ut, ikke bare refereres med §-henvisninger. Basert på en slik dokumentasjon kan man gjennomføre en sårbarhetsanalyse og forbedre rutinene. Deretter kan man eventuelt lage kortversjoner til daglig bruk.

Vi vil peke på at det finnes en rekke IT-baserte verktøy hvor prosesstrinn kan koples med tekst, og hvor det er mulig å lage elektroniske lenker fra et prosesstrinn til en mer detaljert rutinebeskrivelse og til de relevante regeltekstene, tolkningsinstrukser og avgjørelser i forvaltningen og domstolene.

Gjennom arbeidet med rutinen i Fredrikstad, fant prosjektgruppen at regelverket i liten grad eksponerer at informasjonssikkerhet skal ivaretas i saksbehandlingsprosessene, selv om det må forutsettes å være underforstått. Dette bidrar til å forklare det vi tidligere har påpekt som en overfokusering på styringssystem. Flere av de kravene som beskrives i Personopplysningsforskriften gjelder ledelsens overordnede ansvar, og det gis liten hjelp til å relatere kravene til saksflyten. (I rapporten er dette behandlet i kapittel 3.)

Vi tror at eksempler som vist fra Fredrikstad kommune kan være til hjelp for andre virksomheter. Man trenger ikke ”finne opp hjulet” hver for seg. Det bør lages en rekke gode eksempler fra sentrale rutiner fra ulike saksbehandlingsområder i statlig og kommunal virksomhet. Eksempler bør gjøres tilgjengelige som felles ressurs.

7 Forslag til tiltak og videre prosess

Her presenteres forslag til videre arbeid innenfor informasjonssikkerhet. Siden Fornyings- og administrasjonsdepartementet (FAD) er oppdragsgiver for dette prosjektet, er forslagene innrettet på hva vi mener det vil være naturlig for FAD å arbeide videre med, ut fra sin rolle og sitt ansvar. Noen av forslagene er følgelig også adressert til regelverksforvaltere og tilsyn generelt, eller til regelverksmottakere/brukere.

Departementet har et ansvar for strategi- og politikkutvikling knyttet til IT og utvikling av en helhetlig politikk for informasjonssamfunnet, inkludert informasjonssikkerhet. Departementet koordinerer regjeringens IT-politikk. FAD har også en ledende rolle i koordineringen og oppfølgingen av regjeringens nasjonale strategi for informasjonssikkerhet fra 2003, med blant annet etableringen av Koordineringsutvalget for informasjonssikkerhet (KIS) som et sentralt virkemiddel.

Dette prosjektet er et ledd i departementets ivaretakelse av sitt ansvar ut fra de nevnte utgangspunktene. Det er derfor naturlig å se tiltaksforslagene nedenfor i et bredt, nasjonalt perspektiv, ut fra departementets brede og sammensatte ansvar. I tillegg har FAD et særskilt forvalteransvar for to av de sentrale regleverkene på området: personopplysningsforskriften og eForvaltningsforskriften.

På denne bakgrunn foreslås følgende tiltak i punktene 7.1 – 7.5:

7.1 Utvikling av modeller og veiledning for arbeid med informasjonssikkerhet

Forslag 1: Modeller og veiledninger som skiller på styring og operativt nivå

Det settes i gang et arbeid for å utvikle gode modeller og veiledninger for informasjonssikkerhetsarbeidet. Vi har vist at regelverket for informasjonssikkerhet først og fremst er begrenset til et styringsperspektiv, men at dette ikke sies eksplisitt. Det operative perspektivet er stort sett fraværende, og savnes sterkt, ut fra det vi kanskje litt upresist kan kalle et saksbehandlernivå. Vi foreslår at man skiller tydelig på arbeidet med styring ut fra et ledelsesperspektiv og arbeidet med å konkret etterleve regelverket i virksomhetens kjerneprosesser/operative saksbehandling. Modellene bør inngå i en ny veiledning, der elektroniske metoder/læremidler tas i bruk og gjøres tilgjengelig via Internett.

Adressat: FAD ut fra sin rolle. I tillegg: departementer og direktorater med ansvar for å forvalte og føre tilsyn med regelverk for informasjonssikkerhet samt KIS.

Forslaget er todelt (7.1.1 og 7.1.2):

7.1.1 Etablering av en enkel modell/tilnærming til styring av informasjonssikkerhet (ledelsesperspektivet)

Det bør lages en enkel modell for hvilke ledelsesprosesser som skal være på plass i informasjonssikkerhetsarbeidet. Modellen kan ta utgangspunkt i krav i personopplysningsforskriften og eForvaltningsforskriften, og slik at ledelses- og styringsperspektivet rendyrkes. I dette arbeidet bør man også gi veiledning i forhold til NS 7799 eller tilsvarende standarder, for virksomheter som også vil arbeide ut fra en eller flere slike standarder, og så godt som mulig se dette i sammenheng med kravene i ulike regelverk. De overordnede juridiske normene bør ses i sammenheng med relevante styringssystemer.

7.1.2 Etablering av en modell for bruk av regelverket på operativt nivå (blant annet saksbehandlerperspektivet)

Det bør lages en modell for implementering av regelverket på operativt nivå. Den kan ta utgangspunkt i krav om dokumentasjon av virksomhetenes informasjonsinfrastruktur (teknisk infrastruktur, informasjonssystemer, informasjonen) og prosessene knyttet til disse, inkludert saksbehandlingsprosessene. På driftssiden er det flere som jobber med dokumentasjon av arbeidsprosessene etter rammeverket ITIL.

Det er særlig behov for å gi støtte til dokumentasjon av kjerneprosessene i virksomhetene, for eksempel saksbehandlingsprosesser som må utformes for å ivareta flere sett med krav, typisk fra ulike regelverk.

Det er også behov for å vise nærmere hvordan slike prosessbeskrivelser kan legges til grunn for risikovurderinger.

