KOMMUNEREVISJONSDISTRIKT 2
MØRE OG ROMSDAL

Forvaltningsrevisjonsrapport

Informasjonssikkerhet

i

Aukra kommune

9. november 2015

Kommunerevisjonsdistrikt 2 Møre og Romsdal er interkommunalt selskap etter kommuneloven § 27. Eiere er kommunene Aukra, Eide, Fræna, Gjemnes, Molde, Nesset, Rauma, Sunndal og Vestnes. Selskapet utfører regnskapsrevisjon, forvaltningsrevisjon og selskapskontroll for eierkommunene og har i dag seks revisorer. Selskapet har hovedkontor i Molde.

Innholdsliste

1 Innledning

1.1 Bakgrunn

Kommunens revisor har som en av sine oppgaver å utføre forvaltningsrevisjon, jf. kommuneloven § 78 nr. 2 og forskrift om revisjon kapittel 3. Forvaltningsrevisjon innebærer å gjennomføre systematiske vurderinger av økonomi, produktivitet, måloppnåelse og virkninger ut fra kommunestyrets vedtak og forutsetninger, jf. kommuneloven § 77 nr. 4.

Aukra kommune har vedtatt overordnet plan for forvaltningsrevisjon for 2012 til 2015, jf. sak 50/2012 i kommunestyret og sak 7/2012 i kontrollutvalget. Kontrollutvalget har i møte 18.11.2014 i sak 35/2014 vedtatt å prioritere et forvaltningsrevisjonsprosjekt i 2015 om informasjonssikkerhet. Prosjektet gjennomføres av Kommunerevisjonsdistrikt 2 Møre og Romsdal.

1.2 Problemstillinger og revisjonskriterier

Revisjonskriterier er de krav og forventninger som funnene i undersøkelsen blir vurdert opp mot. Kommunerevisjonsdistrikt 2 Møre og Romsdal har basert på kontrollutvalgets bestilling, valgt følgende problemstillinger og revisjonskriterier for forvaltningsrevisjonsprosjektet:

Problemstilling 1 (kapittel 2)
Har Aukra kommune tilfredsstillende informasjonssikkerhet?

Problemstilling 2 (kapittel 3)
Har Aukra kommune tilfredsstillende posthåndtering?

Revisjonskriterier
Kriteriene knyttet til problemstilling 1 er hentet fra:
- Lov om behandling av personopplysninger (personopplysningsloven)
- Forskrift om behandling av personopplysninger (personopplysningsforskriften)
- En veiledning om internkontroll og informasjonssikkerhet, Datatilsynet (november 2009)
- Sikkerhetsbestemmelsene i personopplysningsforskriften, Datatilsynet (desember 2000)
- Anbefalinger fra Statskonsult om IK sikkerhet; IKT i det offentlige (2002)
- Anbefalinger fra KS om IK sikkerhet; Verktøykasse for IKT-planlegging (2004)
- COBIT anbefalinger for god IT-skikk utviklet av ISACA

Lov om behandling av personopplysninger (personopplysningsloven) § 13 bestemmer at:

«Den behandlingsansvarlige databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet men hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger».

Forskrift om behandling av personopplysninger (personopplysningsforskriften) definerer nærmere hvilke krav som hviler på kommunen for å sikre tilfredsstillende informasjons-sikkerhet ved behandling av personopplysninger. Tilfredsstillende informasjonssikkerhet skal oppnås ved hjelp av planlagte og systematiske tiltak. Begrepet innebærer at kjente teknikker og anerkjente standarder for kvalitetsstyring, internkontroll og informasjonssikkerhet skal legges til grunn ved sikkerhetsarbeidet.

Datatilsynet har i 2009 utgitt Veileder til internkontroll og informasjonssikkerhet. Dokumentet gir veiledning til innføring av internkontroll og informasjonssikkerhet for å sikre forsvarlig og sikker behandling av personopplysninger.

Revisjonskriterier gjeldende posthåndtering er hentet fra forvaltningsloven, eForvaltnings-forskriften, arkivlova og arkivforskrifter.

Revisjonskriteriene vil bli ytterligere beskrevet i punkt 2.1.1 til 2.1.9, 3.1 og vedlegg 2.

1.3 Avgrensing av undersøkelsen

Forvaltningsrevisjonsprosjektet omfatter ikke revisjon av de enkelte datasystemene/ informasjonsteknologisystemene i kommunen. Dette betyr at de enkelte datasystemene ikke vurderes i prosjektet.

1.4 Metode

Undersøkelsen er basert på krav fastsatt i kommuneloven § 78, forskrift om revisjon i kommuner og fylkeskommuner og Norges Kommunerevisorforbund (NKRF) sin standard for forvaltningsrevisjon (RSK 001).

Undersøkelsen er i hovedsak lagt opp som en kombinasjon av analyse av innhentet dokumentasjon og intervju av ansatte med ansvar og oppgaver knyttet til informasjonssikkerhet og informasjons- og kommunikasjonsteknologi i kommunen.

Forvaltningsrevisjonen har intervjuet følgende personer:
- Rådmann, behandlingsansvarlig
- Servicesjef, systemansvarlig
- Rådgiver, systemadministrator
- IT-rådgiver Institusjonstjenestene (systemansvarlig Helsenett/ Cos Doc)
- Arkivkonsulent

1.5 Høring

Et foreløpig utkast til rapport har vært forelagt Aukra kommune ved rådmann, og gjennomgått i høringsmøte 27.10.2015. I etterkant av møte ble justert utkast sendt på høring. Høringsuttalelse fra Aukra kommune datert 5.11.2015 følger som vedlegg 1.

1.6 Informasjonssikkerhet

Personopplysningsloven og personopplysningsforskriften

Personopplysningsloven har som formål å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Loven sier at personopplysninger skal behandles i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysningene.

Personopplysningsforskriften gir utfyllende og mer detaljerte krav til behandling av personopplysninger. Forskriftens kapittel 3 gir utfyllende bestemmelser om internkontroll, mens kapittel 2 gir utfyllende bestemmelser om informasjonssikkerhet.

Informasjonssikkerhet
Informasjons- og kommunikasjonsteknologi (IKT) er et begrep som omfatter teknologi for innsamling, lagring, behandling, overføring og presentasjon av informasjon.

I praksis brukes ofte begrepene datateknikk og kommunikasjonsteknologi. IKT er også ofte omtalt som kun *informasjonsteknologi* (IT), og tidligere var begrepet *elektronisk databehandling* (EDB) utbredt.

Informasjonssikkerhet, datasikkerhet, eller IT-sikkerhet er et fagområde som er knyttet til nøkkelbegrepene *konfidensialitet* (sikre at informasjon og informasjonssystemer bare er tilgjengelig for de som skal ha tilgang), *integritet* (sikre at informasjon og informasjonssystemer er korrekte, gyldige og fullstendige) og *tilgjengelighet* (sikre at informasjon og informasjonssystemer er tilgjengelig innenfor de tilgjengelighetskrav som er satt).

Personopplysningsloven krever at personopplysninger skal beskyttes tilfredsstillende mot uberettiget innsyn og endringer. Samtidig skal opplysningene være tilgjengelige for de som trenger opplysningene, *når* de har behov for disse. Informasjonssikkerhet dreier seg om å håndtere risikoen for at personopplysninger og andre informasjonsverdier blir ivaretatt på en tilfredsstillende måte. Dette gjøres ved først å identifisere hvilke personopplysninger virksomheten har. Deretter gjennomføres en risikovurdering for å avklare om eksisterende sikkerhetstiltak er tilfredsstillende.

Dersom risikovurderingen avdekker manglende tiltak må det vurderes om nye tiltak skal iverksettes for å oppnå tilfredsstillende sikkerhetsnivå for personopplysningene. Kontrollrutiner må utarbeides og jevnlig følges, for å kontrollere at tiltakene blir fulgt opp og virker etter hensikten. En slik fremgangsmåte vil sammen med tilhørende rutiner kunne utgjøre virksomhetens styringssystem for informasjonssikkerhet. Dette systemet for informasjonssikkerhet vil være en sentral del av virksomhetens internkontroll. Det er utviklet ulike standarder som beskriver hvordan styringssystem for informasjonssikkerhet skal etableres.

God IT-skikk
Information Systems Audit and Control Association (ISACA) er en verdensomspennende forening for IT-styring og kontroll, sikkerhet, kontroll og revisjon av informasjonsteknologi.

