Rogaland Revisjon IKS

FORVALTNINGSREVISJON AV

ELEKTRONISK BEHANDLING AV SENSITIVE PERSONOPPLYSNINGER

ROGALAND FYLKESKOMMUNE

JANUAR 2013

INNHOLD

Denne rapportens målgrupper er kontrollutvalget, andre folkevalgte, formelt ansvarlige i administrasjonen og utførende fagfolk i administrasjon. Rapporten er et offentlig dokument og er tilgjengelig også for media og andre interesserte. Behovene varierer, men her er en leserveiledning med to nivåer for hvor dypt rapporten kan behandles:

1. Innholdsfortegnelsen, sammendraget og rådmannens kommentarer
2. Hovedrapporten med innledning, fakta og vurderinger, samt vedlegg

SAMMENDRAG

Innledning og avgrensning

Dette forvaltningsrevisjonsprosjektet undersøker om fylkeskommunen legger til rette for informasjonssikkerhet på en tilfredsstillende måte.

Revisjonsprosjektet er avgrenset til *elektronisk* behandling av *sensitive* personopplysninger. Med behandling menes enhver bruk av personopplysninger, eksempelvis innsamling, registrering, sammenstilling, lagring eller utlevering. Med sensitive personopplysninger menes;

- Rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning
- At en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling
- Helseforhold
- Seksuelle forhold
- Medlemskap i fagforeninger

Fylkeskommunen behandler sensitive personopplysninger i følgende datasystemer:

- ESA – Sak- og arkivsystem for bruk i hele fylkeskommunen.
- PPI – Klientsystem for bruk i PP-tjenesten.
- OTTO – Klientsystem for bruk i Oppfølgingstjenesten
- OPUS – Elektronisk pasientjournalsystem for bruk i Tannhelse Rogaland FKF

I tillegg til assisterende rådmann og leder for IKT- og arkivseksjonen, har vi intervjuet systemansvarlige for disse fire fagsystemene. Vi har vurdert praksis opp mot kravene i personopplysningsloven m/ forskrift og fylkeskommunens reglement.

Både organisatoriske og tekniske tiltak

Informasjonssikkerhet oppnås ved hjelp av planlagte og systematiske tiltak. De tiltak som etableres, skal være av både *organisatorisk* og *teknisk* karakter.

Hovedinntrykket er at fylkeskommunen har *tekniske* løsninger som i stor grad sørger for at gjeldende regler for elektronisk behandling av sensitive personopplysninger blir fulgt. Dette er tekniske løsninger som autorisasjonskontroll, inndeling i soner, brannmur, spamfilter, viruskontroll og back-up, for å nevne de viktigste. Fra systemene er det fullt mulig å hente ut logger som viser hvem som har gjort hva. De undersøkte enhetene benytter taushetserklæringer og informerer om hva taushetsplikten innebærer i praksis.

Avvikene i forhold til kravene finner vi først og fremst i tilknytning til de *organisatoriske* tiltakene som loven krever:

- **Sikkerhetsledelse:** Fylkeskommunens sikkerhetsmål- og strategi har ikke blitt gjennomgått av ledelsen så hyppig som forskriften og fylkeskommunens informasjonssikkerhetshåndbok krever.
- **Risikovurdering:** Risikovurderingen vil kunne gi svar på hvilke mangler som finnes og hva som må gjøres. Det er gjennomført svært begrenset med risikovurderinger de senere årene.
- **Sikkerhetsrevisjon:** Ledelsen i fylkeskommunen har plikt til å kontrollere at vedtatte mål, strategier og organisering i forbindelse med informasjonssikkerhet blir fulgt. Faktisk bruk av informasjonssystemet skal sammenlignes med de retningslinjer for bruk som er besluttet. Alle deler av virksomheten skal kontrolleres innenfor en 12 måneders periode. Dette er ikke blitt gjort de seneste årene.
- **Avviksrutiner:** Det er ikke blitt meldt inn noen avvik til leder for IKT- og arkivseksjonen. Når det i slike avvikssystemer ikke blir registrert noen avvik, er det grunn til å vurdere om systemet fungerer etter hensikten.
- **Oversikt over ansvars- og myndighetsforhold:** Gjeldende håndbok for informasjonssikkerhet tegner et bilde av ansvars- og myndighetsforhold som ikke stemmer med virkeligheten. Eksempelvis er ordningen med personvernombud ikke nevnt, til tross for at fylkeskommunen fikk sitt første ombud i 2008.

Mangel på dokumenterte, årlige ledelsesgjennomganger, risikovurderinger og sikkerhetsrevisjoner ble også påpekt i Rogaland Revisjon sitt forvaltningsrevisjonsprosjekt i 2005.

Konsekvenser av avvik

Fylkeskommunen har ikke registrert tilfeller av uautorisert utlevering av sensitive personopplysninger, og revisjonen har heller ikke funnet at sensitive personopplysninger er kommet på avveie, men vi kan ikke utelukke at dette kan skje. Fylkeskommunens tekniske løsninger synes å være godt innrettet mot å forebygge dette, men den organisatoriske oppfølgingen har ikke vært i henhold til forskriften og fylkeskommunens egen håndbok for informasjonssikkerhet. Manglende gjennomføring av organisatoriske tiltak innebærer ikke i seg selv at personopplysninger behandles på en kritikkverdig måte. De organisatoriske tiltakene skal først og fremst forebygge og således forhindre kritikkverdig behandling av sensitive personopplysninger.

I 2008 valgte fylkeskommunen å opprette et personvernombud. Foruten å føre en oversikt over virksomhetens behandling av personopplysninger, skal ombudet påse at virksomheten følger personopplysningsloven. I dette ligger at ombudet kan foreta stikkprøve-kontroller, men ombudet har ikke ansvar for at alle lover og regler faktisk blir fulgt. Dette ansvaret ligger på ledelsen. Intervjusvarene peker imidlertid i retning av at det har hersket noe uklarhet omkring dette punktet så lenge ordningen med personvernombud har eksistert i Rogaland fylkeskommune.

Revisjonens anbefalinger

- **Vi anbefaler** fylkeskommunens ledelse å gjennomføre risikovurderinger når datasystemene endres eller når det oppstår endringer i trusselbildet. Risikovurderingen bør danne grunnlag for iverksetting av nødvendige sikkerhetstiltak.

- **Vi anbefaler** fylkeskommunens ledelse å gjennomføre sikkerhetsrevisjon, det vil si å kontrollere at de sikkerhetstiltak som er besluttet etablert, faktisk er iverksatt og fungerer etter sin hensikt.

- **Vi anbefaler** ledelsen å vurdere hvorvidt sikkerhetsmål, strategi og organisering av fylkeskommunens datasystem, er i samsvar med virksomhetens behov. En slik vurdering bør foretas én gang per år. Resultater fra sikkerhetsrevisjoner og risikovurderinger bør gjennomgås samtidig.

- **Vi anbefaler** at ansvars- og myndighetsforhold vedrørende sikring av sensitive personopplysninger blir klargjort og tydelig kommunisert ut i organisasjonen.

FYLKESRÅDMANNENS OG FYLKESTANNLEGENS KOMMENTAR

Fylkesrådmannens kommentarer
Fylkesrådmannen takker for rapporten og revisjonens anbefalinger.

I arbeidet med informasjonssikkerhet i RFK har en fokusert på tekniske løsninger, systemer og rutiner som skal sørge for at gjeldende regler for elektronisk behandling av sensitive personopplysninger blir fulgt. Etablerte systemer og rutiner skal forebygge at sensitive personopplysninger kommer på avveie. Problemstillinger knyttet til informasjonssikkerhet er tatt opp og løst fortløpende.

På bakgrunn av rapporten, klargjøring av gjeldende regelverk og roller, erkjenner fylkesrådmannen at organisatoriske tiltak må utføres på en mer systematisk måte og dokumenteres. Det må etableres en tilfredsstillende dokumentert internkontroll.

Fylkesrådmannen ser at sikkerhetsorganiseringen må bli bedre kjent i organisasjonen og at det foretas en tilstrekkelig systematisk gjennomgang av informasjonssikkerhet på ledelsesnivå. Dette vil fylkesrådmannen få på plass i løpet av første kvartal 2013 sammen med revidert håndbok for informasjonssikkerhet. Bedre opplæring av ledere og øvrige ansatte vil bli prioritert.

Fylkestannlegens kommentarer
Tannhelse Rogaland er et fylkeskommunalt foretak (FKF) som ivaretar fylkeskommunenes ansvar for den offentlige tannhelsetjenesten slik det beskrives i tannhelsetjenesteloven. Foretaket er ikke et eget rettssubjekt, men en del av fylkeskommunen.

Valget av en slik organisering innebærer at foretaket er direkte underlagt Fylkestinget. Foretakets styre og daglig leders (fylkestannlegens) myndighet er regulert i kommuneloven. Fylkestannlegen er underlagt styret, og ikke fylkesrådmannen. Det er derfor fylkestannlegen som er ansvarlig for internkontrollen vedrørende elektronisk behandling av sensitive personopplysninger i foretaket.

Foretaket skal revideres opp mot «Norm for informasjonssikkerhet i helse-, omsorgs- og sosialsektoren». Denne normen er et omforent sett av krav til informasjonssikkerhet basert på lovverket, og som er utarbeidet av representanter for helsesektoren, bl.a. Le-

geforeningen, Sykepleierforbundet, Tannlegeforeningen, KS, Apotekerforeningen og regionale helseforetak.

Normen kan stille strengere krav enn det som følger av lovverket. Alle aktører i helsesektoren som er tilknyttet Norsk Helsenett er avtalerettslig forpliktet til å følge Normen.

Normen har vært et nyttig verktøy for Tannhelse Rogaland i arbeidet med informasjonssikkerhet. Vi opplever at det er god internkontroll på området, noe som også skyldes kontinuerlig og systematisk oppfølging fra systemansvarlig sin side.

Tannhelse Rogaland har ikke opprettet personvernombud, og med vår organisering har vi heller ikke oppfattet at ombudet i RFK skal ivareta foretaket.