7.2 Etablering av et ”beste praksis”- fellesskap

Forslag 2:Beste praksis-fellesskap

Det etableres et såkalt praksisfellesskap (arena, forum) for arbeid med informasjonssikkerhet og etterlevelse av rettslige krav, av og for de virksomhetene/aktørene som har ansvar for etterlevelse og operativ gjennomføring (i motsetning til de departementer og direktorater som har ansvar for forvaltning og tilsyn i forhold til regelverkene).[30]

Praksisfellesskap kan omfatte møter, seminarer, felles nettsted for informasjon og diskusjon og arbeidsrom for arbeidsgrupper. Nettstedet bør presentere gode eksempler og felles tolkninger av regler om informasjonssikkerhet for de ulike regelverkseierne.

[30] Det er tidligere foreslått at det blir etablert et tilsvarende opplegg, men da for de departementer og direktorater som har ansvar for *forvaltning og tilsyn* for de aktuelle regelverkene. Forslaget kom fra en arbeidsgruppe for regelverk og informasjonssikkerhet, juni 2005, rettet til oppdragsgiver Koordineringsutvalget for informasjonssikkerhet, KIS. Forslaget er for tiden til behandling i KIS.

Deltakelse i nettverksarbeid og bruk av eksempler og veiledningsstoff bør være gratis.

Adressat: De virksomheter i offentlig og privat sektor som ut fra egeninteresse vil delta i dette.

Gjennom prosjektet har vi avdekket at virksomhetene jobber mye alene med informasjonssikkerhetsarbeidet. Noen henter inspirasjon fra deltakelse i kurs og seminarer og noen deltar i organiserte nettverk (medlemsbaserte) eller uformelle nettverk. Det vil være store gevinster ved et utvidet praksisfellesskap rundt arbeidet med informasjonssikkerhet både i offentlig og privat sektor, med fokus på *etterlevelse og gjennomføring i den operative virksomheten*. En del temaer vil være felles for de to sektorene, og en del vil være forskjellige. Dette kan håndteres ved inndeling av praksisfellesskap etter behov i hver sin sektor, i tillegg til fellesinnsats på felles problemstillinger.

Et slikt praksisfellesskap kan både bidra til etablering av gode arbeidsmodeller, som nevnt i foregående forslag, og til erfaringsbaserte forbedringer. I tillegg til utvikling av modeller for hvordan man kan jobbe med informasjonssikkerhet, vil det være behov for arbeid både med etablering av referanseprosesser for bestemte typer saksbehandling og for å etablere oversikter over regelverket knyttet til disse. Med erfaringer fra dette prosjektet, kan vi si at det er relativt mye arbeid med å finne frem til de relevante rettsreglene som gjelder for ulike saksbehandlingstrinn.

På kommunal side er gevinstene åpenbare, i og med at 435 kommuner har de samme oppgavene. Om ikke arbeidsprosessene er helt like, vil mange ha god nytte av å kunne ta mønster fra andre. Også i statlig sektor vil det være mye å hente ved et større praksisfellesskap om saksbehandlingsrutiner. Alle steder der informasjon innhentes, bearbeides, registreres, sendes eller skrives ut, vil de samme generelle krav til informasjonssikkerhet gjelde. Oversikt over hvilke rettsregler som gjelder for ulike saksbehandlingstrinn vil kunne ha stor overføringsverdi. I tillegg vil gode eksempler på sikkerhetsvurderinger og -tiltak knyttet til referanseprosesser ha overføringsverdi på tvers av offentlig sektor.

Gode prosessbeskrivelser vil kunne danne felles utgangspunkt for implementering av krav fra en rekke ulike lover og forskrifter. For virksomhetene vil man da få en enhetlig fremstilling av virksomheten og hvordan ulike krav ivaretas. Dette vil også være nyttig for tilsynsarbeidet.

En forutsetning for å lykkes, er at et praksisfellesskap drives av et miljø med erfaring og entusiasme for informasjonssikkerhetsarbeidet og hvor særinteresser ikke stenger for bred deltakelse.

7.3 Vurdering av økt dokumentasjonskrav i regelverket?

Forslag 3: Økt dokumentasjonskrav

Regelverksforvalterne bør vurdere om det bør gis et generelt krav om dokumentasjon av saksbehandlingsprosessene.

Når det gjelder personopplysningsforskriften og eForvaltningsforskriften, bør disse bli mer tydelige på et dokumentasjonskrav, og mer eksplisitte på når kravet gjelder styringsprosessene og når det gjelder saksbehandlingsprosessene. Dette bør vurderes ved neste revisjon. Frem til da vil utarbeidelse av veiledninger mv. i henhold til pkt. 7.1 kunne gi ytterligere innspill og kunnskap til et slikt arbeid.

Adressat: De enkelte regelverksforvalterne og Fornyings- og administrasjonsdepartementet (FAD) som har forvalteransvaret for de to nevnte forskriftene (og som også er oppdragsgiver for denne rapporten).

Det er et gjennomgående trekk i regelverket at kravene om dokumentasjon knytter seg til ivaretakelsen av en rekke enkeltvise kontrolltiltak mv, og i mindre eller ingen grad til de verdiskapende prosessene som saksbehandling i ulike sammenhenger innebærer, med rutiner for å ivareta kravene.

Dokumentasjon av (saksbehandlings)prosessene bør legges til grunn for arbeidet med informasjonssikkerhet i den operative virksomheten.

7.4 Prosessbeskrivelser som støtte i regelverksutvikling?

Forslag 4: Eksempler på saksbehandlingsrutiner som grunnlag for regelverksutvikling

Det fremskaffes eller utvikles gode eksempler på kjerneprosesser (jf 7.1 og 7.2), som innspill til vurdering ved videreutvikling av regelverkene.

Adressat: Departementer og direktorater med ansvar for å forvalte og føre tilsyn med regelverk for informasjonssikkerhet og KIS.

Myndighetene som lager, forvalter og videreutvikler regelverk bør se dette i forhold til de mest typiske rutinene av felles karakter for saksbehandling som det praktiske liv må leve etter.