Control Objectives for Information and Related Technology (COBIT) er utviklet av ISACA og IT Governance Institute (ITGI) og gir anbefalinger for god IT-skikk. God IT-skikk *anbefaler* at det etableres IT-strategi/ planer og at disse er forankret i og bygger opp under kommunens mål og planer. I tillegg bør en kommune ha konkrete handlingsplaner og investeringsplaner for hvordan de overordnede strategiene skal nås.

God IT-skikk anbefaler at det foreligger dokumentasjon som viser samtlige IT-systemer og sammenhengen mellom disse. Dokumentasjonen bør inneholde en overordnet informasjon om systemene.

God IT-skikk anbefaler at det etableres planer som ivaretar kontinuitet i driften ved alvorlige hendelser. Videre anbefales det at avbrudd i drift av IKT logges og at det informeres om dette til eier og brukere. Det bør innføres kriterier som definerer hva som er alvorlige hendelser.

God IK-skikk beskriver en rekke aktiviteter for å sikre forsvarlig gjennomføring av endringer som påvirker driften av IKT systemene. Det er for eksempel tiltak for å sikre at alle endringer gjennomføres på en effektiv og kontrollert måte. God IT-skikk anbefaler at kommunen etablerer retningslinjer, prosedyrer og instrukser som sikrer at endringer er autorisert, planlagt, risikovurdert, dokumentert, testet og godkjent.

Veileder i informasjonssikkerhet og internkontroll
Datatilsynet publiserte i november 2009 en veileder i *informasjonssikkerhet* og *internkontroll.* Det er utarbeidet en rekke maler til veilederen. Malene skal hjelpe kommunene til å få på plass internkontroll i egen virksomhet. Kommunene kan laste ned malene fra www.datatilsynet.no. Følgende maler foreligger:

<u>Styring og ledelse</u>
- Styringsdokument Internkontroll (1-01)
- Ledelsens gjennomgang (1-02)
- Sikkerhetsmål- og strategi (1-11)
- Sikkerhetsorganisasjon (1-12)

<u>Rutiner og sjekklister</u>
- Rutiner for håndtering av personopplysninger (2-01)
- Risikovurdering (2-11)
- Sikkerhetsinstruks brukere (2-12)
- Informasjonshåndtering (2-14)
- Sjekkliste for nyansatt og ansatte som slutter (2-15)
- Taushetserklæring (2-16)
- Sikkerhetsinstruks leder (2-17)
- Sikkerhetsinstruks sikkerhetsansvarlig (2-19)
- Beskrivelse av informasjonssystemet (2-21)
- Driftsrutiner (2-22)
- Overordnet IT-beredskapsplan (2-23)
- Fysisk sikkerhet (2-24)

<u>Avvik og avvikshåndtering</u>
- Avvikshåndtering og egenkontroll (3-01)
- Avviksskjema (3-02)
- Egenkontrollskjema (3-03)
- Rapport fra avvikshåndtering og egenkontroll med forslag til tiltak (3-04)

Datatilsynet
Datatilsynet er tilsynsmyndighet relatert til kommuners etterlevelse av krav til *informasjonssikkerhet* og *internkontroll.* Datatilsynet har de siste årene gjennomført kontroller av kommuners *behandling av personopplysninger*, med spesielt fokus på internkontroll og tilfredsstillende informasjonssikkerhet. Kommunerevisjonen har nyttet rapporter utarbeidet av

Datatilsynet når vi redegjør for regelverk om informasjonssikkerhet og ved utarbeidelse av revisjonskriterier.

Veiledningsmateriell for internkontroll av informasjonssikkerhet utarbeidet av Difi
Statens kompetansemiljø for informasjonssikkerhet (Difi) arbeider for en styrket og mer helhetlig tilnærming til informasjonssikkerhet i statsforvaltningen. Difi har utarbeidet et praktisk rettet veiledningsmateriell for internkontroll av informasjonssikkerhet. Materiellet er basert på anerkjente standarder for styringssystemer for informasjonssikkerhet. Hensikten er å hjelpe forvaltningen til å få bedre styring og kontroll med informasjonssikkerheten.

2 Informasjonssikkerhet i Aukra kommune

Kommunerevisjonen har i forvaltningsrevisjonsprosjektet vurdert om Aukra kommune har tilfredsstillende informasjonssikkerhet, som sikrer krav til konfidensialitet, integritet og tilgjengelighet. Revisjonen har undersøkt ni områder. For å sikre god leservennlighet har revisjonen valgt å redegjøre for fakta, og knytte egne vurderinger og anbefalinger til hvert av de ni områdene. De ni områdene som er undersøkt er:

1. Aukra kommune har etablert sikkerhetsledelse, sikkerhetsmål og sikkerhetsstrategi
2. Aukra kommune har tilstrekkelig oversikt over personopplysninger som behandles
3. Aukra kommune gjennomfører jevnlig sikkerhetsrevisjon
4. Aukra kommune har etablert avviksbehandlingssystem og behandler sikkerhetsbrudd som avvik
5. Aukra kommune har en klar organisering med etablerte ansvars- og myndighetsforhold
6. Aukra kommune har fysisk sikring mot uautorisert tilgang
7. Aukra kommune har tiltak mot uautorisert innsyn
8. Aukra kommune sikrer tilgang til personopplysninger
9. Aukra kommune har tiltak mot uautorisert endring av personopplysninger

Ytterligere informasjon om innholdet og forståelsen av revisjonskriteriene er gitt under det enkelte punkt i kapittel 2.1.1 til 2.9.1, og i vedlegg 2.

2.1 Sikkerhetsledelse, sikkerhetsmål og sikkerhetsstrategi

2.1.1 Revisjonskriterier

Revisjonskriterier: ***Aukra kommune har etablert sikkerhetsledelse, sikkerhetsmål, sikkerhetsstrategi***

Personopplysningsforskriften § 2-3 stiller krav om at det er etablert en sikkerhetsledelse, sikkerhetsmål og sikkerhetsstartegi:

> *«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».*

I henhold til forskriften § 2-3 skal formålet med behandling av personopplysninger og overordnede føringer for bruk av informasjonsteknologi beskrives i sikkerhetsmål. Valg og prioriteringer skal beskrives i en sikkerhetsstrategi. Bruk av informasjonssystemet skal jevnlig, eksempelvis årlig, gjennomgås for å kartlegge om den er hensiktsmessig for virksomhetens behov og om sikkerhetsstrategien gir tilfredsstillende informasjonssikkerhet som resultat. Sikkerhetsstrategier vil omfatte grunnleggende beslutninger om organisering og gjennomføring av sikkerhetsarbeidet i virksomheten.

Personopplysningsloven definerer i § 2 nr. 4 behandlingsansvarlig som «den som bestemmer formålet med behandlingen av personopplysninger og hvilke virkemiddel som skal brukes». Forskriften § 2-7 stiller krav om at det skal etableres klare ansvars- og myndighetsforhold (sikkerhetsorganisasjon). Sikkerhetsorganisasjon og sikkerhetsledelse er nærmere omtalt under punkt 2.5.

2.1.2 Fakta

Aukra kommune har ikke dokument som omhandler informasjonssikkerhet særskilt. Kommunen har utarbeidet et dokument som viser oversikt over planer som er utarbeidet. Plan for informasjonssikkerhet er ikke på denne listen, og i intervjuer kom det fram at slik plan ikke er utarbeidet. ROR-IKT har utarbeidet dokumenter som omtaler sikkerhetsledelse, sikkerhetsmål og sikkerhetsstrategi. Innhold og avklaringer som gis i disse dokumentene er i liten grad kjent i Aukra kommune. Dokumentene omtales nærmere under punkt 2.5.

Fram til 30.12.2013 var IKT ivaretatt av egne ansatte i kommunen. Kommunen gikk inn i et interkommunalt samarbeid på IKT-området fra 1.1.2014, og driftsansvaret for IKT ble fra samme tidspunkt lagt til ROR-IKT. ROR-IKT ble etablert etter vedtak i medlemskommunene Aukra, Midsund, Molde, Rauma og Vestnes. Bakgrunnen for etableringen var erkjennelsen av at kommunene måtte stå sammen om å løse utfordringene på IKT-området, og for å dempe utviklingen i driftskostnadene ved å ta ut stordriftsfordeler.

I intervju kom det videre fram at Aukra kommune mangler overordnede dokumenter om informasjonssikkerhet.