Det er for øvrig sendt melding til Datatilsynet som meldeplikten tilsier, hvert 3. år, sist gang 28.11.2011.

Pkt 1.2.10 om sikring av konfidensialitet:
Foretaket vil følge opp det som fremkommer om dokumenter som ikke er offentliggjort.

RAPPORTEN

1.1 INNLEDNING

1.1.1 FORMÅL OG PROBLEMSTILLINGER

I dette prosjektet har vi sett nærmere på om Rogaland fylkeskommune legger til rette for informasjonssikkerhet på en tilfredsstillende måte. I prosjektet har vi vurdert fylkeskommunens systemer og rutiner for informasjonssikkerhet, avgrenset til elektronisk behandling av sensitive personopplysninger.

Mandatet for gjennomføring av prosjektet ble vedtatt av kontrollutvalget i møte 04.09.2012. I tillegg til formålet, framgår det av kontrollutvalgets bestilling at følgende problemstillinger skal besvares:

- Hvilke systemer og rutiner har kommunen for å ivareta krav til informasjonssikkerhet ved elektronisk behandling av sensitive personopplysninger?
- I hvilken grad etterlever kommunen kravene til informasjonssikkerhet?
- Blir krav til arkivering og offentliggjøring ivaretatt og har de ansatte kjennskap til regelverket?
- Hvilke korrigerende tiltak bør eventuelt iverksettes for å sikre tilfredsstillende informasjonssikkerhet?

I 2005 gjennomførte Rogaland Revisjon et tilsvarende prosjekt innenfor forvaltningsrevisjon. Revisjonen kom da med følgende anbefalinger:

- *Fylkeskommunen bør snarest mulig og senest innen årets utgang, gjennomføre de kontroller som fylkeskommunen er pålagt å gjennomføre årlig, i henhold til eget regelverk og personopplysningsloven.*

- *Fylkeskommunen bør videre vurdere å øke oppmerksomheten rundt sikkerhetsarbeidet ved organisasjonsmessig å forankre sikkerhetsarbeidet i ledelsesgruppen.*

Revisjonens rapport i 2005 påpekte at det ikke var utført dokumenterte, årlige ledelsesgjennomganger, risikovurderinger og sikkerhetsrevisjoner.

1.1.2 HVA ER SENSITIVE PERSONOPPLYSNINGER?

Hva som regnes som sensitive personopplysninger, er beskrevet i personopplysningsloven. Følgende opplysninger er regnet som sensitive:

- Rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning

- At en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling
- Helseforhold
- Seksuelle forhold
- Medlemskap i fagforeninger

De sensitive personopplysningene ses på som mer inngripende for den enkelte, og regelverket stiller derfor ekstra strenge krav til behandling av disse. Med behandling menes enhver bruk av personopplysninger, eksempelvis innsamling, registrering, sammenstilling, lagring og utlevering, jf. personopplysningsloven § 2 nr 2. Misbruk eller spredning av sensitive personopplysninger kan få store konsekvenser for den enkelte som blir rammet, og det er derfor behov for ekstra sikring av slike opplysninger.

Opplysningene skal beskyttes med hensyn til:

- **Konfidensialitet**: Uvedkommende (interne og eksterne) skal ikke få *tilgang* på opplysningene.
- **Integritet**: Opplysningene skal ikke *endres* uten at dette er tilsiktet og gjøres av rettmessige brukere,
- **Tilgjengelighet**: Opplysningene skal være *tilgjengelige* for autoriserte brukere ved behov.

1.1.3 REVISJONSKRITERIER OG METODE

Revisjonskriteriene er elementer som inneholder krav eller forventninger, og vil bli brukt til å vurdere funnene i de undersøkelser som gjennomføres. Kriteriene skal være begrunnet i, eller utledet av, autoritative kilder innenfor det reviderte området. I prosjektet er følgende kilder vektlagt ved utarbeidelsen av revisjonskriteriene:

- Krav til informasjonssikkerhet i personopplysningsloven med forskrift
- Datatilsynets føringer og veiledere for informasjonssikkerhet
- Håndbok for informasjonssikkerhet i Rogaland fylkeskommune
- IKT og informasjonssikkerhet. Tannhelse Rogaland FKF
- Helsedirektoratets «Norm for informasjonssikkerhet i helse-, omsorgs- og sosialsektoren» (NORMEN).
- Reglement for bruk av RFK sine datasystemer
- Rogaland fylkeskommune sin IKT-strategi

Metodisk er det benyttet intervju og dokumentgransking. Kun *elektronisk* behandling av *sensitive* personopplysninger er undersøkt. Hvordan informasjonssikkerheten er ivaretatt for opplysninger lagret i papirform, er ikke undersøkt.

De behandlingsansvarlige for de ulike fagsystemene, med unntak av behandlingsansvarlig for fagsystemet til PP-tjenesten, oppgir at personopplysningene hovedsakelig

ligger lagret elektronisk. Ved vår gjennomgang er det spurt om sikkerhetsopplegget er fulgt, men det er ikke foretatt noen detaljkontroll.

Tannhelse Rogaland er et fylkeskommunalt foretak (FKF), som er direkte underlagt Fylkestinget. Foretakets styre og daglig leders (fylkestannlegens) myndighet er regulert i kommuneloven. Fylkestannlegen er underlagt styret, ikke fylkesrådmannen. Ansvaret for gjennomføring av internkontroll knyttet til elektronisk behandling av sensitive personopplysninger ligger derfor hos fylkestannlegen.

I rapporten revideres ikke foretaket opp mot rutinene i "Rogaland fylkeskommunes håndbok for informasjonssikkerhet" (2008), men opp mot Normen og egne rutiner beskrevet i dokumentet "IKT og informasjonssikkerhet" (2012).

En nærmere omtale av kriterier, metode og kildehenvisninger ligger i rapportens vedlegg. Vår samlede vurdering er at metodebruk og kildetilfang har gitt et tilstrekkelig grunnlag til å besvare de problemstillinger kontrollutvalget vedtok, som svar på prosjektets formål.

1.2 FAKTAGJENNOMGANG OG VURDERINGER

1.2.1 KOMMUNEUNDERSØKELSEN 2010-2011

Fylkeskommunen står nær den enkelte borger som leverandør av velferdstjenester som skole, tannlege eller hjelp til sysselsetting gjennom Oppfølgingstjenesten. Arbeidet medfører at sensitiv informasjon om den enkelte bruker blir lagret hos fylkeskommunen. Å sikre at sensitive personopplysninger ikke kommer på avveie, er viktig for fylkeskommunens omdømme og publikums tillit.

Våren 2010 iverksatte Datatilsynet en systematisk kartlegging av norske kommuners etterlevelse av personopplysningsloven. Tilsynet tok utgangspunkt i kommunenes plikt til internkontroll. En tilfredsstillende internkontroll innebærer at kommunen har:

- Utarbeidet en samlet oversikt over hvilke personopplysninger kommunen behandler.
- Det rettslige grunnlaget er klarlagt, det vil si at kommunen har kontrollert hvorvidt de har hjemmel i lov, samtykke fra den registrerte[1] eller kan påvise et annet rettslig grunnlag for behandlingen.
- Kommunen har klarlagt ansvars- og myndighetsforhold.
- Ved endringer har kommunen gjennomført risikovurderinger som dokumenterer fortsatt forsvarlig håndtering av personopplysninger.
- Rutiner for å sikre den registrerte lovfestede rettigheter er utarbeidet.
- Et fungerende system for avvikshåndtering er etablert.

Formålet med de ovenfor nevnte tiltakene er å styre aktiviteten i virksomheten slik at driften skjer i overensstemmelse med gjeldende lover og regler og god informasjonssikkerhet oppnås. Kommunen skal ha en viss systematikk i arbeidet med å etterleve regelverket og internkontrollen skal være dokumentert, jf. personopplysningsloven § 13.

I Datatilsynets undersøkelse svarte kun 52 prosent av landets fylkeskommuner og kommuner «ja» på spørsmålet om hvorvidt kommunen har etablert en dokumentert internkontroll.

Den reelle prosentandelen var imidlertid langt lavere. Ved kontroll av kommunenes besvarelser mot *alle* de seks ovenfor nevnte kravene, falt andelen som hadde etablert en tilfredsstillende internkontroll til rundt 7 prosent. Datatilsynet skriver følgende om resultatet fra undersøkelsen:

[1] Den registrerte er her den person som fylkeskommunen har opplysninger om.

«Resultatet er spesielt nedslående sett i lys av den vedvarende satsningen tilsynet har hatt overfor kommunene. Etter tilsynets vurdering reiser resultatet spørsmålet om regelverkets hensiktsmessighet. Det er et kraftig signal til regelverksutvikler at en stor gruppe innenfor regelverkets virkeområde ikke har sett det som mulig å etterleve kravene på en adekvat måte. Dette kan ikke alene tilskrives motvilje, men reelle utfordringer som kommunen står ovenfor. Resultatene vil således spilles inn i pågående regelverksprosess. (…) Er rettsreglene som kommunene stilles ovenfor rimelige? Bør det vurderes forenklinger?».

Videre heter det at: «Mange kommuner ønsker klarere regler for hvordan ting skal gjøres, i motsetning til selv å velge løsninger hvor de selv må dokumentere forholdsmessig sikkerhet (…) Kartleggingen synliggjør behov for en fortsatt betydelig innsats mot kommunene. Av de virkemidlene Datatilsynet har til disposisjon, synes en kombinasjon av veiledning, kontroll og eventuell bruk av sanksjoner som en mulig løsning».