Brukerne oppfatter at det er et stort gap mellom rettslige normer og den operative virksomheten i virksomhetene. Videre har vi sett at det er en rekke parallelle regler om informasjonssikkerhet, og vist eksempler på at ett trinn i en saksbehandlingsprosess skal ivareta informasjonssikkerhetskrav fra flere lover og forskrifter samt fra særlovgivning for saksbehandlingsområdet.

Gode eksempler på kjerneprosesser som viser typisk arbeidsgang og hvilke lover/forskrifter som fra før av gjelder for de ulike arbeidstrinn, kunne være god støtte for utvikling av regelverk som er tydelig på hvordan nye regler kan implementeres i praksis. Prosesseksempler fra sentrale arbeidsprosesser og

hvilke lover/regler som allerede gjelder, vil også kunne medvirke til færre overlappende regler.

Vi foreslår at dette prøves i praksis ved revisjon av regelverk for informasjonssikkerhet.

7.5 Forenkling av regelverk for behandling av fortrolig/taushetsbelagt informasjon

Forslag 5: Forenkling av taushetsregler

Det bør settes i gang et arbeid for å evaluere og eventuelt forenkle innholdsmessig og strukturelt relevante regler om taushetsplikt og den konkrete behandlingen slik informasjon krever. Det er kun taushetspliktreglene i offentlig sivil sektor forslaget knytter seg til. Det omfatter altså ikke reglene for rikets sikkerhet mv., eller næringslivets tilsvarende regler.

Adressat: Forvaltere av aktuelle regelverk, herunder blant annet Justisdepartementet, Statsministerens kontor, Fornyings- og administrasjonsdepartementet, samt helsesektoren.

Brukerne opplever mange regelverk på dette området, som beskrevet blant annet foran i kapitel 3.2. Den samlede mengden av regler å holde oversikt over er meget utfordrende både i forhold til overordnet styring og for etterlevelse på det operative nivået. Å legge opp gode rutiner på området er så vidt vi kan forstå meget krevende. I tillegg kommer at reglene om taushetsplikt må vurderes i forhold til regler om opplysningsplikt mv. (ikke fremstilt foran i 3.2).

Lov- og forskriftsreglene som pålegger taushetsplikt er tilnærmet tause om hvordan taushetsplikten i praksis skal følges. De sier at informasjon må beskyttes på betryggende måte, men ikke *hvordan* dette kan skje. Det er opp til den enkelte. I statlig sektor finner vi ett unntak fra dette i reglene i beskyttelsesinstruksen. Der er det detaljerte behandlingsregler. De etterleves imidlertid neppe i særlig grad. Dette skyldes nok at få vet om dem, og at reglene er koblet til forsvarets regler på en tung og kompliserende måte, som sikkert frister mange til å se bort fra dem.[31]

Vi foreslår at reglene på dette området blir gått gjennom og forenklet, både innholdsmessig og strukturelt. Det er også et hensyn at det bør være like regler både i stat og kommune, hvilket det ikke er i dag. Det bør vurderes om beskyttelsesinstruksens formål kan oppnås på en annen måte enn ved dagens løsning, for eksempel ved regler i forvaltningsloven og/eller i forskrift til forvaltningsloven, i forlengelsen av de generelle reglene om taushetsplikt der. Det er her reglene på mange måter hører hjemme, og de bør balanseres mot aktuelle regler i personvernlovgivningen og i særlovgivningen.

[31] Se nærmere omtale i kapitel 3.2.4

Vedlegg 1 Oppsummering av Statskonsults oppdrag 2005

Dette vedlegget gir en oppsummering av Statskonsults arbeid med informasjonssikkerhet de siste par årene, med særlig fokus på virksomheten i 2005.

1.1 Bakgrunn

Arbeidet har sin bakgrunn i Nasjonal strategi for informasjonssikkerhet og er gjennomført på oppdrag for Moderniseringsdepartementet som en del av departementets oppfølging av eget ansvarsområde i forhold til nasjonal strategi. Departementet har definert sitt ansvar til å omfatte tiltak både i statlig og kommunal sektor, da det er avgjørende viktig å etablere tillit til informasjonssikkerhet i offentlig sektor for å nå målene om eForvaltning.

Statkonsult har bidratt med planarbeid i forhold til departementets oppfølging av Nasjonal strategi og med gjennomføring av konkrete prosjekter. Prosjektene har dels hatt fokus på regelverket for informasjonssikkerhet, dels på forvaltning av regelverket og dels på etterlevelse av regelverket i virksomheter. I forbindelse med innhenting av informasjon om etterlevelse av regelverket, er det også innhentet informasjon fra noen få private virksomheter.

1.2 Problemstillinger

I første halvår 2005, gjennomførte en arbeidsgruppe nedsatt av Koordineringsutvalget for informasjonssikkerhet (KIS), en studie av regelverket for informasjonssikkerhet og forvaltningen av regelverket. Arbeidsgruppen Regelverk og informasjonssikkerhet ble ledet av Amund Eriksen, Statskonsult, og hadde deltakere fra Universitetet, avdeling for forvaltningsinformatikk, fra Nasjonal sikkerhetsmyndighet, Post- og teletilsynet, Datatilsynet, Forsvarsdepartementet og Kredittilsynet. Arbeidet er dokumentert i en forprosjektrapport[32] som foreslår en rekke tiltak.

Arbeidsgruppens mandat var dels å skaffe til veie en oversikt over regelverk med betydning for informasjonssikkerheten, dels å peke på mulige problemområder med hensyn til eventuelle mangler, overlappinger og/eller motstridigheter, samt etterlevbarhet, og å utarbeide anbefalinger til hvordan identifiserte problemområder kan angripes på kort og lang sikt.