Aukra kommune har etablert et helhetlig kvalitetssystem: Kvalitetslosen.
I politisk sak i forbindelse med investering i Kvalitetslosen er krav til internkontroll omtalt. Aukra kommune har ikke et spesifikt dokument som omhandler informasjonssikkerhet særskilt, men kommunen har dokument som sier noe om databruk og taushetsplikt. Aukra kommune har startet arbeidet med en kvalitetshåndbok. Kommunen har utarbeidet en kvalitetsplakat som viser hva kommunen har jobbet med i forhold til internkontroll på overordnet nivå. Aukra kommune har gjennomført en ROS-analyse på kommunehuset i forhold til brannsikkerhet.

I intervju framkom det kommunen skal starte et arbeid med å utarbeide plan for informasjonssikkerhet, og gjennom dette utarbeide rutiner.

Oppgaver knyttet til IKT var fram til og med 2013 lagt til Personalavdeling, fra 2014 er dette ivaretatt av ROR-IKT. I 2014 ble det lyst ut stilling i Aukra kommune som rådgiver for digitale-tjenester, inkludert oppgaver knyttet til Kvalitetslosen og informasjonssikkerhet. Det er ikke klart definert hva dette arbeidet omfatter. Stillingen ble besatt høsten 2014, og stillings-innehaver har hittil hatt hovedfokus på innføring av Kvalitetslosen. Stillingsinnehaver har

deltatt på kurs og har startet med å avklare prioriterte oppgaver knyttet til informasjonssikkerhet.

Det framgår ikke av delegasjonsskriv hvordan og hvem som ivaretar arbeid med informasjonssikkerhet. Informasjonssikkerhet er ikke omtalt i politisk- eller administrativt delegasjonsskriv.

Det pågår et arbeid med å utarbeide tjenesteavtaler mellom stabsavdelingene og avdelingene. Det opplyses at det vil bli vurdert å ta inn avklaringer om informasjonssikkerhet i den del som omtaler Servicekontoret.

Det kom fram i samtaler at leder av Servicekontoret framover ønsker å ha møter med enhetslederne om rutiner. I slike møter vil det bli gitt informasjon om informasjonssikkerhet.

Tjenestenivåavtale mellom ROR-IKT og Aukra kommune gir avklaringer av ansvars- og myndighetsforhold i Aukra kommune gjeldende informasjonssikkerhet. Det er blant annet avklart at rådmannen i Aukra kommune er behandlingsansvarlig iht personopplysningsloven. I intervju framkom det at avtalen i liten grad er kjent og implementert i Aukra kommune.

Styret i ROR-IKT godkjente 4.2.2015 «Digitaliseringsstrategi for kommunene i ROR-IKT 2015-2018». Det opplyses i strategidokumentet at medlemskommunene har et stort felles behov for å utvikle og effektiviserte kommunens interne prosesser og tjenesteproduksjon og å møte forventninger om digitale tjenester.

I dokumentet er informasjonssikkerhet omtalt i kapittel 10.2. Under gjengis hovedinnholdet i nevnte kapittel:

10.2 Informasjonssikkerhet
Kommunene i ROR-IKT behandler store mengder person- opplysninger, og omfatter alle innbyggere. På mange tjenesteområder behandles det sensitive personopplysninger, og ivaretakelse av personvern, taushetsplikt og innsynsrett er viktig for å opprettholde tillit hos innbyggerne

10.2.1 Mål
- *Kommunene i ROR-IKT har en felles strategi for informasjonssikkerhet*
- *Kommunene i ROR-IKT har en felles databehandleravtaler med andre som behandler personopplysninger på vegne av kommunene*
- *Kommunene i ROR-IKT har databehandleravtaler med andre som kommunene behandler personopplysninger for*
- *Kommunene i ROR-IKT har ledelsesforankret internkontroll og styringssystem på plass*
- *Kommunene i ROR-IKT har løsninger som tilfredsstiller kravene til sikkerhetsarkitektur*
- *Når kommunene i ROR-IKT som tar i bruk skytjenester, skal det gjennomføres felles grundige risiko- og sårbarhetsanalyser og inngå en databehandleravtale*

10.2.2 Tiltak

2015	*Etablert nettverk for datasikkerhetsansvarlige, utarbeide en felles strategi for informasjonssikkerhet* *Databehandleravtale etablert*
2016	
2017	*Felles internkontrollsystem etablert*
2018	

I intervju ble det opplyst at Aukra kommune har stoppet sitt arbeid med informasjonssikkerhet. Dette er gjort fordi kommunen venter på avklaringer i forbindelse med arbeid som eventuelt skal gjennomføres i regi av ROR-IKT. I følge digitaliseringsstrategien som ROR-IKT har utarbeida, skal det etableres en faggruppe som skal jobbe med informasjonssikkerhet. Aukra kommune skal ha med minimum en representant i denne gruppa. Gruppa skal etableres i 2015. I intervju framkom det at Aukra kommune regner med at denne gruppa skal jobbe med rolleforståelse, avklaring av oppgaver som skal ligge til den ansvarlige for informasjonssikkerheten i den enkelte kommune, og utarbeidelse av felles dokumenter.

Dokumenter utarbeidet av ROR-IKT tilsier at ansvar for informasjonssikkerhet må ivaretas av den enkelte kommune.

I intervju framkom det at bruk av sikker sone ivaretas av ROR-IKT. Avdelingsleder bestiller tilgang og ROR-IKT gir nødvendige tilganger eller dette gis via superbruker i avdelingen. I intervju framkom det at det er forventninger om at databrukere nytter skjermsparer, låser dører når kontor forlates, og at utskrift av dokumenter med sensitiv informasjon skal håndteres ved kode på skriver. Det var ikke en ens forståelse av disse kravene, og erfaring viser at kravene ikke alltid følges.

2.1.3 Kommunerevisjonens vurdering og anbefaling

Aukra kommune har ikke dokument som omhandler informasjonssikkerhet særskilt, men kommunen har dokumenter som sier noe om databruk og taushetsplikt. Gjennom ROR-IKT har kommunen dokumenter som omtaler sikkerhetsledelse, sikkerhetsmål eller sikkerhetsstrategi. Disse dokumentene er i liten grad kjent i kommunen.

Det er positivt at Aukra kommune har tatt i bruk et helhetlig kvalitetssystem: Kvalitetslosen.

Oppgave med informasjonssikkerhet er lagt til Servicekontoret, og det er ansatt rådgiver som blant annet skal arbeide med dette. Det er positivt at det er besluttet at det skal startes et arbeid med å utarbeide plan for arbeid med informasjonssikkerhet, og gjennom dette utarbeide informasjonssikkerhetsstrategi og konkrete rutiner.

Revisjonen er kjent med at Molde kommune har utarbeidet en rekke rutiner som omhandler informasjonssikkerhet. Disse rutinene er tilgjengelig for ansatte i kommunens kvalitetssystem. Aukra kommune kan med fordel samarbeide med de kommunene som får tjenester fra ROR-IKT om informasjonssikkerhet.

Anbefaling: Aukra kommune bør sikre at det utarbeides sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet og implementere dette i egen organisasjon.

Aukra kommune bør klargjøre arbeidsdeling gjeldende informasjonssikkerhet med ROR-IKT.

2.2 Oversikt over personopplysninger som behandles

2.2.1 Revisjonskriterier

Revisjonskriterier: ***Aukra kommune har tilstrekkelig oversikt over personopplysninger som behandles***

Personopplysningsforskriften § 2-4 stiller krav om at kommunen har tilstrekkelig oversikt over de personopplysninger som behandles:

«Det skal føres oversikt over hva slags personopplysninger som behandles».

For at den behandlingsansvarlige skal ha oversikt over omfanget av sitt ansvar må virksomheten ha oversikt over hvilke behandlinger av personopplysninger som foretas og hvilke opplysninger som inngår i disse. Dette er en nødvendig del av virksomhetenes internkontroll etter personopplysningsloven § 14. Oversikten er nødvendig for å sikre at grunnvilkårene i § 11 er oppfylt.

Oversikten danner grunnlag for utarbeidelse av virksomhetens sikkerhetsmål og sikkerhetsstrategi og vil være underlag ved virksomhetens risikovurderinger. Kravet til oversikt over behandlinger følger derfor også av forskriften § 2-4.

Oversikten over behandlinger må blant annet omfatte behandlingsgrunnlag (§§ 8 og 9) for den enkelte behandling, samt formålet med behandlingen (§ 11). Alternativt må angivelse av behandlingsgrunnlag og formål fremkomme et annet sted i dokumentasjonen. Kravene til oversikt over behandlinger og behandlingsgrunnlag er utdypet i veilederen *Internkontroll og informasjonssikkerhet,* Datatilsynet. Veilederen har eksempel på hvordan oversikten kan utformes.