1.2.2 HVOR FOREKOMMER ELEKTRONISK BEHANDLING AV SENSITIVE PERSONOPPLYSNINGER?

Fylkeskommunen har utarbeidet en oversikt over hvilke datasystemer som inneholder personopplysninger, herunder også sensitive personopplysninger. Ut fra denne oversikten har vi plukket ut de fire fagsystemene som inneholder sensitive personopplysninger:

- ESA – Sak- og arkivsystem for bruk i hele fylkeskommunen.
- PPI – Klientsystem for bruk i PP-tjenesten.
- OTTO – Klientsystem for bruk i Oppfølgingstjenesten
- OPUS – Elektronisk pasientjournalsystem for bruk i Tannhelse Rogaland FKF

ESA er et felles sak- og arkivsystem som brukes på tvers av fylkeskommunens ulike avdelinger og seksjoner. De andre tre datasystemene er lukkede systemer som kun brukes av ansatte i PP-tjenesten (PPI), Oppfølgingstjenesten (OTTO) og tannhelsetjenesten (OPUS). Det faktum at dette er lukkede systemer, innebærer at det ikke er mulig å logge seg inn i disse systemene via Internett. Alle systemene er knyttet opp mot en sentral serverløsning. Dette innebærer at all lagring og backup av sensitive personopplysninger skjer sentralt ved IKT- og arkivseksjonen i sentraladministrasjonen.

Det er kun disse fire datasystemene som inneholder sensitive personopplysninger.

1.2.3 PERSONVERNOMBUD

Personopplysningsloven § 31 gir virksomheter som behandler personopplysninger en meldeplikt til Datatilsynet. Meldingen skal opplyse om:

- Navn og adresse på den behandlingsansvarlige.
- Når behandlingen starter.
- Hvem som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter, og formålet med behandlingen.
- Oversikt over hvilke typer personopplysninger som behandles.
- Hvor personopplysningene hentes fra.
- Det rettslige grunnlaget for innsamlingen av opplysningene.
- Hvem personopplysningene vil bli utlevert til.
- Hvilke sikkerhetstiltak som er knyttet til behandlingen.

Virksomheter som oppretter personvernombud, kan få fritak fra denne meldeplikten til Datatilsynet, jf. personopplysningsforskriften § 7-12. Dersom fritak innvilges, forutsetter Datatilsynet at personvernombudet fører den ovenfor nevnte oversikten selv.

På forespørsel fra revisjonen, kan fylkeskommunen ikke dokumentere at denne oversikten er blitt utarbeidet. Fylkeskommunen valgte å opprette et personvernombud i 2008. Fra nåværende personvernombud, som tiltrådte i april 2012, får vi opplyst at en slik oversikt vil være klar i januar/ februar 2013.

Foruten å føre en oversikt over virksomhetens behandling av personopplysninger, skal personvernombudet påse at virksomheten følger personopplysningsloven. I dette ligger at personvernombudet kan foreta stikkprøve-kontroller, men ombudet har ikke ansvar for at alle lover og regler for behandling av personopplysningene faktisk blir fulgt. Dette ansvaret ligger på ledelsen. Intervjusvarene peker imidlertid i retning av at det har hersket noe uklarhet omkring ombudets rolle, ansvar og oppgaver så lenge ordningen har eksistert i Rogaland fylkeskommune.

I det følgende vil vi presentere våre funn med hensyn til hvorvidt fylkeskommunen følger personopplysningsloven:

1.2.4 SIKKERHETSLEDELSE

Personopplysningsforskriften § 2-3:
"Den som har den daglige ledelsen av virksomheten som den behandlingsansvarlige driver, har ansvar for at bestemmelsene i dette kapittelet følges. Formålet med behandling av personopplysninger og overordnede føringer for bruk av informasjonsteknologi, skal beskrives i sikkerhetsmål. Valg og prioriteringer i sikkerhetsarbeidet skal beskrives i en sikkerhetsstrategi.

Bruk av informasjonssystemet skal jevnlig gjennomgås for å klarlegge om den er hensiktsmessig i forhold til virksomhetens behov, og om sikkerhetsstrategien gir tilfredsstillende informasjonssikkerhet som resultat. Resultatet fra gjennomgangen skal dokumenteres og benyttes som grunnlag for eventuell endring av sikkerhetsmål og strategi."

Fylkesrådmannen er øverste ansvarlig for at de sensitive personopplysningene som behandles, er tilfredsstillende sikret. Avdelingsdirektørene, seksjonslederne og rektorene er gjennom linjen gitt ansvar for de datasystem de benytter.

Overordnede beslutninger om *hva* informasjonsteknologien skal brukes til og *hvordan* teknologien skal benyttes i virksomheten, kalles sikkerhetsmål. Med sikkerhetsstrategi menes de valg og prioriteringer som virksomheten har gjort for å *sikre* opplysningene som ligger lagret.[2]

I henhold til *Datatilsynets veileder for internkontroll og informasjonssikkerhet*, skal ledelsen årlig gjennomgå sikkerhetsmål, sikkerhetsstrategi og organisering av informasjonssystemene; «Ledelsen skal kontrollere at disse er i samsvar med virksomhetens behov og eventuelt oppdaterte mål, strategi og organisering».

I ledelsens gjennomgang av informasjonssystemene skal blant annet følgende vurderes:

- Resultater fra sikkerhetsrevisjoner og kontroller utført av offentlig myndighet.
- Endringer med betydning for drift av informasjonssystemet eller for informasjonssikkerheten, herunder:
    - Endringer i offentlige sikkerhetskrav
    - Endringer i de personopplysninger virksomheten skal behandle
    - Endringer i trusselbildet som blant annet beskrevet i rapport fra utførte risikovurderinger
- Om informasjonssystemet bør endres, eksempelvis som følge av ønske om ny funksjonalitet.
- Overordnet behandling av alvorlige avvik og hendelser.

I henhold til Rogaland fylkeskommune sin egen håndbok for informasjonssikkerhet, skal ledelsen i fylkeskommunen ha en årlig gjennomgang av sikkerhetsmål, strategi og organisering. Dette for å kontrollere at informasjonssystemet er i samsvar med fylkeskommunens behov.

Vi finner at fylkeskommunen ikke har hatt slike årlige gjennomganger av sikkerhetsmål, strategi og organisering av informasjonssystemet. Siden utarbeidelsen av informasjonssikkerhetshåndboka i 2008, er det ikke foretatt noen systematisk gjennomgang av

[2] Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer, Datatilsynet 2000.

sikkerhetsmål, strategi og organisering av informasjonssystemet i rådmannens ledergruppe, som tilfredsstiller forskriftens krav.

Direktør for administrasjonsavdelingen har tatt opp ulike spørsmål om informasjonssikkerhet i sine ledermøter, men gjennomgangene kan ikke sies å tilfredsstille forskriftens krav. For øvrig dekker ikke administrasjonsavdelingens ledergruppe hele fylkeskommunens virksomhet (Organisasjonskart er gjengitt i rapportens vedleggsdel).

Tannhelse Rogaland har på sin side hatt årlige gjennomganger av sikkerhetsmål, strategi og organisering, i tråd med Helsedirektoratets «Norm for informasjonssikkerhet i helse-, omsorgs- og sosialsektoren».

Vurdering: Både personopplysningsforskriften og fylkeskommunens egen håndbok for informasjonssikkerhet, slår fast at en årlig gjennomgang av sikkerhetsmål, strategi og organisering av informasjonssystemet er påkrevet. Dette kravet er ikke blitt oppfylt i fylkeskommunen, med unntak av Tannhelse Rogaland sine årlige gjennomganger.

1.2.5 RISIKOVURDERING

Personopplysningsforskriften § 2-4:
"Det skal føres oversikt over hva slags personopplysninger som behandles. Virksomheten skal selv fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger. Den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten.

Resultatet av risikovurderingen skal sammenlignes med de fastlagte kriterier for akseptabel risiko forbundet med behandling av personopplysninger, jf. første ledd og § 2-2. Resultatet av risikovurderingen skal dokumenteres."

Risiko betegner forholdet mellom sannsynlighet for at en uønsket hendelse vil inntreffe og konsekvenser av en slik hendelse. Formålet med en risikovurdering er å sikre at den risiko som avdekkes, er innenfor de akseptkriterier virksomheten har fastlagt. Med akseptkriterier menes holdepunkter for hva som anses akseptabelt. Eksempler:

- Det vil ikke være akseptabelt at personer utenfor virksomheten får tilgang til opplysningene.
- Det vil ikke være akseptabelt at medarbeidere snoker i opplysninger som ikke er relevante for deres arbeidsoppgaver.

Ut fra disse akseptkriteriene kan man utlede hvilke tiltak som er nødvendige for å komme innenfor akseptabel risiko. Risikovurderingen danner grunnlag for iverkset-

ting av nødvendige sikkerhetstiltak, og skal være en del av ledelsens gjennomgang av informasjonssikkerheten, jf. Datatilsynets *Veiledning om internkontroll og informasjonssikkerhet* (2009).

Personopplysningsforskriften § 2-4 krever at det gjennomføres risikovurderinger ved endringer som kan påvirke informasjonssikkerheten, for eksempel når datasystemene endres eller når det oppstår endringer i trusselbildet. Eksempler på endringer som krever ny risikovurdering:

- endring i klassifisering av opplysninger
- endringer i trusselbildet
- organisasjonsendringer
- endret tilkopling til sikret sone
- endret tilkopling til eksterne datanett
- ekstern overføring av nye typer opplysninger eller til nye partnere

Personopplysningsforskriften § 2-4 stiller ikke bare krav om gjennomføring av risikovurderinger ved endringer i det aktuelle datasystem. Også ved hendelser som den behandlingsansvarlige ikke har herredømme over, eksempelvis endringer i trusselbildet, feil i standard programvare eller lignende, skal en risikovurdering gjennomføres[3]. Videre kan behov oppstå over tid ved at enkeltendringer av datasystemene i sum blir store.

Datatilsynets *Veileder om internkontroll og informasjonssikkerhet* stiller krav om at «Ledergruppen i virksomheten, med tillegg av IT-driftsansvarlig og sikkerhetsansvarlig, skal minst én gang årlig gjennomføre risikovurdering bl.a. i forbindelse med vurdering av endringer i trusselbildet og/eller planlagte endringer i informasjonssystemet».