Prosjektet pekte på behovet for bedre empiri som grunnlag for videreutvikling av regelverket for informasjonssikkerhet og at det bør ses nærmere på hvordan regelverket samordnes. Det er ikke etablert et formalisert samarbeid mellom myndigheter med ansvar for regelverk og informasjonssikkerhet, og dette fører til at koordineringen må skje i den enkelte virksomhet, med de problemer dette medfører for virksomhetene. Det er også behov for bedre informasjonskanaler

[32] Forprosjektrapport fra arbeidsgruppen Regelverk og informasjonssikkerhet til Koordineringsutvalget for informasjonssikkerhet (KIS), Oslo, 7. juni 2005.

og pedagogiske tiltak rettet mot virksomheter. Andre tiltak som ble foreslått var knyttet til bruk av standarder for administrasjon av informasjonssikkerhet, som ISO 17799 (BS 7799/NS 7799), og en vurdering av om flere regelverk bør henvise til eller bygge på standarder som et minstekrav for oppfyllelse av regelverket.

Departementet ønsket eksempler på hvordan virksomheter konkret opplevde regelverket, og Statskonsult gjennomførte i august/september 2005 intervjuer med utvalgte virksomheter. Undersøkelsen hadde ikke krav om representativitet, det skulle kun innhentes eksempler på brukererfaringer. Brukererfaringene[33] ble oppsummert som følger:

- Det er vanskelig for en virksomhet å etablere full oversikt over regelverket
- Det er vanskelig å etablere oversikt over hvilke deler av den operative virksomheten som berøres av de ulike kravene
- Det kan se ut som det er en overdimensjonert fokus på styring av informasjonssikkerhet i forhold til å sikre implementering av regelverket på operativt nivå i virksomhetene
- Det må skapes forståelse, både hos regelverksforvaltere og virksomheter, for at de enkelte regelsett ikke kan medføre egne kontrollsystemer pr regelsett i virksomhetene. På operativt nivå, hvor ansatte i næringsliv, kommuner og statlige virksomheter 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/saksbehandlingsflyt. Virksomheter som har erfaring med ISO 9000-serien for kvalitetsutvikling og/eller BS 7799/ NS 7799 mener selv å ha god kontroll i informasjonssikkerhetsarbeidet.
- Regelverket benytter et juridisk språk som er vanskelig tilgjengelig i virksomhetene, og ulike deler av regelverket benytter ulike begreper på samme sak
- Det oppleves at forholdet mellom ulike regelverk er vanskelig å forstå
- Det er behov for bedre veiledning fra myndighetenes side når man henvender seg dit med tolkningsproblemer
- Det oppleves at det er et stort gap mellom rettslige normer og den operative hverdag i virksomhetene. Reglene sier noe om hva som skal gjøres, men det sies lite eller ingenting om hvordan.

Basert på de to arbeidene som her er referert, har Statskonsult på oppdrag fra Moderniseringsdepartementet (nå Fornyings- og administrasjonsdepartementet, FAD) høsten 2005 gjennomført videre intervjuundersøkelser og drøftinger med virksomheter. Med bakgrunn i KIS-arbeidsgruppens spørsmål knyttet til bruk av standarder som grunnlag for regelverket og med bakgrunn i at virksomheter som har erfaringer med bruk av kvalitetsstandarder og/eller standarden for administrasjon av informasjonssikkerhet synes å lykkes i arbeidet med

[33] Regelverk og informasjonssikkerhet; eksempler på brukererfaringer. Statskonsult 5. september 2005.

informasjonssikkerhet, ble arbeidet innrettet mot en dypere studie av bruken av standarden for administrasjon av datasikkerhet. Er det slik at bruk av BS 7799/ NS 7799 gjør det enklere å implementere regelverket for informasjonssikkerhet?

Ganske snart ble det klart at av de vi fikk kontakt med var det relativt få virksomheter i offentlig som i privat sektor som hadde benyttet BS 7799/NS 7799. Det ble også ganske fort avdekket at det er mange ulike tilnærminger til arbeidet med informasjonssikkerhet, og undersøkelsen ble derfor vinklet mer generelt på hvordan virksomheter har innrettet seg i arbeidet med informasjonssikkerhet. Med bakgrunn i det vi i brukererfarings-rapporten kalte overdimensjonert fokus på styring av informasjonssikkerheten og informasjon som kom frem gjennom de videre intervjuene, har prosjektgruppen sett på hvordan deler av regelverket kan identifiseres og brukes direkte ned på de operative saksbehandlingsrutinene. Det er gjennomført ett eksempel på dette, og eksemplet beskrives nærmere i denne rapporten.

Prosjektarbeidet som er hovedanliggendet for denne rapporten dreier seg hovedsakelig om to tilnærminger til informasjonssikkerhetsarbeidet:

- Arbeidet på overordnet nivå i virksomhetene (ledelsesnivået)
- Arbeidet på operativt nivå (dvs. blant annet saksbehandlingsnivå).

Basert på de erfaringene som kom frem gjennom prosjektet, ble det også naturlig å vurdere deler av regelverket med tanke på hvordan det støtter/ ikke støtter informasjonssikkerheten på henholdsvis overordnet og operativt nivå.

Vedlegg 2 Regelverket i forhold til styring og saksbehandling

I dette prosjektet har vi gjennomgått en del av regelverket for informasjonssikkerhet med tanke på å finne ut hva i forskriften som dreier seg om styringsprosesser og hva som egner seg for implementering i kjerneprosessene/saksbehandlingsprosessene. Ikke uventet er det flest bestemmelser som kan kategoriseres som styringsprosesser. En del av bestemmelsene er imidlertid av en slik karakter at de egner seg for implementering i saksbehandlingsprosessene. Vår analyse må betraktes kun som en foreløpig analyse.

Hva sier regelverket og standardene om generell styring av informasjonssikkerhet?