2.2.2 Fakta

Aukra kommune har fagsystemer som nyttes i de ulike avdelingene. Det foreligger ikke en ajourført oversikt over fagsystemene, men revisjonen har på forespørsel mottatt informasjon om at kommunen har følgende fagsystem:

Fagsystem på intern sone: 1) Saksbehandling – ePhorte 2) Visma Barnehage 3) Visma Skole 4) Visma Enterprise 5) Wintid/Mintid 6) Visma Ressursstyring

Fagsystem på sikker sone: 1) Acos CosDoc 2) SystemX 3) Visma Hs Pro 4) Visma Velferd

Arkivplan har oversikt over arkivskaper og arkivserier med sentral informasjon som: daglig ansvar, journalførende enhet, innhold, tilgang, oppbevaringsmedium, fysisk plassering, kassasjon, hvem som har godkjent arkivserien, dato for godkjenning. Enkelte arkivserier har også informasjon om informasjonssikkerhet, om arkivserien er konsesjonspliktig eller om det er meldingsplikt. Følgende omtales i arkivplanen:

Sentralarkivet

- *Møtebøker, Journalar og overgripande register, Sakarkiv, Objektarkiv, Spesialarkiv*

Organisasjonsavdelinga

- *Personalmapper*

Økonomiavdelinga

- *Terminoppgjer, Lønsbilag, variable transaksjonar, Lønstilvisingar, Pensjonsordningar, Refusjonsliste frå NAV Trygd, Skattekort, Sjukemeldingar,*

foreldre- og adopsjonspengar, inntekts- og skatteopplysningar, AA-register, Personalmapper

Serviceavdelinga
- *Personalmapper*

Kultur
- *Personalmapper*

Gossen barne- og ungdomsskole
- *Vikarliste skole, Elevmapper, Vitnemålsprotokollar, Karakterprotokollar, Klassedagbøker, Personalmapper*

Julsundet skole
- *Personalmapper, Vikarliste skole, Elevmapper, Vitnemålsprotokollar, Karakterprotokollar, Klassedagbøker*

Teknikk, eigedom og brann
- *Personalmapper*

Utbyggingsavdelinga
- *Personalmapper*

Plan og utvikling
- *Personalmapper*

Bergetippen barnehage
- *Personalmapper, Barnehagesøknader, Vikarliste barnehage, Elevmapper*

Barnebo barnehage
- *Personalmapper, Barnehagesøknader, Elevmapper*

Helse
- *Rekneskapsbilag fysioterapi, Pasientjournalar fysioterapi, Personalmapper*

Heimetenester
- *Personalmapper, Timelister, Brukararkiv*

Institusjonstenester
- *Brukararkiv, Pasientarkiv, Timelister, Personalmapper, Brukar-/pasientrekneskap*

NAV Aukra
- *Kopibok frå fagsystem, Klientarkiv sosialtenesta, Støttekontakt/avlastning, Sosiale lån, Husbankens bustønad, Startlån og tilskot, Løn/timelister/lønstilvisingar, Personalmapper*

Samtaler med ansatte avdekket at beskrivelsene i arkivplan i liten grad er kjent for andre enn arkivkonsulent.

2.2.3 Kommunerevisjonens vurdering og anbefaling

Aukra kommune har ikke oversikt som omfatter grunnlag for den enkelte behandling, samt formålet. Kommunen har imidlertid arkivplan med oversikt over de personopplysningene som kommunen håndterer. Disse er i liten grad kjent blant ansatte som revisjonen har vært i kontakt med.

Revisjonens undersøkelser viser at det ikke er utarbeidet oversikt over personopplysninger som behandles i kommunen.

Anbefaling: Aukra kommune bør utarbeidet en enkel oversikt over de personopplysninger som behandles i kommunen. Oversikten bør gjøres kjent for de med ansvar for informasjonssikkerhet og aktuelle ansatte i organisasjonen.

2.3 Sikkerhetsrevisjon

2.3.1 Revisjonskriterier

Revisjonskriterier: Aukra kommune gjennomfører jevnlig sikkerhetsrevisjon

Personopplysningsforskriften § 2-5 stiller krav om at det gjennomføres jevnlig sikkerhetsrevisjon:

«Sikkerhetsrevisjon av bruk av informasjonssystemet skal gjennomføres jevnlig».

Virksomheten plikter i henhold til forskriften § 2-5 å gjennomføre sikkerhetsrevisjoner jevnlig, eksempelvis årlig. Sikkerhetsrevisjon skal omfatte vurdering av organisering og at sikkerhetstiltak som er besluttet etablert er iverksatt og fungerer etter sin hensikt.

Resultatet av sikkerhetsrevisjon skal dokumenteres.

Sikkerhetsrevisjon er et viktig grunnlag for kontinuerlig forbedring av informasjonssikkerhet i virksomheten. Resultatet fra sikkerhetsrevisjonen vil være en del av grunnlaget for ledelsens gjennomgang jf. forskriften § 2-3.

2.3.2 Fakta

I intervju framkom det at det skal startes et arbeid med å utarbeide plan for informasjonssikkerhet, og gjennom dette utarbeide rutiner. Det har så langt ikke blitt gjennomført jevnlige sikkerhetsrevisjoner i Aukra kommune.

2.3.3 Kommunerevisjonens vurdering og anbefaling

Revisjonens undersøkelser viser at kommunen ikke har utarbeidet sikkerhetsstrategi eller beskrivelser av sikkerhetsmål. Undersøkelsen viser videre at Aukra kommunen ikke gjennomfører jevnlige sikkerhetsrevisjoner.

Oppgave med informasjonssikkerhet er lagt til Servicekontoret, og det er ansatt rådgiver som blant annet skal arbeide med dette. Det er positivt at det er besluttet at det skal startes et arbeid med å utarbeide plan for informasjonssikkerhet.

Anbefaling: Aukra kommune må utarbeide rutiner for sikkerhetsrevisjon, og gjennomføre jevnlige sikkerhetsrevisjoner.

2.4 Avviksbehandling

2.4.1 Revisjonskriterier

Revisjonskriterier: ***Aukra kommune har etablert avviksbehandlingssystem og behandler sikkerhetsbrudd som avvik***

Personopplysningsforskriften § 2-6 stiller krav om at det er etablert avviksbehandlings-system:

> *«Bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd, skal behandles som avvik».*

Det følger av forskriften § 2-6 at virksomheten skal ha rutiner for avvikshåndtering. Resultatet fra avviksbehandling skal dokumenteres. Etter forskriften § 2-8, 2. ledd skal medarbeidere ha nødvendig kunnskap for å bruke informasjonssystemet i tråd med de rutiner som er fastlagt. Det er således et krav til at de foreliggende rutiner må implementeres i virksomheten.

For de tilfeller der avvik har avdekket uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig, skal Datatilsynet orienteres.

2.4.2 Fakta

Aukra kommune har besluttet at det skal arbeides med informasjonssikkerhet. Arbeidet har stoppet opp, fordi kommunen avventer at ROR-IKT skal etablere en IKT gruppe. I den forbindelse ønsker Aukra kommune å avklare hvordan ansvar og roller skal fordeles mellom kommunen og ROR-IKT.

I 2014 har Aukra kommune arbeid med å etablere et helhetlig kvalitetssystem – Kvalitetslosen. Det opplyses i intervju at informasjonssikkerhet skal inngå som del av dette systemet. Noen rutiner og prosedyrer relatert til informasjonssikkerhet ble utarbeidet og lagt inn i dette systemet i 2014.

En viktig del av kvalitetssystemet er avvikssystemet. Det opplyses i intervju at avvik i forhold til informasjonssikkerhet skal meldes i Kvalitetslosen. Det ble opplyst at det er meldt avvik på dette området. 80 % av de ansatte har fått opplæring i Kvalitetslosen inkludert bruk av avviksmeldingssystemet. En rådgiver på Servicekontoret har hatt ansvar for gjennomføring av opplæringen.

I 2014 var opplæring i bruk av Kvalitetslosen prioritert. I 2015 er det fokus på risiko og sårbarhetsvurderinger, og utarbeidelse av dokumentmoduler. Enhetene har superbrukere som har fått særlig opplæring i Kvalitetslosen.

Det er ikke mottatt avvik knyttet til uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig. Aukra kommune har dermed ikke orientert Datatilsynet om slike saker.