Eksempler på elementer som inngår i en risikovurdering:

- Beskrivelse av trusler mot informasjonssikkerheten med hensyn til konfidensialitet, integritet og tilgjengelighet.
- Årsaksanalyse – vurdering av hvordan en uønsket hendelse kan inntreffe.
- Konsekvensanalyse – vurdering av de følger en uønsket hendelse kan medføre.
- Frekvensanalyse – vurdering av sannsynlighet for at en uønsket hendelse kan inntreffe.
- Vurdering av hvorvidt den avdekkede risiko er innenfor akseptkriteriene.
- Vurdering av sikkerhetstiltak.

Krav om årlige risikovurderinger følger også av fylkeskommunens håndbok for informasjonssikkerhet, jf. punkt 2.4.1 og 2.6.1. Håndboken slår fast at «risikovurderingen skal følges opp med en tiltaksliste, ansvar for de ulike tiltakene og tidsrammer for gjennomføring av tiltak». Behandlingsansvarlig, det være seg den enkelte seksjonsle-

[3] Veiledning om internkontroll og informasjonssikkerhet, Datatilsynet 2009 og Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer, Datatilsynet 2000.

der/ enhetsleder, er gitt ansvaret for at risikoanalyser blir gjennomført for sitt datasystem.

Tannhelse Rogaland har gjennomført flere risikovurderinger i tilknytning til sitt elektroniske pasientjournalsystem, OPUS. I forbindelse med innføringen av Norsk helsenett, et elektronisk system for samhandling i helse-, omsorgs- og sosialsektoren, har Tannhelse Rogaland avtalerettslig forpliktet seg til å følge Helsedirektoratets «Norm for informasjonssikkerhet i helsesektoren». Denne normen gir klare føringer og er utarbeidet i forbindelse med innføringen av det nye elektroniske systemet.

For PP-tjenestens klientsystem (PPI) og klientsystemet til Oppfølgingstjenesten (OTTO) er det ikke gjennomført risikovurderinger de siste fire år. Problemstillinger som har dukket opp har i stedet blitt diskutert og løst fortløpende, men det foreligger ingen dokumentasjon på at det er gjennomført noen risikoanalyser.

Til det overordnede sak- og arkivsystemet (ESA) er det utarbeidet en risikoanalyse i forbindelse med utviklingen av en ny overordnet beredskapsplan. En risikovurdering i forbindelse med saksbehandling i elevsaker er også gjennomført.

Vurdering: Datatilsynets *Veileder om internkontroll og informasjonssikkerhet* stiller krav om gjennomføring av risikovurderinger minst én gang årlig. Krav om årlige risikovurderinger følger også av Rogaland fylkeskommune sin håndbok for informasjonssikkerhet.

For PP-tjenestens klientsystem (PPI) og klientsystemet til Oppfølgingstjenesten (OTTO) er det ikke gjennomført risikovurderinger de siste fire år. Til det overordnede sak- og arkivsystemet (ESA) er det utarbeidet en risikoanalyse i forbindelse med utviklingen av en ny overordnet beredskapsplan. En risikovurdering i forbindelse med saksbehandling av elevsaker er også gjennomført.

Tannhelse Rogaland har gjennomført flere risikovurderinger i tråd med Helsedirektoratets «Norm for informasjonssikkerhet i helsesektoren».

1.2.6 SIKKERHETSREVISJON

Personopplysningsforskriften § 2-5:
"Sikkerhetsrevisjon av bruk av informasjonssystemet skal gjennomføres jevnlig. Sikkerhetsrevisjon skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører. Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemet som ikke er forutsatt, skal dette behandles som avvik, jf. § 2-6. Resultatet fra sikkerhetsrevisjon skal dokumenteres."

Bestemmelsen pålegger den behandlingsansvarlige å foreta jevnlige kontroller for å sjekke at de sikkerhetstiltak som er besluttet etablert, faktisk er iverksatt og fungerer etter sin hensikt. Ved sikkerhetsrevisjon sammenlignes faktisk bruk av informasjonssystemet med de retningslinjer for slik bruk som er besluttet.[4]

Under punkt 2.6.1 om "egenkontroll" i håndboken har fylkeskommunen bestemmelser knyttet til sikkerhetsrevisjon. Her heter det at egenkontroller skal gjennomføres slik at alle deler av virksomheten kontrolleres innenfor et 12 måneders intervall. Det er virksomhetens ledelse som har ansvaret for at egenkontroller iverksettes. Formålet med egenkontrollen er å sikre at besluttet sikkerhetsmål, -strategi og organisering etterleves i hele virksomheten. Ved gjennomføringen av kontrollen skal blant annet følgende elementer gjennomgås:

- Ansvars- og myndighetsforhold.
- Ledelsen og ansattes kompetanse, samt etterlevelse av sikkerhetstiltak.
- Avviksrapportering og generell bruk av kvalitetssystem for informasjonssikkerhet.
- Gjennomgang av avvik registrert siden forrige kontroll.

I Tannhelse Rogaland er det blitt gjennomført årlige sikkerhetsrevisjoner i tråd med forskriftens krav. Gjennom de årlige sikkerhetsrevisjonene gjennomgås sikkerheten på hver enkelt tannklinikk. Ansvars- og myndighetsforhold blir også gjennomgått, deriblant et organisasjonskart som viser hvem som har tilgang til hva.

For PP-tjenestens klientsystem (PPI) og Oppfølgingstjenestens klientsystem (OTTO), er det ikke gjennomført sikkerhetsrevisjoner i tråd med forskriftens krav de siste fire år. For fylkeskommunens overordnede sak- og arkivsystem (ESA) er det gjennomført en sikkerhetsrevisjon, avgrenset til å gjelde behandling av elevsaker.

Vurdering: Ved sikkerhetsrevisjon sammenlignes faktisk bruk av informasjonssystemet med de retningslinjer for slik bruk som er besluttet. Med noen få unntak, er det ikke gjennomført årlige sikkerhetsrevisjoner, det vil si sammenligninger av faktisk bruk av informasjonssystemet mot de retningslinjer som er besluttet. Dette til tross for at fylkeskommunens håndbok for informasjonssikkerhet slår fast at «egenkontroller skal gjennomføres slik at alle deler av virksomheten kontrolleres innenfor et 12 måneders intervall».

1.2.7 Avvik

Personopplysningsforskriften § 2-6:

[4] Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer, Datatilsynet 2000.

"Bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd, skal behandles som avvik. Avviksbehandlingen skal ha som formål å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentagelse. Dersom avviket har medført uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig, skal Datatilsynet varsles. Resultatet fra avviksbehandling skal dokumenteres."

Dersom personopplysninger håndteres i strid med fastlagte rutiner, eller det er mistanke om eller dokumentert brudd på informasjonssikkerhet, skal virksomheten iverksette avviksbehandling. Formålet med avviksbehandling er å lukke avviket så raskt som mulig, gjenopprette normaltilstand og hindre gjentagelse.

Avviksbehandling skal dokumenteres i en rapport som inneholder opplysninger om selve avviket, gjennomførte strakstiltak, iverksatte korrigerende tiltak, resultater fra evaluering av de korrigerende tiltakenes effekt over tid, samt opplysninger om hvilke medarbeidere som har vært involvert i behandlingen av avviket[5].

I henhold til håndboken punkt 3.5.1 skal eventuelle avvik registreres ved bruk av fylkeskommunens skjema for avvik. Etter registering skal det iverksettes strakstiltak. Og etter noe tid, skal den som er utpekt som ansvarlig, vurdere hvorvidt tiltakene fungerer etter sin hensikt.

Leder for IKT- og arkivseksjonen oppgir at det ikke er meldt inn noen avvik. Det samme oppgir de systemansvarlige for det enkelte fagsystem. De ansvarlige svarer at de ikke har hatt noen tilfeller av alvorlige avvik, og at avviksskjemaet dermed ikke er blitt benyttet.

Tannhelse Rogaland oppgir imidlertid at de har meldt avvik på andre måter enn ved bruk av avviksskjemaet. I forbindelse med årlig sikkerhetsrevisjon meldes det inn avvik fra tannklinikkene og fylkestannlegekontoret som samles i egen rapport. Nærmeste leder er ansvarlig for oppfølging. Forhold rundt saksbehandling i ESA inngår i revisjonen for de som er brukere av det systemet. Ved implementering av «QM+», som er fylkeskommunens nye, felles, elektroniske avvikssystem, er intensjonen å få til en mer fortløpende registering og oppfølging av avvik. Målet er også å få bedre rutiner på melding av avvik som skal følges opp av IKT- og arkivseksjonen.

Alle rutiner og håndbøker skal etter planen legges inn i det nye avvikssystemet, slik at disse er samlet på ett sted. Fylkeskommunen har nylig lansert plandokumentet «*Strategi for sikkerhets- og kvalitetskultur i Rogaland fylkeskommune*», for å sikre «en kultur der systematisk sikkerhets- og kvalitetsarbeid ligger i ryggmargen til alle ledere og medarbeidere», som det heter i plandokumentet. I forbindelse av lanseringen inngår ulike aktiviteter som skal bidra til at terskelen for å melde avvik reduseres.

[5] Datatilsynets veileder om internkontroll og informasjonssikkerhet.

Vurdering: Fylkeskommunens håndbok for informasjonssikkerhet stiller krav om bruk av fylkeskommunens skjema ved registering av avvik. Verken leder IKT- og arkivseksjonen eller de ansvarlige for det enkelte fagsystem, har registrert noen avvik. Avviksskjemaet har dermed ikke blitt benyttet. Når det i slike avvikssystem ikke blir registrert noen avvik, er det grunn til å vurdere om systemet fungerer etter hensikten.

Et nytt elektronisk avvikssystem er implementert i sentraladministrasjonen og vil være på plass på skolene ved nyåret. Utfordringen blir å få de ansatte til å bruke avvikssystemet i praksis.

1.2.8 ORGANISERING

Personopplysningsforskriften § 2-7:
"Det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemet. Ansvars- og myndighetsforhold skal dokumenteres og ikke endres uten autorisasjon fra den behandlingsansvarliges daglige leder. Informasjonssystemet skal konfigureres slik at tilfredsstillende informasjonssikkerhet oppnås.