Generelle styringsparametere	**Regel/standard**
	Forvaltningsloven - Fvl *eForvaltningsforskriften* – eF *Sosialtjenesteloven* - LoSt *Personopplysningsloven*- Pol *Personopplysningsforskriften- Pof* *Sosialtjenestel. § 4A-10* *Arkivloven*- Arkivl *Arkivforskriften*- Arkivf *NS 7799 Tillegg A 7 (fysisk og miljømessig sikkerhet)* *NS 7799 Tillegg A 8 (Kommunikasjons- og driftsadministrasjon)*
Hvem er behandlingsansvarlig?	Pol §§ 2, 3 og 4 Pof kap 1 eF § 3 Sosialtjenstel. Kap. 2 Fvl § 1
Mål	Pof § 2-3 annet ledd eF Kap 3
Strategi	Pof § 2-3 tredje ledd e-fvf. Kap 3 NS 7799 Tillegg A 3 NS 7799 Tillegg A 4

Oversikt over personopplysninger Klassifisering av informasjon	Pol § 8 (vilkår for å behandle) Barnevernl. § 3-1 (barnevern) Helsepersonell. §§ 39 flg (helseopplysninger) Sosialtjenestel. § 2-1 (sosial omsorg) Opplæringsl. § 13-5 (elever, foresatte) Pol § 13 NS 7799 Tillegg A.6
Risikovurdering	Pol § 13 Pof § 2-4 eF § 5 Datatilsynets veileder om risikovurdering av informasjonssystem NS 5814 krav til risikoanalyse NS 7799 Tillegg A 5
Sikkerhetsrevisjon	Pol § 13 Pof § 2-5
Organisering av arbeidet/ Ansvars- og myndighetsforhold	Pol § 13 Pof § 7-2 NS 7799 Tillegg A 8
Beredskapsplanlegging *Utilsiktet avbrudd* *Sikkerhetskopiering* *Avviksbehandling*	Pol § 13 Pof § 2-4 Pof § 2-6 NS 7799 Tillegg A 11
Sikkerhet hos andre virksomheter	Pol § 13, jf. § 15 Pof § 2-15 NS 7799 Tillegg A 4.2 og A 4.3
Sikkerhet *Personellsikkerhet (kompetanse, taushetsplikt, autorisasjon)* *Fysisk sikkerhet (adgangskontroll)* *Systemteknisk sikkerhet*	Pol § 13 Pof §§ 2-8, 2-9 Pof § 2-10 Pof §§ 2-11, 2-13 Pof §§ 2-12, 2-14 Sosialtjenestel. §§ 2-3, 4A-10, 8-8, 8-8a eF §§ 2-8, 5, 15 eFkap 4 og 5 NS 7799 Tillegg A 6

Dokumentsikkerhet (tilgang, intern og ekstern forsendelse, oppbevaring og sletting)	NS 7799 Tillegg A 9 NS 7799 Tillegg A 10 NS 7799 Tillegg A 11
Dokumentasjon *Dokumentasjonskontroll (korrekt utformet og kjent blant ansatte)* *Styrende dokumenter (sikkerhetsmål, strategier mv.)* *Prosedyrer (risikovurdering, sikkerhetsrevisjon, ledelsens gjennomgang, konfigurasjonsendring, beredskapsplaner, avviksbehandling, adgangskontroll, tilgangskontroll, datakommunikasjon, dokumentsikkerhet)* *Registreringer (resultater av arbeidet med informasjonssikkerhet, hendelsesregister/aktivitetslogg)*	Pof § 2-16 NS 7799 Tillegg A 12
Internkontroll	Pol § 14 Pof kap. 3

Hva sier regelverket om saksbehandling?

Gjennomgangen av regelverket viser at relativt få krav relaterer seg direkte til saksbehandlingsflyten/operativt nivå.

Hendelse	**Regel/standard**
	Se forkortelser i forrige tabell.
Bruker henvender seg til	eF §§ 3, 4, 5, 6, 7 (alm. Krav ved bruk av

forvaltningsorgan	el.komm. med forvaltningen)
Førstelinjen informerer om muligheter og rettigheter	Fvl § 11 (veiledningsplikten) LoSt §4-1 (veil./inf.plikten)
Avklare at man ikke fyller vilkår for søknad – opplyse om klageadgang	Fvl §§ 11 jf kap V (klagebehandling) eF § 9 (klage)
Saksbehandler registrerer sak	Pol §§ 3a, 8, 9, 11, 12, 13, 14 (alm. regler for beh. av personoppl.) LoSt § 8-8 (taushetsplikt) Pof §§ 2-10 – 2-14 (fysisk sikring) Fvl §§ 13 flg (taushetsplikt)
Saksbehandler innhenter ytterligere opplysninger	Fvl § 17 (utrednings- og inf.plikt) Pol § 27 (retting av feil)
Saksbehandler registrerer foreløpig vedtak	Pol §§ 3a, 8, 9, 11, 12, 13, 14 (alm. regler for beh. av personoppl.) LoSt § 8-8 (taushetsplikt) Pof §§ 2-10 – 2-14 (fysisk sikring) Fvl §§ 13 flg (taushetsplikt)
Saken sendes avdelingsleder	*Papir, e-post eller internt it-system*
Avdelingsleder treffer vedtak og utformer dokument (registrerer)	Pol §§ 3a, 8, 9, 11, 12, 13, 14 (alm. regler for beh. av personoppl.) LoSt § 8-8 (taushetsplikt) Pof §§ 2-10 – 2-14 (fysisk sikring) Fvl §§ 13 flg (taushetsplikt)
Vedtak sendes til effektuerende myndighet (for eksempel bank)	Pol §§ 3a, 8, 9, 11, 12, 13, 14 (alm. regler for beh. av personoppl.) LoSt § 8-8 (taushetsplikt) Pof §§ 2-10 – 2-14 (fysisk sikring) Fvl §§ 13 flg (taushetsplikt)
Søker orienteres om vedtak	eF§ 8 (underretning om vedtak)
Saken arkiveres	Arkivl § 6 (plikten til å ha arkiv) Arkivf. § 2-13, kap 3 A og 5 eF § 26 (om arkivering av avansert elektronisk signatur)
Saksbehandler rapporterer funksjonssvikt	eF § 23 (varslingsplikt ved tap eller mistanke om misbruk) NS 7799 Tillegg A 6.3.2

Vedlegg 3 Noen aktuelle standarder og verktøy

Dette vedlegget nevner kort de standarder og verktøy intervjuobjektene refererer til i arbeidet med informasjonssikkerhet, samt noen flere. Et felles perspektiv for disse standardene er at de kan bidra til å gi tillit til en virksomhets evne (og vilje) til å ivareta sikkerhetsbehovene i et helhetlig og organisasjonsmessig forsvarlig perspektiv.