2.4.3 Kommunerevisjonens vurdering og anbefaling

Aukra kommune har etablert et enhetlig kvalitetssystem. Det er positivt at ansatte i 2014 fikk opplæring i bruk av kvalitetssystemet, avvik og avviksmeldinger. I 2015 er det gitt opplæring i bruk av dokumentmodul. Opplæring i dokumentmodul omfatter arbeid med å utarbeide og legge inn overordnede planer, prosedyrer, retningslinjer etc. Det er viktig at ledelsens forventninger om at det meldes avvik implementeres i kommunen.

Aukra kommune skal framover arbeide med utarbeidelse av styrende dokumenter om informasjonssikkerhet. Når dokumenter og prosedyrer implementeres i organisasjonen, vil sannsynlighet for at avvik meldes økes.

Kommunerevisjonen registrerer at brudd i forhold til informasjonssikkerhet skal meldes i avvikssystemet i Kvalitetslosen. Det er positivt at kommunen velger et felles avvikssystem.

Anbefaling: Aukra kommune bør utarbeide og implementere rutiner for melding av avvik fra bestemmelser om informasjonssikkerhet. Ledelsen bør formidle klare forventninger om at det meldes avvik knyttet til informasjonssikkerhet.

2.5 Organisering av ansvars- og myndighetsforhold

2.5.1 Revisjonskriterier

Revisjonskriterier: ***Aukra kommune har en klar organisering med etablerte ansvars- og myndighetsforhold***

Personopplysningsforskriften § 2-7 stiller krav om en klar organisering med etablerte ansvars- og myndighetsforhold:

> *«Det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjons-systemet».*

Forskriften § 2-3 understreker at det er den behandlingsansvarlige som skal sørge for tilfredsstillende informasjonssikkerhet ved at det blant annet opprettes en sikkerhetsorganisering med klare roller, ansvar og myndighet. Forskriften § 2-7 understreker at det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemet.

2.5.2 Fakta

I intervju kom det fram at Aukra kommune mangler overordnede dokumenter om informasjonssikkerhet. Dette gjelder også informasjon om funksjon som behandlingsansvarlig. De som ble intervjuet antok at rådmann er behandlingsansvarlig i Aukra kommune, men kunne ikke vise til dokumentasjon som viser at rådmann er behandlingsansvarlig og hva dette innebærer. Avtale med ROR-IKT gir informasjon om behandlingsansvarlig, avtalen omtales under.

Behandlingsansvarlig er den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes, personopplysningsloven § 2 nr. 4. Behandlingsansvarlig skal blant annet sørge for: 1) sikkerhetsmål, sikkerhetsstrategi og akseptkriterier 2) sikkerhetsorganisasjon 3) dokumenterte rutiner og tekniske tiltak for oppfyllelse av sikkerhetsstrategi og akseptkriterier

I oppstartmøte ble det avklart hvilke dokumenter som var av særlig interesse for revisjonen å få tilgang til. Revisjonen fikk tilsendt en rekke dokumenter, jf vedlagt oversikt. I forhold til ansvars- og myndighetsforhold var tjenestenivåavtale mellom ROR-IKT og Aukra kommune datert 4.2.2015 særlig aktuell. Hensikten med avtalen er både å definere rollefordeling, ansvars- og myndighetsforhold mellom ROR-IKT og kommunen, og å angi tjeneste- og servicenivået ROR-IKT skal yte sine tjenestemottakere.

Kommunen har ansvar for å bekjentgjøre tjenestenivåavtalen og sikre etterlevelse av denne i egen organisasjon.

Avtalen har bestemmelser som avklarer roller, ansvar og myndighet relatert til informasjonssikkerhet mellom Aukra kommune og ROR-IKT. Det bestemmes at Aukra kommune har ansvar for å melde inn oppnevnelser av systemeier og systemansvarlige til ROR-IKT. ROR-IKT har ansvar for å revidere oversikten av oppnevnte systemeiere, systemansvarlige, koordineringsansvarlige og driftsansvarlige. Tjenestemottager er også ansvarlig for å melde fra om egne organisasjonsendringer slik at ROR-IKT kan tilpasse AD struktur og tilganger tilsvarende.

Avtalen gir følgende avklaringer av roller:

Behandlingsansvarlig (Aukra kommune)
Rådmann er behandlingsansvarlig etter personopplysningsloven, helseregisterloven og tilhørende forskrifter.

Databehandler (ROR-IKT)
Den som behandler personopplysninger på vegne av den behandlingsansvarlige, pol § 2 nr 5. ROR-IKT er definert som databehandler etter personopplysningsloven, helseregisterloven og tilhørende forskrifter.

Virksomhetsansvarlig (Aukra kommune)
Leder for den virksomheten der behandlingen foregår har på rådmannens vegne ansvar for at gjeldende bestemmelser følges.

Systemeier (Aukra kommune)
Systemeier er øverste leder for den/ de virksomheten(e) som bruker systemet, og tjenestemottager har ansvar for å oppnevne systemeier for alle fagsystemer som benyttes. Systemeier er/ har i forhold til informasjonssikkerhet det daglig ansvar for å oppfylle plikter som behandlingsansvarlig på vegne av rådmannen jfr. personopplysningsloven og retningslinjer for IKT-sikkerhet. Videre har denne ansvar for å utnevne systemansvarlig, og det overordnet ansvar for å gi egne brukere nødvendig opplæring i systemet.

Systemansvarlig (Aukra kommune)
Systemansvarlig har faglig ansvar for bruk og administrasjon av systemet og oppnevnes av tjenestemottagerens Systemeier. Systemansvarlig har den daglige forvaltningsansvaret for systemet og skal gjennom systemeier sine retningslinjer sikre at systemet er levedyktig og oppdatert. Systemansvarlig er/ har blant annet ansvar for:

- *Etablere og dokumentere system for vedlikehold og tildeling av brukertilganger.*
- *Etablere og dokumentere rutiner som er nødvendige i forhold til bruk av systemet.*
- *Etablere og dokumentere rutiner for sikker tjenesteytelse ved midlertidig systembortfall*

- *Deltaker i interkommunal faggruppe der det er etablert.*

Sikkerhetsansvarlig (Aukra kommune)
Sikkerhetsansvarlig har rådmannens fullmakt til å fatte bindende vedtak i spørsmål som angår informasjonssikkerhet og personvern. Sikkerhetsansvarlig er/ har blant annet:
- *Ansvar for implementering av beskrevne sikkerhetsrutiner i egen kommune*
- *Ansvar for integrering av sikkerhetsrutiner i kommunens øvrige kvalitetsarbeid.*

Driftsansvarlig (ROR-IKT)
ROR-IKT Driftsavdeling har ansvar for teknisk drift av systemene. Drift foregår i team, bestående av et server-, applikasjon- og nettverksteam. Driftsavdelingen har:
- *Ansvar for at den tekniske driften av systemet er ihht. gjeldende lovverk og retningslinjer for IT-sikkerhet.*
- *Ansvar for at oppgradering og drift av system er forsvarlig og i samsvar med gjeldende lover og retningslinjer*

Alle brukere (Aukra kommune)
Enhver person registrert i ROR-IKTs katalogtjeneste (ROR-IKTs oversikt over alle gyldige brukere) har fått tilgang til nettverket og er definert som Bruker. Brukere er/ har:
- *Pliktig til å sette seg inn i og følge veiledninger for bruken av informasjonssystemene.*
- *Pliktig til å sette seg inn og skrive under den til enhver tid gjeldende databrukeravtale/ sikkerhetsinstruks*

I intervjuer kom det fram at ovennevnte avklaringer er lite kjent. Dette hadde som følge at det er usikkerhet knyttet til ansvar og roller i Aukra kommune vedrørende informasjonssikkerhet. De som ble intervjuet hadde liten kunnskap om at tjenestenivåavtalen mellom ROR-IKT og Aukra kommune har bestemmelser om ansvars- og myndighetsforhold, og gjennom dette også bestemmelser om ansvar og roller på området informasjonssikkerhet i Aukra kommune.

Avtalen har bestemmelser om at Aukra kommune skal melde inn oppnevnelser av systemeier og systemansvarlige til ROR-IKT. ROR-IKT har ansvar for å revidere oversikten av oppnevnte systemeiere, systemansvarlige, koordineringsansvarlige og driftsansvarlige. Revisjonen har vært i kontakt med ROR-IKT, som opplyser at de per september 2015 ikke har mottatt informasjon om hvem som er systemeier og systemansvarlige.

2.5.3 Kommunerevisjonens vurdering og anbefaling

Kommunerevisjonen ser av mottatt dokumentasjon at rådmann har rolle som behandlingsansvarlig. Videre er det avklart at servicesjef har ansvar for å utøve det daglige arbeidet med informasjonssikkerhet.