Konfigurasjonen skal dokumenteres og ikke endres uten autorisasjon fra den behandlingsansvarliges daglige leder. Bruk av informasjonssystemet som har betydning for informasjonssikkerheten, skal utføres i henhold til fastlagte rutiner."

Med konfigurasjon menes informasjonssystemets utforming, det vil si utstyr og program, samt sammenkoblinger mellom disse. Ved valg av konfigurasjon skal virksomhetens behov for informasjonssikkerhet tillegges vekt, i tillegg til vurdering av økonomi og behov for funksjonalitet. En slik vurdering vil kunne omfatte etablering av sikkerhetsbarrierer, bruk av nettverkssegmentering for å skille forskjellige behandlinger av personopplysninger fra hverandre i informasjonssystemet og lignende.

Virksomheten skal konfigurere informasjonssystemet slik at tilfredsstillende informasjonssikkerhet oppnås i henhold til risikovurderinger og beslutninger om sikkerhetstiltak. Konfigurasjonen skal dokumenteres i en oversikt, eksempelvis i form av konfigurasjonskart, som angir:

- Koblinger mellom utstyr og program.
- Inndeling av informasjonssystemet i soner.
- Kommunikasjonspunkt for tilkobling til ekstern dataoverføring.
- Navn eller modellbetegnelse, og serienummer eller versjonsnummer på sikkerhetsutstyr/-programmer.
- Sikkerhetsfunksjoner med opplysninger om oppsett/innstilling av utstyr/program.
- Når sikkerhetsutstyret ble tatt i bruk, eller når utstyret ble tatt ut av bruk.
- Opplysninger om vedlikehold, skade, funksjonsfeil og reparasjoner.

Håndboken angir hvilken systemteknisk løsning fylkeskommunen har valgt. Fylkeskommunen har et system bygget opp som et internt nettverk med sikre soner. Sensitive personopplysninger er lagret i en ekstra sikker sone, kalt «sensitiv sone», slik at uvedkommende ikke skal få tilgang. Denne sonen har ingen forbindelse med fylkeskommunens intranett og har ingen tilgang mot Internett. Sensitive personopplysninger skal kun behandles i sensitiv sone. Fylkeskommunen har utarbeidet et kart som viser hvordan informasjonssystemet er satt opp.

I fylkeskommunens håndbok, punkt 2.1.1, heter det at: «Selv om fylkeskommunen juridisk betraktes som én virksomhet, har vi av organisatoriske og sikkerhetsmessige hensyn valgt å dele fylkeskommunen inn i flere enheter som hver gis et selvstendig ansvar for egen informasjonssikkerhet (…) Seksjonssjefene er ansvarlige for informasjonssikkerheten innenfor hver seksjon. Rektorene er ansvarlige for sin skole. Fylkesrådmannen har det overordnede ansvar for at fylkeskommunens datasystemer og databaser er tilfredsstillende ivaretatt».

I fylkeskommunens håndbok punkt 3.1.1 skisseres hvilke roller som er gitt ansvar når det gjelder å ivareta fylkeskommunens informasjonssikkerhet:

- Fylkesrådmannen
- Informasjonssikkerhetsstyret (rådmannens ledergruppe)
- Informasjonssikkerhetsleder som har det daglige praktiske arbeidet med å følge opp informasjonssikkerhetsstyrets instrukser.
- Avdelingene, seksjonene og skolene har gjennom linjen informasjonssikkerhetsansvar for sin enhet.

Ut fra de tilbakemeldingene revisjonen har fått i intervjuene av de behandlingsansvarlige for fagsystemene PPI (PP-tjenesten), OTTO (Oppfølgingstjenesten) og ESA (sak- og arkivsystemet), synes kunnskapen om hvilke oppgaver og plikter den enkelte behandlingsansvarlige har, å være noe mangelfull. Alle respondentene med lederansvar er kjent med at de faktisk har et ansvar, men kunnskapen om hva ansvaret innebærer av plikter og oppgaver, er ikke tilstrekkelig.

Fylkeskommunen har utarbeidet en oversikt over hvilke datasystemer som inneholder personopplysninger, herunder også sensitive personopplysninger. Oversikten viser hvilke typer opplysninger systemet inneholder og hvilken enhet, avdeling eller seksjon som er ansvarlig eier.

Vurdering: Alle respondentene med lederansvar er kjent med at de faktisk har et ansvar, men kunnskapen om hva ansvaret innebærer av plikter og oppgaver, synes i noen tilfeller å være noe mangelfull.

Informasjonssystemets utforming, det vil si utstyr og program, samt sammenkoblinger mellom disse, er dokumentert i et konfigurasjonskart.

1.2.9 PERSONELL OG TAUSHETSPLIKT

Personopplysningsforskriften §§ 2-8, 2-9
"Medarbeidere hos den behandlingsansvarlige skal bare bruke informasjonssystemet til å utføre pålagte oppgaver, og selv være autorisert for slik bruk. Medarbeiderne skal ha nødvendig kunnskap for å bruke informasjonssystemet i samsvar med de rutiner som er fastlagt.

Autorisert bruk av informasjonssystemet skal registreres. Medarbeidere hos den behandlingsansvarlige skal pålegges taushetsplikt for personopplysninger hvor konfidensialitet er nødvendig. Taushetsplikten skal også omfatte annen informasjon med betydning for informasjonssikkerheten."

Virksomheten er pålagt å logge autorisert bruk og forsøk på uautorisert bruk av informasjonssystemet i henhold til personopplysningsforskriften:

- Autorisert bruk av informasjonssystemet skal registreres.
- Forsøk på uautorisert bruk av informasjonssystemet skal registreres.

Hensikten med logging av autorisert bruk er å i ettertid kunne spore hvem som gjorde hva med hvilke personopplysninger, og på hvilket tidspunkt.

Medarbeidere som har tilgang til sensitive personopplysninger, eller til informasjon om sikring av slike opplysninger, skal ha taushetsplikt og undertegne taushetserklæring. Taushetserklæringer brukes for å gjøre oppmerksom på at det forekommer konfidensiell informasjon i virksomheten. De ansatte skal undertegne en slik erklæring samtidig med ansettelseskontrakten. Taushetserklæringer bør gjennomgås på nytt når ansettelsesforholdet endres, særlig når ansatte skal forlate organisasjonen, eller kontrakter løper ut, jf. *Datatilsynets veiledning om internkontroll og informasjonssikkerhet*.

I henhold til Rogaland fylkeskommune sin håndbok for informasjonssikkerhet, må alle ansatte skrive under på en taushetserklæring ved starten av ansettelsesforholdet. Den ansattes nærmeste leder er ansvarlig for å informere om forhold rundt taushetsplikten. Hvert år foretar revisjonen stikkprøvekontroller på tilfeldig utvalgte, videregående skoler. Av 89 kontrollerte i perioden 2010 – 2012, manglet underskrevet taushetserklæring i 4 tilfeller. Dette gir en feilmargin på 4,5 prosent.

Som autorisert helsepersonell er det fleste ansatte i Tannhelse Rogaland pålagt taushetsplikt etter helsepersonell-lovens § 21. Den enkeltes arbeidsavtale inneholder en presisering om at det etter straffelovens § 121 er straffbart å bryte taushetsplikten.

Informasjonssystemet har tilgangskontroll til nettverket og fagsystemene, noe som sikrer at de som til enhver tid har tilgang, er autoriserte brukere. Kun brukere som er autoriserte til de ulike sonene, skal ha tilgang og tilgangen er regulert utfra hvilke arbeidsoppgaver den enkelte ansatte er satt til å utføre. All tilgang blir automatisk loggført. Håndboken slår fast at det skal «etableres rutiner for gjennomgang av hendelsesregistre». Slike rutiner er imidlertid ikke blitt etablert.

Revisjonen får opplyst at tildeling av tilganger alltid går via leder. En ansatt i fylkeskommunen har ikke anledning til å ringe IKT-avdelingen selv. Dette for å sikre at uvedkommende ikke får adgang til det enkelte fagsystem og den enkelte sone. Den enkelte leder er også gitt ansvar for å melde ut ansatte som flytter internt eller slutter i fylkeskommunen.

En ansatt i fylkeskommunen som ønsker tilgang til sensitive personopplysninger, må gjennom flere innlogginger før han/hun kommer inn til opplysningene. Tilgang til de sensitive personopplysningene krever med andre ord at man husker ulike sett med brukernavn og passord.

Systemet er satt opp med en ytre brannmur mot internett og en indre brannmur mot sikker sone. Alt som blir stoppet i brannmuren blir logget. Brannmurens logg brukes til feilsøking dersom noen har problemer med å få tilgang, og loggen sjekkes med jevne mellomrom av IKT- og arkivseksjonen.

Ingen av respondentene har registrert tilfeller av ulovlig utlevering av sensitive personopplysninger. Formelle henvendelser, eksempelvis fra barnevern eller politi, om utlevering av opplysninger, går via Dokumentsenteret, som krever samtykke fra ansvarlig saksbehandler.

Vurdering: Håndboken går et skritt lenger enn personopplysningsforskriften og slår fast at det skal «etableres rutiner for gjennomgang av hendelsesregistre». Slike rutiner er imidlertid ikke blitt etablert. Imidlertid foretas noe kontroll, eksempelvis av hva som blir stoppet i brannmuren. Informasjonssystemet har dessuten tilgangskontroll til nettverket og fagsystemene, noe som sikrer at de som til enhver tid har tilgang, er autoriserte brukere.

Tildeling av tilganger går alltid via leder. Alle ansatte må skrive under på en taushetserklæring ved starten av ansettelsesforholdet. Den ansattes nærmeste leder er ansvarlig for å informere om hva taushetsplikten innebærer.

Samlet sett fremstår tiltakene som tilfredsstillende, men manglende taushetserklæringer i 4,5 prosent av kontrollerte ansettelsesforhold, viser at fylkeskommunen kan bli flinkere til å innhente taushetserklæringer.