Vi har to norske varianter av en sentral, britisk standard; BS 7799: A Code of Practice for Information Security Management, som har to deler. BS 7799 er basert på såkalt beste praksis/god praksis innen arbeidet med informasjonssikkerhet både i England og i mange andre land. Del 1 omhandler god praksis for styring av informasjonssikkerhet og del 2 beskriver styringssystem for informasjonssikkerhet.

Del 1 er blitt internasjonal standard med betegnelsen *ISO/IEC 17799:2005, Information technology -- Security techniques -- Code of practice for information security management*. Denne ble fastsatt som Norsk Standard; *NS-ISO/IEC 17799:2005 i juni 2005. Den norske oversettelsen ble utgitt i februar 2006; Informasjonsteknologi – Sikkerhetsteknikk - Administrasjon av informasjonssikkerhet(ISO/IEC 17799:2005).*

Del 2 ble opprinnelig videreutviklet som britisk standard BS 7799-2:2002 Information security management systems – Specification with guidance for use. Den er også oversatt og blitt norsk standard *NS 7799:2003 Styringssystem for informasjonssikkerhet. Beskrivelse med veiledning for bruk.*[34]

Siste nytt er en ny internasjonal standard publisert 15. oktober i fjor; *ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements*. Denne bygger på en revidert versjon av den britiske standardens del 2 , og inngår i en ny ISO nummerserie 27000, som etter hvert skal omfatte også de andre standardene på dette området.[35]

---

[34] Se sidene til Norsk senter for informasjonssikring http://www.norsis.no for en nærmere omtale av de norske variantene av disse standardene (trykk på "veiledninger", så "sertifisering og evaluering"). Standardene kan kjøpes fra Standard Norge, se http://www.standard.no/. Noen av standardene ligger også til grunn for en norsk ordning for frivillig sertifisering av informasjonssikkerhet i organisasjoner, forvaltet av Norsk Akkreditering. Ved å bruke søkeordet *Informasjonssikkerhet* på nettsiden deres kan en få oversikt over de som er sertifisert i henhold til ulike relevante standarder; http://www.akkreditert.no. Der kan en finne de tre firmaene i Norge som er akkreditert (godkjent) til å sertifisere organisasjoner etter bl.a. NS 7799, og BS 7799-2: Veritas, Nemko og Teknologisk Institutt. En kanskje enklere oversikt får man her: www.kvalex.no.

[35] Se for nærmere omtale http://www.xisec.com/, som er nettsiden til den internasjonale brukergruppen av Information Security Management Systems (ISMS). Her står bl.a. følgende forklaring: "The ISMS International User Group is a business-led, international network of users of ISO/IEC 17799 and BS 7799 Part 2. It was established by the DTI (Department of Trade and Industry) in 1997 to facilitate a means of sharing experiences in the use of these standards. The ISMS International User Group and this web site continues to be supported by the DTI as part of their wider promotion of best practice to the business community." Denne nettsiden gir god oversikt og innsikt i disse standardene, og tilgang til siste nytt.

ITIL (Information Technology Infrastructure Library) er et rammeverk for IT-drift basert på britisk standard BS 15000.[36] Rammeverket ivaretar store deler av BS 7799 på informasjonssikkerhet, men ikke på alle områder. Enkelte virksomheter har gitt uttrykk for at kontinuerlig arbeid med ITIL ivaretar informasjonssikkerhetsarbeidet. ITIL forutsetter at sentrale arbeidsprosesser knyttet til driften dokumenteres.

WLA (World Lottery Association) er standarden for virksomheter som driver med lotterivirksomhet, typisk Norsk Tipping. I følge vår informant derfra er standarden i utgangspunktet 80-85% tilnærmet lik BS 7799, og WLA Security Committee vurderer å trekke ut lotteridelen i standarden for deretter kun å videreutvikle denne delen, og for øvrig forholde seg til den til enhver tid gjeldende/mest aktuelle variant av BS 7799.

Et annet sentralt regelverk er den amerikanske Sarbanes-Oxley Act (SOX) fra 2002. SOX ble vedtatt som et resultat av de store skandalene i amerikansk næringsliv knyttet til presisjonen i finansiell informasjon. SOX stiller omfattende krav til etablering og dokumentasjon av internkontrollprosesser relevant for regnskapet. Dette omfatter IT-systemer og infrastruktur. Myndighetene har pekt på COBIT og ISO/IEC 17799 som mulige rammeverk for å dokumentere samsvar med SOX. SOX gjelder for alle selskap som er notert på amerikansk børs og underlagt det amerikanske Kredittilsynet (Security and Exchange Commission) sitt myndighetsområde. Dette gjør den relevant for en rekke norske selskap: Statoil, Norsk Hydro, Telenor mfl.[37]

En helt annen type standard er *Common Criteria for information technology security evaluation*, i kortform Common Criteria eller CC. Denne gir grunnlag for å spesifisere og evaluere sikkerhet i IT-produkter og systemer, under forutsetning om at bestemte regler og metoder er fulgt. CC finnes også i form av en internasjonal standard: ISO/IEC 15408:2005, Information technology. Security techniques. Evaluation criteria for IT security. CC skal brukes i henhold til Common Evaluation Methodology (CEM). Begge har versjonsnummer v2.3, siste versjoner i denne serien. En høringsversjon v3.0 foreligger allerede, og v3.1 vil bli obligatorisk.[38] Virksomheter med krav til relativt høy grad av sikkerhet kan med fordel kombinere krav til virksomheten (for eksempel NS 7799) med krav til virksomhetskritiske tekniske komponenter ut fra CC.[39]

I prosjektet har de vi har intervjuet kjennskap til eller jobber etter følgende standarder; NS ISO/IEC 17799, ITIL (BS-15000), WLA. Noen av standardene har henvisninger til hverandre, eksempel ITIL henviser til BS 7799 når det gjelder prosessen Security Management.