I 2014 ble det opprettet en stilling på Servicekontoret som blant annet fikk oppgave med å ivareta informasjonssikkerhet. Stillingen innehar også funksjon som systemadministrator. Ansatt tiltrådte stillingen på ettersommeren 2014, og har det første året prioritert arbeid med implementering av Kvalitetslosen.

Mange avklaringer er tatt, men er i liten grad kjent blant ansatte som har funksjoner knyttet til informasjonssikkerhet. Aukra kommune kan med fordel klargjøre dokumenter og implementere disse i egen organisasjon.

Anbefaling: Aukra kommune bør utarbeide oppdatert organisasjonskartet i forhold til behandlingsansvaret etter personopplysningsloven, og gjennom dette tydeliggjør ansvarslinjene knyttet til informasjonssikkerhet.

2.6 Sikring mot uautorisert tilgang

2.6.1 Revisjonskriterier

Revisjonskriterier: Aukra kommune har fysisk sikring mot uautorisert tilgang

Personopplysningsforskriften § 2-10 stiller krav om fysisk sikring mot uautorisert tilgang:

> *«Det skal treffes tiltak mot uautorisert adgang til utstyr som brukes for å behandle personopplysninger...».*

Forskriften §§ 2-11, 2-12 og 2-13 stiller krav om at det gjennomføres tiltak som sørger for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet.

Forskriften § 2-14 pålegger at det skal innføres sikkerhetstiltak som skal hindre uautorisert bruk av informasjonssystemet og gjøre det mulig å oppdage forsøk på slik bruk. Videre pålegger forskriften § 2-8, 3. ledd og § 2-14 annet ledd at henholdsvis autorisert og uautorisert bruk av informasjonssystemet skal registreres.

2.6.2 Fakta

I oppstartmøte ble det avklart hvilke dokumenter som var av særlig interesse for revisjonen å få tilgang til. Revisjonen fikk tilsendt en rekke dokumenter, jf vedlagt oversikt. I forhold til temaene sikring mot uautorisert tilgang er følgende dokumenter særlig relevante: 1) databrukeravtale 2) tjenestenivåavtale mellom ROR-IKT og Aukra kommune datert 4.2.2015

Alle medarbeidere som har tilgang til informasjonssystemene, skal lese gjennom og signere en databrukeravtale. Den enkelte medarbeider skal ha utlevert et underskrevet eksemplar av databrukerkontrakten.

Gjennom inngåelse av databrukeravtale bekrefter den enkelte ansatt at han/ hun er kjent med sikkerhetsreglene ved behandling av personopplysninger, og IT- sikkerhetsreglene for Aukra kommune. Den ansatt forplikter seg til å følge bestemmelsene. Nærmeste leder skal også signere på avtalen, og bekrefter gjennom dette at reglene i avtalen blir fulgt i avdelingen.

I intervju kom det fram at Aukra kommune har nyttet databrukeravtaler de siste årene. Hovedregelen er at ansatte må skrive under på avtalen for å få tilgang til kommunens datasystem. Aukra kommune inngikk avtale med ROR-IKT om levering av IKT tjenester til kommunen med virkning fra 1.1.2014. I avtalen er det en forutsetning at nye ansatte må inngå databrukeravtale før disse får tilgang til kommunens datasystemer. I intervju framkom det at det noen ganger gis tilgang til datasystemene uten at databrukeravtale er signert.

I intervju kom det fram at det etter inngåelse av databrukeravtaler er lite fokus på avtalen. Enkelte av de som ble intervjuet antok at mange ansatte som har inngått avtale for mange år siden i liten grad er klar over dette, og derfor har liten kunnskap om innholdet i avtalen.

Enkelte som revisjonen intervjuet savner bestemmelser om jevnlige gjennomgang av avtalene, for eksempel som fast punkt på et avdelingsmøte en gang per år.

Det ble opplyst i intervjuer at opplæring og vedlikehold av kunnskap om informasjons-sikkerhet er tilfeldig etter at databrukeravtale er signert. De som gjennom profesjonslovgivning har særskilte krav om taushetsplikt har mer fokus på informasjonssikkerhet, dette gjelder særlig helsepersonell.

2.6.3 Kommunerevisjonens vurdering og anbefaling

Aukra kommune har innført sikkerhetstiltak som skal hindre uautorisert bruk av informasjonssystemet gjennom inngåelse av databrukeravtale med ansatte og tjenestenivåavtale med ROR-IKT.

I intervju framkom det at det er lite fokus på etterlevelse av databrukeravtalen etter at denne er inngått. Aukra kommune har ikke system som sikrer at alle ansatte jevnlig går gjennom databrukeravtalen og reflekterer rundt hvordan denne kan etterleves.

Aukra kommuner kan med fordel nytte veiledningsmateriale utarbeidet av Difi. Veilederen er tilgjengelig på Difi sine hjemmesider: http://internkontroll.infosikkerhet.difi.no

Anbefaling: Aukra kommune bør gjennomgå og revidere tiltak som er innført for å hindre uautorisert bruk av informasjonssystemene. Aukra kommune bør innføre system som sikrer at alle ansatte jevnlig går gjennom disse tiltakene.

2.7 Tiltak mot uautorisert innsyn

2.7.1 Revisjonskriterier

Revisjonskriterier: Aukra kommune har tiltak mot uautorisert innsyn

Personopplysningsforskriften § 2-11 stiller krav om tiltak mot uautorisert innsyn:

> *«Det skal treffes tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig».*

Forskriften §§ 2-11, 2-12 og 2-13 stiller krav om at det gjennomføres tiltak som sørger for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet. Forskriften § 2-14 annet ledd pålegger at uautorisert bruk av informasjonssystemet skal registreres.

2.7.2 Fakta

Tjenestenivåavtalen mellom Aukra kommune og ROR-IKT har bestemmelser om tiltak mot uautorisert innsyn. Enhver person registrert i ROR-IKTs katalogtjeneste og har fått tilgang til nettverket er definert som *bruker* og er/ har:

- *Pliktig til å sette seg inn i og følge veiledninger for bruken av informasjonssystemene.*
- *Pliktig til å sette seg inn og skrive under den til enhver tid gjeldende databrukeravtale/ sikkerhetsinstruks*

Aukra kommune har ikke dokumentert de risikovurderinger som er tatt for å hindre uautorisert innsyn, men de enkelte databrukeravtalene har bestemmelser som skal hindre uautorisert innsyn. Avtalene har blant annet bestemmelser om følgende tiltak:

- *Utstyr som nyttast til behandling av personopplysningar, skal vere sikra mot uautorisert tilgang m.a. ved bruk av passord som rullerast og ved låsing av rom. Medarbeidarar som forlet arbeidsplassen sin utan å logge seg av nettverk og/eller arbeidsstasjon (PC), skal kople inn skjermsperre.*
- *Sensitive personopplysningar skal ikkje sendast ved bruk av telefaks eller vanleg elektronisk post. Unnateke dersom prosedyrar for kryptering og dataoverføringar vert fulgt.*
- *Personopplysningar skal berre behandlast i databaser som tilfredsstiller Datatilsynets sikringskrav - ikkje som tekst- eller reknearkfiler o.l.. Behandling av personopplysningar kan berre gjerast på Aukra kommune sine serverar eller på utlevert PC dersom IT-driftsansvarleg spesielt har lagt til rette for dette teknisk og rutinemessig.*
- *Det er ikkje tillate å kopiere informasjon frå personregister til eigen PC eller å ta ut sensitive personopplysningar eller anna beskytta informasjon på ekstern lagringsmedium (t.d usb-penn, diskett eller tape).*
- *Personopplysningar skal ikkje lagrast på eksternt lagringsmedium. Dersom dette likevel er naudsynt, skal dei oppbevarast i låsbare skåp. Tilsendte lagringsmedium skal leverast til IT - driftsansvarleg for "virustesting" og kopiering til IT-systemet.*
- *Passord for skjermsperre, tilgang til nettverket og/eller for tilgang til ulike fagsystem og dokument, skal huskast eller oppbevarast slik at dei ikkje kjem uvedkomande i hende. Det er heller ikkje tilete å låne bort brukarkode og personlege passord til andre. Unngå å bruke namnet på ektefelle, barn, hunden, bilnummer eller anna som lett kan koplast til deg som passord.*
- *Brukarar skal hindre at ikkje autoriserte personar får utilsikta tilgang til systema og har plikt til å melde frå til næraste overordna om det skulle hende eller på anna mistanke.*
- *Pass på å tilpasse skjermen slik at andre personar ikkje får innsyn til skjermbildet gjennom vindauget eller døropningar. Dette er spesielt viktig på kontor med vindauge ut i korridor.*

Det opplyses i intervju at det ikke er mulig å hente ut informasjon fra sikker sone til minnepinner. Videre opplyses det at det ikke er mulig å kopiere til e-post fra sikker sone.