1.2.10 SIKRING AV KONFIDENSIALITET

Personopplysningsforskriften § 2-11:
"Det skal treffes tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig. Sikkerhetstiltakene skal også hindre uautorisert innsyn i annen informasjon med betydning for informasjonssikkerheten. Personopplysninger som overføres elektronisk ved hjelp av overføringsmedium utenfor den behandlingsansvarliges fysiske kontroll, skal krypteres eller sikres på annen måte når konfidensialitet er nødvendig.

For lagringsmedium som inneholder personopplysninger hvor konfidensialitet er nødvendig, skal behovet for sikring av konfidensialitet fremgå ved hjelp av merking eller på annen måte. Dersom lagringsmediet ikke lenger benyttes for behandling av slike opplysninger, skal opplysningene slettes fra lagringsmediet."

Konfidensialitet handler om å hindre at uvedkommende får tilgang til sensitive personopplysninger. Håndboken tar ikke opp spørsmålet om bruk av epost, men revisjonen får opplyst fra de behandlingsansvarlige, at de har informert sine ansatte om at sensitive personopplysninger ikke skal sendes per epost.

Det skal i følge respondentene ikke være mulig å kopiere informasjon fra sikker sone i de ulike datasystemene og over til eksterne dataprogrammer. Den systemtekniske løsningen setter en stopper for dette. Det er dermed ikke mulig å kopiere fra sikker sone til e-post. Rogaland fylkeskommunes reglement for bruk av datasystemer slår fast at taushetsbelagte opplysninger aldri skal sendes på e-post.

Revisjonen får opplyst at det ikke lagres sensitive personopplysninger på andre typer lagringsmedium, som for eksempel minnepinner eller DVD-plater. Dette har vi ikke hatt mulighet til å kontrollere.

Elektronisk behandling av sensitive personopplysninger foregår utelukkende innenfor lukkede fagsystemer. Kun ansatte i de enkelte enhetene har tilgang og det er ikke mulig å hente ut informasjon fra systemene, med unntak av papirutskrift. For å holde orden på utskriftene, er antallet skrivere som er koblet til det enkelte fagsystem, redusert til et minimum.

Hovedregelen om sletting følger av personopplysningsloven § 28. Bestemmelsen forbyr unødvendig lagring av personopplysninger. Her heter det at «den behandlingsansvarlige skal ikke lagre personopplysninger lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. Hvis ikke personopplysningene deretter skal oppbevares i henhold til arkivloven eller annen lovgivning, skal de slettes».

De behandlingsansvarlige for de fire fagsystemene, med unntak av behandlingsansvarlig for ESA, oppgir at de har rutiner for behandling av sensitive personopplysninger som det ikke lenger er nødvendig å lagre. I PP-tjenesten overføres opplysninger til et fjernarkiv og slettes fra fagsystemet PPI. I Oppfølgingstjenestens system vil klienter

som overskrider aldersgrensen for rett til videregående opplæring, bli slettet automatisk. I Tannhelse Rogaland vil opplysninger som er lagret i mer enn ti år bli behandlet i henhold til lov om offentlig tannhelsetjeneste.

Når det gjelder sletting av sensitive personopplysninger i ESA, er dette et spørsmål som er under vurdering. Riksarkivet er i gang med en utredning som vil kunne gi noen svar i løpet av 2013. Fylkeskommunen har heller ikke tatt stilling til hvordan slettingen eventuelt skal foregå rent teknisk.

I henhold til offentlighetsloven § 3 er fylkeskommunens saksdokumenter offentlige så langt det ikke er gjort unntak i lov eller i medhold av lov. Fylkeskommunens arkivplan slår fast at det er den arkivansvarlige i hver enhet som skal sjekke gradering og skjerming av dokumentene før offentliggjøring i postlistene. Med gradering menes koding av dokumentet, som gjør det mulig for et dataprogram å skille ut hvilke dokumenter som skal legges ut. Med skjerming menes at man tar bort opplysninger i dokumentet som ikke skal offentligjøres.

Fylkesarkivaren kontrollerer arbeidet som gjøres vedrørende gradering og skjerming. Hittil har ikke fylkeskommunen registrert tilfeller hvor sensitive personopplysninger ved en feiltakelse er blitt offentliggjort i postlistene. Imidlertid finnes det et forholdsvis høyt antall dokumenter som ikke er blitt offentliggjort. Dette skyldes trolig at saksbehandleren eller arkivtjenesten i den enkelte enhet ikke har fulgt gjeldende rutiner.

Figur 1 – Prosentandel inn- og utgående dokumenter som ikke er offentliggjort i postlistene (Kilde: Rogaland fylkeskommune):

- **Rogaland kollektivtrafikk:**
  01.01.2010 til 19.12.2012: 281 av 2592 dok. (10,8 prosent)
- **De videregående skolene:**
  01.01.2010 til 03.10.2012: 813 av 60517 dok. (1,3 prosent)
- **Tannhelse Rogaland:**
  01.01.2010 til 03.10.2012: 51 av 7123 dok. (0,7 prosent)
- **Dokumentsenteret (fylkesrådmannens kontor):**
  01.01.2010 – 28.11.2012: 550 av 104 998 dok. (0,5 prosent)

Kommentar: Til sammen 1695 dokumenter er ikke blitt offentligjort i siden 01.01.2010. Oversikten viser at antallet dokumenter som ikke er blitt offentliggjort er stort.

Vurdering: De systemtekniske løsningene med lukkede nettverk hindrer uautoriserte brukere å få tilgang til sensitive personopplysninger. Begrensninger i mulighetene for å hente ut opplysninger sørger for god konfidensialitet. De behandlingsansvarlige for PPI og OTTO oppgir at de sletter opplysninger som virksomheten ikke lenger har behov for. Hvilke og hvordan sensitive personopplysninger skal slettes fra ESA, har fylkeskommunen foreløpig ikke tatt stilling til.

Siden 01.01.2010 er et uforholdsmessig høyt antall dokumenter ikke blitt offentliggjort i postlistene.

1.2.11 SIKRING AV TILGJENGELIGHET

Personopplysningsforskriften § 2-12:
"Det skal treffes tiltak for å sikre tilgang til personopplysninger hvor tilgjengelighet er nødvendig. Sikkerhetstiltakene skal også sikre tilgang til annen informasjon med betydning for informasjonssikkerheten. Alternativ behandling skal forberedes for de tilfeller informasjonssystemet er utilgjengelig for normal bruk. Personopplysninger og annen informasjon som er nødvendig for gjenoppretting av normal bruk, skal kopieres."

Håndboken slår fast at det skal foretas sikkerhetskopiering av data som inneholder personopplysninger. Formålet med sikkerhetskopieringen er å gjøre det mulig å gjenopprette normal drift av informasjonssystemet etter avbrudd eller feil, herunder etablere tekniske sikkerhetsløsninger på nytt, samt gi tilgang til de personopplysninger som behandles.

Videre heter det i håndboken at: «Det er den behandlingsansvarlige som har ansvaret for å utarbeide beredskapsplaner og å iverksette alternativ drift for de ulike behandlingene (...) Vurdering av avbruddets virkning på informasjonssystemet og for informasjonssikkerheten skal være beskrevet for hver enkelt behandling i form av risikovurdering og tiltak som skal gjennomføres for å forbedre kontinuitet i forhold til driftsavbrudd».

Dette punktet er ikke blitt fulgt opp i praksis, men fylkeskommunen har utarbeidet en overordnet risikoanalyse (ROS-analyse), som vil danne grunnlag for en ny beredskapsplan. Fylkeskommunens ROS-analyse fra 2011 berører spørsmålet om tilgjengelighet av personopplysninger. Her skisseres ulike scenarier som strømstans, teknisk svikt eller andre former for driftsavbrudd.

Fylkeskommunen svarer i intervju at det tas back-up flere ganger per dag/uke /måned, avhengig av hvilke typer opplysninger det er tale om. Serverne er imidlertid plassert i samme bygg, noe som åpner for sårbarhet ved eksempelvis brann. For å re-

dusere risikoen, er datarommet som ble pusset opp for fire år siden, utstyrt med brannalarm, vannalarm, dieselaggregat og batterier.

Det overordnede sak- og arkivsystemet (ESA), anses å være det mest virksomhetskritiske systemet. Fylkeskommunen har derfor valgt å inngå et samarbeid med Stavanger kommune om deling av datarom, for å ha en ekstra server med backup-utstyr. Her tas det back-up av informasjonen i ESA. For de andre fagsystemene som inneholder sensitive personopplysninger finnes det foreløpig ingen ekstra server med backup-utstyr plassert utenfor fylkeskommunens datarom.

Hvorvidt sensitive personopplysninger oppbevares i papirform eller elektronisk, varierer. I PP-tjenesten foreligger alt i papirform når saken anses som ferdigbehandlet. Underveis i saksbehandlingen blir noe lagret elektronisk, men hovedtyngden av informasjonsmengden foreligger i papirform.

I tannhelsetjenesten oppbevares sensitive personopplysninger utelukkende elektronisk. Tannhelse Rogaland sin nylig utarbeidede beredskapsplan fra september 2012 definerer hvilke aktiviteter og tekniske løsninger som skal settes inn dersom datasystemene ligger nede. Målsettingen er å sikre kortest mulig nedetid. Beredskapsplanen inneholder blant annet krav om gjennomføring av en årlig test. I testen simuleres en mindre hendelse for å kontrollere om det er behov for endringer i prosedyrer, kontaktlister og annet. Hvert tredje år gjennomføres en test av større omfang.

For fagsystemene i PP-tjenesten og Oppfølgingstjenesten er det ikke utarbeidet planer for hva som skal gjøres dersom systemene ligger nede. For de ansatte blir løsningen å legge inn opplysningene når systemet er kommet opp igjen. Disse enhetenes arbeidsoppgaver, sammen med det faktum at mye av arbeidet kan utføres uten tilgang til fagsystemet, gjør at driftsavbrudd får begrensede konsekvenser.