Enkelte virksomheter har nevnt at de kjenner til COBRA og som har brukt dette som bakgrunnsmaterilale. COBRA er et IT-verkøty med en modul Risk

---

[36] Se den offisielle nettsiden til ITIL: http://www.itil.co.uk/

[37] Kilde: Veiledning lover og regler med betydning for informasjonssikkerhet, IT-SikkerhetsForum, versjon 1.1 september 2004.

[38] Se den offisielle nettsiden her: http://www.commoncriteriaportal.org/

[39] Se den norske ordningen for sertifisering i henhold til CC: http://sertit.no

Consultant og en modul for å undersøke samsvar med ISO 17799. Risk Consultant kan håndtere ulike risikovurderinger[40].

[40] Rapport Informasjonssikkerhet Risikovurdering og sikkerhetsstyring – metoder og verktøy 18. aug. 2004

Vedlegg 4 Ny skisse til rutine i Sosialtjenesten

LIVSOPPHOLD.					
Fredrikstad kommune - sosialtjenesten - brukerrettet rutine - saksbehandling					
Vedtatt av k-delssjef dato:	12.09.00	Iverksettings dato:	12.09.00	**Dato siste revisjon:** **Dato neste revisjon:**	**01.06.05** **uke 2**
Godkjent av fagn.v. dato:	15.06.00				**s.1 av 2**
Vedlegg: **1. Telefonutgifter** **2. Inntekter** **3. Oversikt over nødvendig dokumentasjon** **4. Gebyr for sjekk/utbetalingsanvisning** **5. Kartleggingsskjema (under utarbeidelse)**				**Lovhenvisning:** **Lost §§ 5-1 og 5-2** **POF Personopplysningsloven** **POL Personopplysningsforskriften** **Fvl Forvaltningsloven** **eF eForvaltningsforskriften**	
Formål:					
SIKRE AT SOSIALHJELPSMOTTAKER YTES TILSTREKKELIG HJELP TIL LIVSOPPHOLD. (Rutinen er tilpasset for å vise regelverk for informasjonssikkerhet og er ikke kontorets virkelige rutine.)					

Utføres av:	**Trinn:**	**Beskrivelse:**	**NB! Viktige merknader:**	**Eksempler på rettsregler, bl.a. om informasjons-sikkerhet**
Resepsjon (1.-linjen)	1	**Informér** bruker om muligheter og rettigheter	Hvis stønad er aktuelt, gi bruker 4-siders blått søknadskjema og informasjon om utfylling	**Fvl § 11** (veiledningsplikt) og **§ 13** (Taushetsplikt) **LoST § 4-1** (Opplysning, råd og veiledning) og **§8-8** (Taushetsplikt) Hvis elektr søknad: **eF §§ 3** (Bruk av elektronisk kommunikasjon ved henvendelser til forvaltningen), **4** (Krav til bruk av sikkerhetstjenester og – produkter mv. ved henvendelser til forvaltningsorgan), **5** (Formidlling av taushetsbelagte opplysninger og personopplysninger til forvaltningen), **6** (Bekreftelse på et en henvendelse er mottatt) og **7** (Henvendelser som ikke tilfredsstiller aktuelle krav)

Merkantil	2	For aktuelle søkere: **Vurder om møte med saksbehandler er nødvendig**		
Merkantil	3	**Avtal møte** med saksbehandler Tidspunkt og navn registreres i Outlook- kalender for aktuell saksbehandler		
Forts. neste side				
Merkantil	4	**Informer om** erklæring om riktige opplysninger og om informert samtykke til innhenting av opplysninger. Bruker må skrive under på dette på søknadskjemaet.		**POL §§** **8** (Vilkår for å behandle personopplysninger), **9** (Behandling av sensitive personopplysninger), **11** (Grunnkrav til behandling av personopplysninger) **POF kap 2** (Informasjonssikkerhet)
Saks-behandler	5	**Saksbehandler møter bruker** Kartlegg livssituasjon og behov. Påse at nødvendige opplysninger er vedlagt. **Informerer** klienten om veiledende satser, sosialtjenesten og klageadgang samt om betalingsutsettelse av evt gjeld.		**Fvl § 13** flg **LoST § 8-8** Hvis søknad elektr: **eF §§3,4,5,6 og 7** Hvis søknad manuell: **eF § 1 (2)** (Forskriften gjelder elektronisk kommunikasjon og elektronisk saksbehandling. Dvs. gjelder selv om søknad sendes manuelt, da man benytter elektronisk saksbehandlingssystem)
Saks-behandler	6	**Saksbehandler vurderer tilsendt søknad.** **Påser at** nødvendig dokumentasjon er vedlagt. **Ved manglende** dokumentasjon/ufullstendig utfylt søknad sendes forvaltningsmelding, jfr. Forvaltningsloven § 17.	Jfr. dokumentasjonsliste vedlegg 3. Ta ut informasjon fra trygde- og folkeregistret, evt foreta adresse søk i fagsystemet om det er flere som er registrert på adressen.	