Mange ansatte nytter samme skriver. I samtaler kom det fram usikkerhet om alle skrivere er plassert slik at de sikrer at uvedkommende ikke får tilgang til utskrifter. Skrivere er tilrettelagt slik at ansatte kan nytte kode når de henter utskrifter fra skriver. Det ble i intervju opplyst at ansatte oppfordres til å nytte kode på skrivere, men at mange ikke nytter dette.

I intervju kom det fram at det er uklart for ansatte om og i tilfelle hvordan uautorisert bruk av informasjonssystemet registreres.

2.7.3 Kommunerevisjonens vurdering og anbefaling

Databrukeravtalen omtaler tiltak som skal hindre uautorisert innsyn i sensitive opplysninger. I intervju kom det fram at avtalen inngås med nye ansatte. Ut over inngåelse av avtale er det lite fokus på å etterleve de krav og forventninger som avtalen gir. Kommunen mangler system som sikrer at avtalen blir etterlevd.

Aukra kommune mangler system som sikrer at alle ansatte jevnlig går gjennom tiltak som skal hindre uautorisert innsyn i dokumenter.

Anbefaling: Aukra kommune bør utarbeide dokument(er) som tydeliggjør tiltak som skal hindre uautorisert innsyn. Videre bør det utarbeides system som sikrer implementering og vedlikehold av slik kunnskap.

2.8 Tilgang til personopplysninger

2.8.1 Revisjonskriterier

Revisjonskriterier: Aukra kommune sikrer tilgang til personopplysninger

Personopplysningsforskriften § 2-12 stiller krav om at kommunen sikrer tilgang til personopplysninger:

> *«Det skal treffes tiltak for å sikre tilgang til personopplysninger hvor tilgjengelighet er nødvendig».*

Forskriften §§ 2-11, 2-12 og 2-13 stiller krav om at det gjennomføres tiltak som sørger for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet. Personopplysningsforskriften § 2-12 stiller krav om at kommunen sikrer tilgang til personopplysninger.

Helsedirektoratet har utarbeidet en norm for informasjonssikkerhet i helse og omsorgstjenesten; *Normen*. *Normen* er et omforent sett av krav til informasjonssikkerhet basert på lovverket. En forutsetning for å kunne ta i bruk helsenett er at Aukra kommune tar i bruk Normen.

2.8.2 Fakta

Systemansvarlig i Aukra kommune har iht avtale med ROR-IKT faglig ansvar for bruk og administrasjon av systemet. Systemansvarlig har det daglige forvaltningsansvaret for systemet og skal gjennom systemeier sine retningslinjer sikre at systemet er levedyktig og oppdatert. Videre har vedkommende ansvar for:

- *Etablere og dokumentere system for vedlikehold og tildeling av brukertilganger.*
- *Etablere og dokumentere rutiner som er nødvendige i forhold til bruk av systemet.*
- *Etablere og dokumentere rutiner for sikker tjenesteytelse ved midlertidig systembortfall*
- *Bistå ROR-IKT ved behov for feilretting/ feilsøking.*

Driftsavdeling i ROR-IKT har ansvar for teknisk drift av systemene. Drift foregår i team, bestående av et server-, applikasjon- og nettverksteam. Driftsavdelingen har ansvar for at:

- *Tekniske drift av systemet er ihht. gjeldende lovverk og retningslinjer for IT-sikkerhet.*
- *Oppgradering og drift av system er forsvarlig og i samsvar med gjeldende lover og retningslinjer*

Aukra kommune har en rekke fagsystemer der taushetsbelagte opplysninger håndteres, jf omtale under punkt 2.2.2.

Fra 1.1.2014 har ROR-IKT iht avtale levert tilgang til fagsystemet fram til brukerpålogging. Brukernavn og passord til fagsystemet skal leveres av Systemansvarlige i Aukra kommune.

All oppgradering og vedlikehold av eksisterende systemer skal koordineres på tvers av kommunene og bestilles gjennom ROR-IKT servicedesk i god tid. Ved driftsproblemer i fagsystemet utover det som skal meldes leverandørens brukerstøtte har ROR-IKT et koordinerende ansvar.

I prosjektet har kommunerevisjonen vurdert informasjonssikkerhet knyttet til fagsystemet Acos CosDoc som nyttes i helse-, pleie- og omsorgtjenesten.

Aukra kommune opprettet høsten 2013 en prosjektstilling i forbindelse med innføring av helsenett/ e-melding. Prosjektstillingen fikk ansvar for å utarbeide manualer og lokale prosedyrer for bruk av CosDoc. I tillegg ble det arbeidet med utarbeidelse av rutiner for innføring av helsenett og e-melding. Prosjektstillingen hadde også ansvar for opplæring av ansatte.

Aukra kommune (PLO) starta med eMeldinger i 2014. Kommunen måtte ved innføring av eMeldinger signere på at kommunen forplikta seg til å bruke *Normen*. *Normen* må nyttes på grunn av utveksling av sensitiv informasjon. Det opplyses at ansatte har fått opplæring i hva som kreves når sensitiv informasjon skal håndteres. Kommunen har tidligere tatt i bruk eResept og SMS-tjeneste (helse).

I opplæring av ansatte i kommunen er det gitt informasjon om *Normen*. I intervju ble det opplyst at det ble gitt generell informert om systemet. Det er videre opplyst at *Normen* og tilhørende faktaark (rutiner) ikke er gjennomgått med ansatte.

2.8.3 Kommunerevisjonens vurdering

Intervju og dokumentgjennomgang tilsier at ansatte med berettiget behov for personopplysninger får tilgang til dette.

Det har vært hendelse der det har vært brudd på kabel til fastlandet og som følge av dette har de tilganger en normalt har til personopplysninger vært borte. Det er satt inn tiltak som skal sikre at nødvendig informasjon er tilgjengelig ved bortfall av tilgang til datasystemene. Tiltak som er innførte omfatter papirkopier av særlig aktuell informasjon om pasienter i hjemmetjenesten og i institusjonstjenesten.

2.9 Tiltak mot uautorisert endring av personopplysninger

2.9.1 Revisjonskriterier

Revisjonskriterier: ***Aukra kommune har tiltak mot uautorisert endring av personopplysninger***

Personopplysningsforskriften § 2-13 stiller krav om tiltak mot uautorisert endring av personopplysninger:

> «*Det skal treffes tiltak mot uautorisert endring av personopplysninger der integritet er nødvendig*».

Personopplysningsforskriften § 2-13 stiller krav om tiltak mot uautorisert endring av personopplysninger. Den behandlingsansvarlige skal hindre utilsiktet endring av

personopplysninger. Også informasjon om informasjonssystemet og om sikkerhetstiltak skal sikres mot uautorisert endring når dette er nødvendig for informasjonssikkerheten.

2.9.2 Fakta

ROR-IKT har i egenskap av å være kommunenes Databehandler, ansvaret for datasikkerheten. Dette er avklart gjennom Tjenestenivåavtale mellom ROR-IKT og Aukra kommune. Med datasikkerhet menes det «å sikre at informasjon ikke er tilgjengelig uten autorisasjon (konfidensialitet), at informasjon ikke uautorisert endres eller ødelegges (integritet), og at informasjon er til stede og anvendelig for medarbeidere slik at pålagte oppgaver kan utføres (tilgjengelighet).»

I tillegg til å sikre sentralt lagrede data ved hjelp at backupløsninger har ROR-IKT også følgende sikkerhetskontroller:

- Antivirus: Alle servere og PCer har antivirusbeskyttelse. Dette skal sikre mot virusangrep både internt og eksternt. Systemet oppdateres automatisk. ROR-IKT rapporterer årlig antall virusangrep stoppet/ ikke stoppet.
- Innholdskontroll: Sentralt installert programvare hindrer tilgang til uønskede websider og bruk av uønskede applikasjoner. Dette gjelder også ved bruk av arbeidsgivers PC utenfor ROR-IKTs nettverk.
- E-postvasking: Sentralt installert programvare fjerner uønsket masseutsendt e-post (spam). ROR-IKT rapporterer årlig antall spammail stoppet/ ikke stoppet.