For alle enhetene vil det være vanskelig å drive ordinær saksbehandling dersom datasystemene ligger nede.

Vurdering: Fylkeskommunens ROS-analyse fra 2011 berører spørsmålet om tilgjengelighet av personopplysninger. Denne ROS-analysen dannet grunnlaget for en ny beredskapsplan som ble ferdigstilt høsten 2012. Den nylig utarbeidede beredskapsplanen til IKT og arkiv definerer hvilke aktiviteter som skal settes inn dersom systemene ligger nede. Det samme gjør Tannhelse Rogaland sin beredskapsplan fra september 2012.

For fagsystemene i PP-tjenesten og Oppfølgingstjenesten er det ikke utarbeidet planer for hva som skal gjøres dersom systemene ligger nede, men et kortere driftsavbrudd vil få begrensede konsekvenser.

1.2.12 SIKRING AV INTEGRITET

Personopplysningsforskriften § 2-13:
"Det skal treffes tiltak mot uautorisert endring av personopplysninger der integritet er nødvendig. Sikkerhetstiltakene skal også hindre uautorisert endring av annen informasjon med betydning for informasjonssikkerheten. Det skal treffes tiltak mot ødeleggende programvare."

Med integritet menes at det verken tilsiktet eller utilsiktet skal skje uautoriserte *endringer* av personopplysninger. Fylkeskommunens rutiner for autorisasjonskontroll, herunder inndeling i ulike soner og tilgangsgrupper, er viktige elementer for å sikre personopplysningenes integritet. Det samme gjelder tiltak som viruskontroll, spamfilter, sikkerhetsrutiner og brannmur. Fylkeskommunen har også anledning til å stanse nedlastingsprogrammer.

Fylkeskommunen samarbeider tett med leverandøren av bredbåndsforbindelsen for å sikre en god beskyttelse mot uønsket mail eller angrep. Forsøk fra utenforstående på å gjøre endringer i fylkeskommunens informasjonssystem, har ikke forekommet.

Behandlingsansvarlig for det enkelte datasystem opplever at informasjonssikkerheten blir godt ivaretatt med dagens system, hvor inndelingen i soner og tilgangskontroll fremstår som meget viktige tiltak. De behandlingsansvarlige er tilfredse med de tiltakene som IKT- og arkivseksjonen har satt i verk på dette området.

Vurdering: Fylkeskommunens tiltak for sikring av de sensitive personopplysningene mot autoriserte endringer, anses tilfredsstillende.

1.2.13 SIKRINGSTILTAK

Personopplysningsforskriften § 2-14:
"Sikkerhetstiltak skal hindre uautorisert bruk av informasjonssystemet og gjøre det mulig å oppdage forsøk på slik bruk. Forsøk på uautorisert bruk av informasjonssystemet skal registreres.
Sikkerhetstiltak skal omfatte tiltak som ikke kan påvirkes eller omgås av medarbeiderne, og ikke være begrenset til handlinger som den enkelte forutsettes å utføre. Sikkerhetstiltak skal dokumenteres."

For å hindre uautorisert tilgang er det definert sikkerhetsbestemmelser i håndbokens punkt 5.1.3. Her heter det blant annet at kontroll med at tildelte autorisasjoner fungerer etter forutsetningene, skal utføres.

Arbeidsoppgavene i både PP-tjenesten, Oppfølgingstjenesten og i Tannhelse Rogaland tilsier at alle ansatte må ha tilgang til alt i sine respektive datasystemer. Revisjonen får opplyst at tilganger til ansatte som har sluttet eller flyttet til andre deler av fylkes-

kommunen, blir slettet. I tillegg kontrollerer IKT- og arkivseksjonen tilgangslister mot ansattelister, med jevne mellomrom.

I datasystemene er det mulig å avgrense tilgangen til et mindre antall personer. I det overordnede sak- og arkivsystemet (ESA), har fylkeskommunen laget små tilgangsgrupper, for å hindre at sensitive personopplysninger tilflyter uvedkommende. Egenproduserte dokumenter er det den ansatte selv som graderer.

Fylkesarkivaren gjennomfører jevnlig kontroller ute på skolene for å påse at bruken av tilgangsgrupper i ESA fungerer etter sin hensikt. Så langt viser kontrollene at skolene er flinke til å begrense informasjonsflyten til mindre grupper. I ett tilfelle oppdaget fylkesarkivaren unødvendig store tilgangsgrupper, noe som nå er rettet opp.

I Rogaland fylkeskommune sin håndbok for informasjonssikkerhet slås det fast at: «Alle ansatte som har behov for å bruke fylkeskommunens dataanlegg skal i tillegg til ren brukeropplæring også få opplæring i datasikkerhet» (jf. punkt 2.3.1). Kunnskap om informasjonssikkerhet har imidlertid ikke vært en del av opplæringen for nyansatte. Nyansatte blir kun henvist til å lese informasjonssikkerhetshåndboken og «Reglement for bruk av datasystemer».

Fylkeskommunen har imidlertid arrangert kurs for rektorer og seksjonsledere. Kursene har omhandlet hvilket ansvar de har som «behandlingsansvarlige», etter personopplysningsloven.

Vurdering: De ansvarlige for det enkelte fagsystem oppgir at tilganger til ansatte som har sluttet eller fått andre oppgaver, blir slettet. Gjennom fylkesarkivarens undersøkelser blir bruken av tilgangsgrupper på skolene kontrollert med jevne mellomrom. Bruk av tilgangsgrupper er et effektivt middel for å hindre unødig spredning av sensitive personopplysninger.

1.2.14 SIKKERHET HOS ANDRE VIRKSOMHETER

Personopplysningsforskriften § 2-15:
"Den behandlingsansvarlige skal bare overføre personopplysninger elektronisk til den som tilfredsstiller kravene i forskriften her. Den behandlingsansvarlige kan overføre personopplysninger til enhver dersom overføringen skjer i samsvar med reglene i personopplysningsloven §§ 29 og 30, eller når det er fastsatt i lov at det er adgang til å kreve opplysninger fra et offentlig register.

Leverandører som gjennomfører sikkerhetstiltak, eller gjør annen bruk av informasjonssystemet på den behandlingsansvarliges vegne, skal tilfredsstille kravene i dette kapittelet. Den behand-

lingsansvarlige skal etablere klare ansvars- og myndighetsforhold overfor kommunikasjonspartnere og leverandører. Ansvars- og myndighetsforhold skal beskrives i særskilt avtale.

Den behandlingsansvarlige skal ha kunnskap om sikkerhetsstrategien hos kommunikasjonspartnere og leverandører, og jevnlig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet."

Fylkeskommunens leverandører skal undertegne taushetserklæring. Det skal lages oversikt over hvilke av partnerens eller leverandørens personell som gis tilgang til informasjonssystemet eller adgang til områder eller utstyr, samt hvordan virksomhetens kontroll av sikkerhet hos partner og leverandør skal utføres[6].

Leverandøren skal til enhver tid ha en organisatorisk og teknisk sikkerhetsløsning som tilfredsstiller Datatilsynets retningslinjer. Dette skal kunne dokumenteres overfor oppdragsgiver og Datatilsynet. Som ledd i virksomhetens årlige egenkontroll, bør det være et møte for å gjennomgå leverandørens organisatoriske og tekniske sikkerhetstiltak.

Ifølge fylkeskommunens håndbok for informasjonssikkerhet, punkt 4.1.1, skal leverandører skrive under på en taushetserklæring. Revisjonen får opplyst at alle kontrakter som inngås mellom fylkeskommunen og en leverandør, inneholder et punkt om taushetsplikt. Hver enkelt reparatør som kommer for å utføre et konkret oppdrag, må underskrive en taushetserklæring.

I møter ved kontraktsinngåelse, underveis og i etterkant av oppdraget får fylkeskommunen kjennskap til leverandørens rutiner for informasjonssikkerhet. Ved bruk av rammeavtaler er innsyn i HMS-rutiner en del av anskaffelsesprosessen.

Vurdering: Hver enkelt representant fra eksterne leverandører må underskrive en taushetserklæring. Fylkeskommunen får kjennskap til leverandørens sikkerhetsstrategi og rutiner for informasjonssikkerhet underveis i prosessen.

1.2.15 DOKUMENTASJON

Personopplysningsforskriften § 2-16:
"Rutiner for bruk av informasjonssystemet og annen informasjon med betydning for informasjonssikkerheten, skal dokumenteres. Dokumentasjon skal lagres i minst 5 år fra det tidspunkt dokumentet ble erstattet med ny gjeldende utgave.

[6] Datatilsynets veileder til internkontroll og informasjonssikkerhet.

Registrering av autorisert bruk av informasjonssystemet og av forsøk på uautorisert bruk, skal lagres minst 3 måneder. Det samme gjelder registreringer av alle andre hendelser med betydning for informasjonssikkerheten."

Forsøk på såkalt "hacking" eller andre former for uautorisert bruk, er det ingen av de behandlingsansvarlige for de ulike fagsystemene som har registrert. All aktivitet blir loggført og lagret i henhold til forskriftens krav.

Gjeldende håndbok for informasjonssikkerhet ble utarbeidet i 2008. Håndboken fremstår som noe unøyaktig. Eksempelvis inneholder eksemplaret som ligger ute på intranettet formuleringen «ikke vedtatt» på flere sider.

Et annet eksempel er håndbokens beskrivelse av ansvars- og myndighetsforhold, som aldri er blitt en realitet. I punkt 3.1.1 heter det at «Videre er det en informasjonssikkerhetsleder som har det daglige praktiske arbeidet med å følge opp informasjonssikkerhetsstyrets instrukser». Revisjonen får opplyst at det aldri har vært utnevnt en informasjonssikkerhetsleder. Mellom rådmannsnivå og den enkelte avdeling/seksjon/ skole har det ikke være noen informasjonssikkerhetsleder.

Fylkeskommunens personvernombud er i samarbeid med en arbeidsgruppe i gang med å utarbeide en ny utgave av håndboken for informasjonssikkerhet. En ny og oppdatert utgave av håndboken skal være klar i løpet av januar 2013.