Saks-behandler	7	**Saksbehandler registrerer sak i fagsystemet** Fagsystemet Oscar. Brukers navn og personnummer registreres og systemet gir saken en saks-id. Saks-id føres på søknadsskjema.		**POL §§ 8, 9, 11**, **12** (Bruk av fødselsnummer m.v.), **13** (Informasjonssikkerhet), **14** (Internkontroll), jf **POF kap 2 og** **3** (Internkontroll) **Arkivforskr kap 3 A** (Behandling av post og saksdokumenter)
Forts. neste side				
Saks-behandler	8	**Saksbehandler vurderer om det foreligger tilstrekkelig informasjon** og innhenter evet ytterligere opplysninger **(**kartleggingsskjema, jfr. vedlegg .	Alle nye klienter innkalles til samtale med saksbehandler, og evt senere ved behov. - Arbeidsledige ungdommer mellom 18 - 20 år skal henvises direkte til Oppfølgingstjenesten og Aetat for praksisplass. - Utenlandske statsborgere må dokumentere gyldig oppholds-tillatelse/gyldig pass.	**LoST §§ 8-4** (Plikt til å rådføre seg med klienten), **8-5** (Innhenting av opplysninger)
Saks-behandler	9	**Oppdater/kontroller** bakgrunnsopplysninger i Oskar i *Personalia* og fanene *Arbeid Utdanning og Trygd*, og *Økonomiopplysninger*. **Kontroller** at riktig saksbehandler er registrert i *Personalia/Diverse.*	Det er meget viktig å oppdatere alle opplysninger. Dette bør gjøres på de klienter som er ukjent for saksbehandler og deretter jevnlig.	

Saks- behandler	10	**Vurderer** søknaden i forhold til søkers økonomiske situasjon. **Ved innvilgelse** av støtte vurderes det om: - hvilken sats som skal benyttes - skal det settes vilkår for utbetaling, jfr § 5-3 - skal ytelsen gis som lån, jfr egen rutine - er det søkt Husbankens bostøtte. Vurdering av transporterklæring - er det søkt trygdeytelse. Vurdering av refusjonskrav til trygdekontoret, jfr egen rutine.	Alle nye skal i utgangspunkt vurderes etter korttidsnorm i 3 - 6 måneder hvis klienten har hatt et høyt grunnlag for livsopphold eller har konkrete muligheter til å bli selvhjulpen innen rimelig tid. Ved disponeringsproblem er vurderes utbetalingshyppighet.	**LoST § 8-5** (Innhenting av opplysninger)
Fagteam	11	**Saken vurderes evt av fast fagteam**		
Saks- behandler	12	**Saksbehandler lager forslag til vedtak**		**Fvl kap 5** (Regler om skriftlighet og begrunnelse)
Forts. neste side				
Saks- behandler	13	**Saksbehandler registrerer forslag til enkeltvedtak** Saken registreres klar for kontroll. Status settes til M for Møtebok (Avdelingsleders møtebok) Saken mellomlagres i avdelingsleders hylle.	(spml: er mellomlagring i leders hylle omfattet av betryggende sikkerhet?)	
Avd. leder	14	**Avdelingsleder fatter** vedtak. Saker med mangler legges i saksbehandlers hylle med mangellapp for ny behandling. Saker med vedtak gis behandlingskode F for "ferdigstilt". Saksdokumenter og vedtak skrives ut og sak legges i hylle for merkantil behandling. Se pkt 15.	Økonomisk beregning skal inn i vedtaksteksten.	**POF § 2-10 til 2-14** (Fysisk sikring, Sikring av konfidensialitet, tilgjengelighet, integritet, Sikkerhetstiltak) **Fvl § 13 flg** (Taushetsplikt) **LoST § 8-8** (Taushetsplikt)

Merkantil saks-behandling	15	**Merkantil saksbehandler** lager utbetalingstransaksjon til banken, sender vedtaksoriginal til bruker og arkiverer saken.		**Arkivlov § 6** og **Ark-forskr § 2-13** (Elektronisk saksdokument)**, kap 3A** (Behandling av post og saksdokument) **og kap 5** (Eldre og avslutta arkiv) **Fvl § 27** (Underretning om vedtak) **eF § 8** (Underretning om enkeltvedtak og enkelte andre meddelelser fra forvaltningsorgan)

Figur 3: Figuren, som går over flere sider, viser en arbeidsversjon av saksbehandlingsflyt ves Fredrikstad kommune, Sosialtjenesten. I høyre kolonne er det lagt inn referanser til aktuelle rettskilder. Rutinen må bearbeides videre med hensyn til en korrekt gjengivelse av saksflyt mv.

Vedlegg 5 Intervjuer om arbeidet med informasjonssikkerhet

Intervjuene ligger som separat vedlegg og kan hentes fra www.kunnskapsnettverk.no.

Referanseark for Statskonsult

Tittel på rapport:	Arbeid med informasjonssikkerhet; fra juss til styring og rutiner
Statskonsults rapportnummer:	2006:4
Forfatter(e):	Kirsti Berg , Amund Eriksen, Margaret Hagevik og Heidi Høiskar
Evt. eksterne samarbeidspartnere:	
Prosjektnummer:	1053
Prosjektnavn:	Informasjonssikkerhet
Prosjektleder:	Kirsti Berg
Prosjektansvarlig avdeling:	eForvaltning
Oppdragsgiver(e):	Fornyings- og administrasjonsdepartementet

Resymé/omtale:

Regelverket for informasjonssikkerhet har særlig fokus på styring av informasjonssikkerheten, selv om mange regler kan brukes på operativt nivå, for eksempel i saksbehandlingsrutinene. Rapporten viser hvordan rutiner kan utformes med basis i prosessbeskrivelser og analyse av regelverket med hensyn til de enkelte trinn i saksbehandlingsrutinene.

Rapporten tar blant annet til orde for økt krav til dokumentasjon av saksbehandlingsrutiner og at regelverket bør skille på krav til styringssystemer og til dokumentasjon av ivaretakelse av regelverket på operativt nivå.

Emneord:

Informasjonssikkerhet, styring av informasjonssikkerhet, informasjonssikkerhet i saksbehandlingsrutiner, forenkling av taushetsreglene

Totalt antall sider til trykking (uten forside):	58 Rapporten kan også hentes fra www.kunnskapsnettverk.no
Dato for utgivelse:	30. mars 2006
Utgiver:	**Statskonsult as** Postboks 8115 Dep 0032 OSLO www.Statskonsult.no