Vurdering: Rutiner for bruk av informasjonssystemet fremstår som noe unøyaktig og uoversiktlig. En arbeidsgruppe er nå nedsatt for å «rydde opp». Håpet er at forholdene vil bedre seg og at både rutiner og ansvars- og myndighetsforhold vil bli klargjort.

VEDLEGG

Om forvaltningsrevisjon

I kommunelovens § 77.4 pålegges kontrollutvalgene i fylkeskommunene og kommunene å påse at det gjennomføres forvaltningsrevisjon. Forvaltningsrevisjon innebærer systematiske vurderinger av økonomi, produktivitet, måloppnåelse og virkninger ut fra kommunestyrets vedtak og forutsetninger. Lovens bestemmelser er nærmere utdypet i revisjonsforskriftens kapittel 3 og kontrollutvalgsforskriftens kapittel 5.

Revisjon i norsk offentlig sektor omfatter både regnskapsrevisjon og forvaltningsrevisjon, i motsetning til i privat sektor hvor kun regnskapsrevisjon (finansiell-) er obligatorisk.

Rogaland Revisjon IKS utfører forvaltningsrevisjon på oppdrag fra kontrollutvalget i kommunen. Arbeidet er gjennomført i henhold til NKRF sin standard for forvaltningsrevisjon, RSK 001. Les mer på www.rogaland-revisjon.no.

Denne rapporten er utarbeidet av forvaltningsrevisor Frode K. Gøthesen, under ledelse av fagansvarlig for forvaltningsrevisjon Bernt Mæland.

Revisjonskriterier og metode

Revisjonskriteriene er elementer som inneholder krav eller forventninger, og vil bli brukt til å vurdere funnene i de undersøkelser som gjennomføres. Kriteriene skal være begrunnet i, eller utledet av, autoritative kilder innenfor det reviderte området. I prosjektet er følgende kilder vektlagt ved utarbeidelsen av revisjonskriteriene:

- Krav til informasjonssikkerhet i personopplysningsloven med forskrift
- Datatilsynets føringer og veiledere for informasjonssikkerhet
- Håndbok for informasjonssikkerhet i Rogaland fylkeskommune
- Reglement for bruk av RFK sine datasystemer
- Rogaland fylkeskommune sin IKT-strategi

Metodisk er det benyttet intervju og dokumentgransking. Kun *elektronisk* behandling av *sensitive* personopplysninger er undersøkt. Hvordan informasjonssikkerheten er ivaretatt for opplysninger lagret i papirform, er ikke undersøkt.

De behandlingsansvarlige for de ulike fagsystemene, med unntak av behandlingsansvarlig for fagsystemet til PP-tjenesten, oppgir at personopplysningene hovedsakelig ligger lagret elektronisk. Ved vår gjennomgang er det spurt om sikkerhetsopplegget er fulgt, men det er ikke foretatt noen detaljkontroll.

Gjennomgåtte dokumenter:

- Rogaland fylkeskommune sin håndbok for informasjonssikkerhet (2008)
- Reglement for bruk av Rogaland fylkeskommune sine datasystemer (ikke datert)
- IKT-strategi 2011-14. Rogaland fylkeskommune
- IKT-strategi 2011-14 – Handlingsplan. Rogaland fylkeskommune
- Strategi for Sikkerhets- og kvalitetskultur i Rogaland fylkeskommune (2012)
- Saksforelegg til ledergruppen i Rogaland fylkeskommune 24.09.2012 om Strategi for Sikkerhets- og kvalitetskultur i Rogaland fylkeskommune.
- IKT informasjonssikkerhet Tannhelse Rogaland (2012)
- Beredskapsplan IKT Tannhelse. Rogaland fylkeskommune (ikke datert)
- Overordnet ROS-analyse Rogaland fylkeskommune (2012)
- Retningslinjer for publisering av dokumenter i Qm pluss.
- Melding om uønsket hendelse i Qm pluss. Rogaland fylkeskommune (2012)

- Prosjekthåndbok – Dilbert – Kvalitetssystem. Versjon 2-0.
- Retningslinjer for dokumentsystem Dilbert. Rogaland fylkeskommune.

- Rogaland Revisjon: Gjennomgang av sikkerhetsopplegg for behandling av personopplysninger (2005)
- Rogaland Revisjon: Elektronisk behandling av sensitive personopplysninger i Sandnes kommune (2010)

- Datatilsynets veileder for internkontroll og informasjonssikkerhet (2009)
- Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer Datatilsynet (2000).
- Datatilsynets veileder for personvernombudets oppgaver (2010)
- Datatilsynets veileder for databehandleravtaler (2009)
- Kommuneundersøkelsen 2010-2011 om internkontroll og informasjonssikkerhet. Datatilsynet (2011)
- Presentasjonsbrosjyre personvernombud (Datatilsynet)

- Sikre riktig person tilgang til riktig informasjon til rett tid. Temahefte. Uninett ABC (2007)
- Rådmannens internkontroll. Orden i eget hus. KS (2012).

Informanter

Personer som er intervjuet:

- Direktør for administrasjonsavdelingen, Håkon Schwalb
- Leder for IKT- og arkivseksjonen, Odd Bård Risvoll

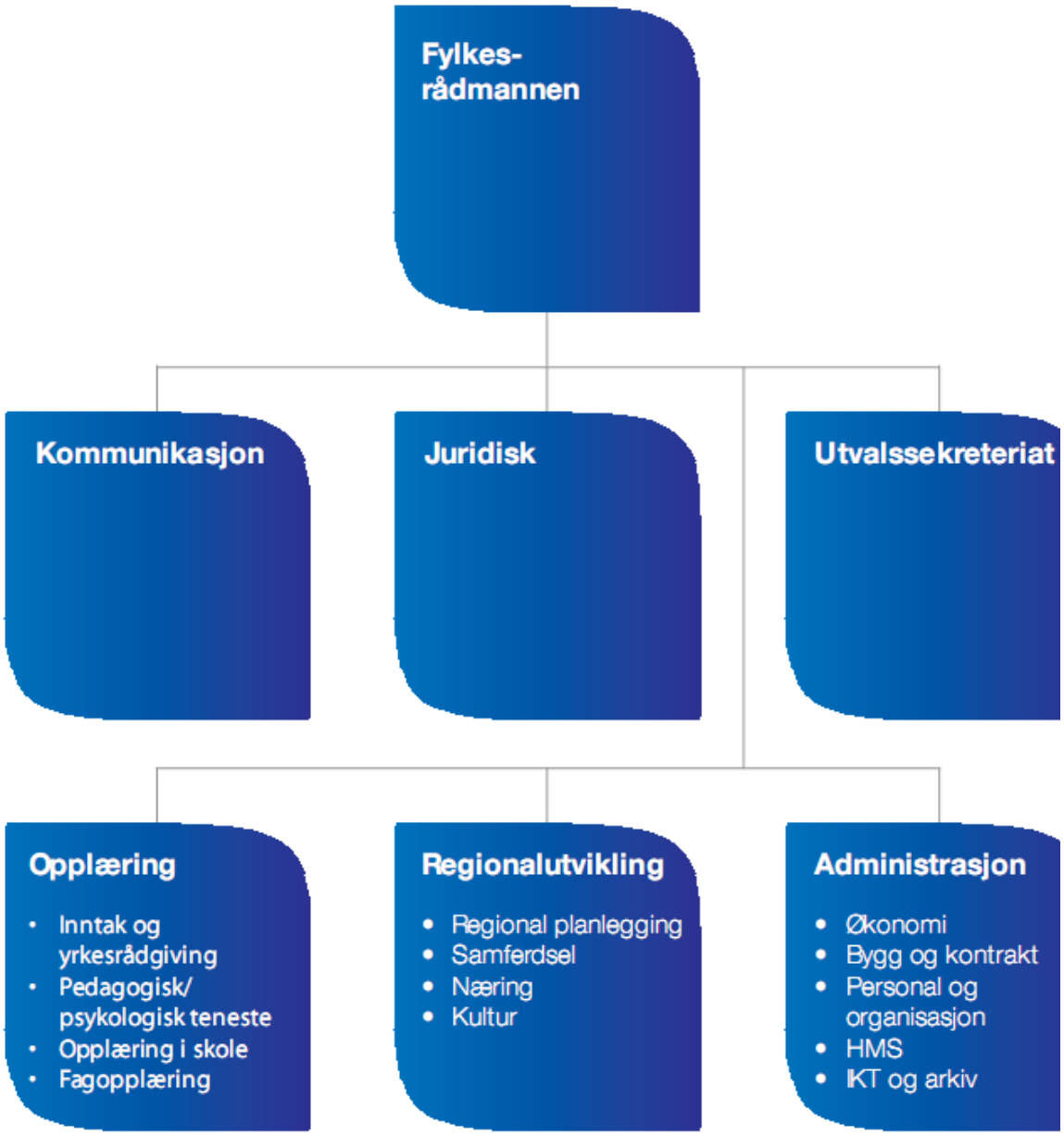
- Personvernombud Liv Fredriksen
- Fylkesarkivar Marie Manshaus

- Fylkestannlege/ daglig leder i Tannhelse Rogaland, Helene Haver
- Systemansvarlig Tannhelse Rogaland, Steinar Løgith Aase
- IKT-rådgiver Geir Jørgensen Tannhelse Rogaland

- Leder for PP-tjenesten, Gunnar Gaard
- Konsulent ved PP-tjenesten, Anny Sydow Nedrebø

- Leder for Inntak- og yrkesrådgivningsseksjonen, med ansvar for Oppfølgingstjenesten, Ståle Wold

Figur 1 – Organisasjonskart Rogaland fylkeskommune.



Rogaland Revisjon IKS

Regnskapsrevisjon **Forvaltningsrevisjon** **Selskapskontroll** **Andre tjenester**

Rogaland Revisjon IKS

Løkkeveien 10
4008 Stavanger

Tlf 40 00 52 00
Faks 51 84 47 99

www.rogaland-revisjon.no