For spørsmål knyttet til informasjonssikkerhet og personvern henvises det i tjenestenivåavtalen til kommunens data/ informasjonssikkerhetsansvarlige.

Det understrekes i tjenestenivåavtalen at bruker ikke skal oppgi passord til andre, heller ikke til ROR-IKT Servicedesk ved behandling av supportsaker.

I kapittel 2.2.2 er det redegjort for vurderinger som er tatt for å avklare hvilke opplysninger som det skal sikres integritet for, og hvilke sikkerhetstiltak som må etableres.

2.9.3 Kommunerevisjonens vurdering og anbefaling

Aukra kommune har innført tiltak som skal hindre uautorisert endring av personopplysninger. Dette er særlig ivaretatt i avtale med ROR-IKT. Intervju og dokumentgjennomgang viser at det gjenstår noe arbeid med å implementere sikkerhetsarbeid i egen organisasjon.

Anbefaling: Aukra kommune bør gjennomgå og revidere tiltak som skal hindre uautorisert endring av personopplysninger. Aukra kommune bør innføre system som sikrer at alle ansatte jevnlig får vedlikeholde og oppdatere kunnskap om dette.

3 Posthåndtering i Aukra kommune

3.1 Problemstilling og revisjonskriterier

Kontrollutvalget ønsker at rutiner for Postmottaket i Aukra kommune omtales som del av forvaltningsrevisjonsrapporten. Kommunerevisjonen har valgt noen revisjonskriterier som posthåndtering i Aukra kommune er vurdert mot.

Problemstilling
Har Aukra kommune tilfredsstillende posthåndtering?

Revisjonskriterier
Revisjonen har utledet revisjonskriterier etter forvaltningslovens § 18, 23 og 27, eForvaltningsforskriften, arkivlova § 1 og arkivforskrifter §§ 2-6, 3-1, 3-3, 3-5, 3-6, 3-9, 3-10 og 3-11. Utledningen fremkommer av vedlegg til rapporten.

Revisjonen har undersøkt fem områder.

1. Aukra kommune har utarbeidet dokumenthåndteringsrutiner som omhandler mottak og åpning av vanlig post, og arkivbegrensning
2. Aukra kommune har elektronisk arkiv. Når kommunen mottar saksdokumenter på annet medium, sørger en for at slike dokumenter skannes og arkiveres.
3. Aukra kommune journalfører saksdokumenter i journal før de går til saksbehandling. Dette gjelder også hastesaker.
4. Aukra kommune har kopibok - eller elektroniske lagrede saksdokumenter - som inneholder kopi av alle undertegnede dokumenter som er sendt ut, og har rutiner for hvem som har ansvar for at dokumenter kommer i kopiboka/ elektronisk saksarkiv.
5. Aukra kommune har avklart hvordan kommunen skal forholde seg til elektronisk kommunikasjon, og gjennom dette forebygge risiko og informere brukere om risiko ved bruk av elektronisk kommunikasjon.

3.2 Fakta

Aukra kommune har utarbeidet en rekke prosedyrer og sjekklister som skal sikre forsvarlig posthåndtering. Rutinene er i hovedsak gitt i arkivplan for Aukra kommune. Rutinene i arkivplanen er retningsgivende for dokumentbehandling. Målsetning er å få en kontrollert håndtering av posten slik at kommunen har oversikt over sin fullstendige dokumentproduksjon. Rutinene/ retningslinjene skal sikre at krav i forskriftene til arkivlova kapittel III etterleves. Arkivplanen er nettbasert.

Arkivleder har utarbeidet prosedyrer og sjekklister for håndtering av inngående post og utgående post. Aukra kommune har rutine for postmottak, journalføring og sjekkpunktliste for vurdering av om dokument er unntatt offentlighet. I samtaler kom det fram at rutinene for postmottak er kjent blant ansatte i postmottaket og merkantilt ansatte ute i enhetene og ledergruppen.

Fram til 30.6.2015 håndterte enhetene som er lokalisert utenfor kommunehuset sin egen post. Aukra kommune etablerte 1.7.2015 et felles postmottak for alle enhetene i kommunen, med unntak av helse, legekontor og NAV. Postmottak er lokalisert i servicekontoret.

Hovedoppgaven med å håndtere post og arkivtjenesten løses av ansatte på servicekontoret. Det er etablert en felles rutine for dette området. Rutinen er under oppdatering.

Avdelingene har også etter 1.7.2015 egne merkantilt ansatt som utfører deler av arbeidet etter at dokument er: 1) stemplet mottatt 2) skannet 3) lagt i aktuell importsentral. Arkivet fører sak i ePhorte for avdelingene på kommunehuset, og avdelingene utenfor kommunehuset gjør dette selv.

Ansvar for leder, saksbehandler og arkivtjenesten
I mottaksprosessen har arkivtjenesten ansvar for å registrere all inngående post som tilhører journalenheten. I forbindelse med å sende ut post skal arkivtjenesten, når saksbehandler ikke ekspederer sine dokument selv, kontrollere registeropplysningene på de utgående brevene. Ellers blir dette gjort ved kvalitetssikring av postjournal.

I forbindelse med oppbevaring har arkivtjenesten ansvar for: 1) Avslutte saker etter melding fra saksansvarlig 2) Kontinuerlig kvalitetssikring av arkiv og dokumentbehandling gjennom jevnlig oppfølging av saksbehandlerne og å utføre kontroller i sak- og arkivsystemet 3) Til en hver tid kunne gi tilstrekkelig opplysninger om kommunen sine arkiv og innholdet 4) Se til at dokumentasjon av arkivrutiner og arkivsystem blir tatt vare på for ettertiden.

I mottaksprosessen skal saksbehandler kontrollere registeropplysningene på saker og dokument en er ansvarlig for, opplysninger som for eksempel dokumentkategori, avsender.

I prosessen med å sende ut post skal saksbehandler knytte dokumentet til en allerede eksisterende saksmappe eller reservere ny sak dersom det ikke eksisterer saksnummer fra før på dette emnet. Registrere alle utgående dokument med tilhørende vedlegg i sak- og arkivsystemet. Endre status til ferdigstilt på egne dokument etter hvert før utsending.

Åpning og sortering av post – felles postmottak
All sakspost som ikke skal behandles i eget fagsystem, skal sendes felles postmottak.
Saksposten fra ytre enheter sendes daglig til rådhuset (felles postmottak).
Med post menes dokumenter uavhengig av forsendelsesmåte (brev, e- post, fax, skjema, innskannede dokumenter osv.) Postmottak henter ut post som er kommet på faks og har ansvar for at e-post sendt til post@aukra.kommune.no blir journalført.
Telefaks og elektronisk post (e-post) skal behandles som vanlig post. De skal derfor vurderes og behandles etter de samme kravene som til et saksdokument som vanlig post.

Posten sorteres i arkivverdig og ikke arkivverdig post. Arkivverdig post er dokumenter som er gjenstand for saksbehandling eller har verdi som dokumentasjon. Tilfredsstilles disse kravene, blir det regnet som sakspost og går til skanning og journalføring. Ikke arkivverdig post er trykksaker, offentlige publikasjoner, rundskriv, kurs- og konferansetilbud, reklame, årsmeldinger/ rapporter fra andre offentlige institusjoner

Kommunen har felles mottak for e-post til virksomheten: post@aukra.kommune.no.
Denne e-post kontoen blir sjekket flere ganger per dag og arkivverdig post blir journalført av felles postmottak.

Saksbehandler er ansvarlig for at inngående og utgående post blir journalført. Dette gjelder både brevpost og e-post som ikke har vært innom felles postmottak. Saksbehandlerne er også ansvarlig for å vurdere om journalført post er ført i rett mappe og er sendt til rett mottaker.

Enkelte ganger blir hastesaker kopiert eller skannet og sendt videre til saksbehandler, før journalføring. Originaldokument følgjer vanlige registreringsrutiner.

Alle inngående dokumenter skal påføres stempel som inneholder kommunenavn og dato før dokumentene blir skannet. Saksvedlegg som ikke lar seg skanne skal stemples med eget stempel og påføres journalopplysninger, arkivkode og saksbehandler.

Saksdokumenter som er mottatt på papir skannes for å gi alle brukere snarest mulig tilgang til informasjon.

Postjournal
Postjournal publiseres på kommunens nettsider med fire dagers forsinkelse. Dokumenter skal kvalitetssikres av arkivet før utlegging. Stemplet papirbaserte dokument påføres mottatt dato og skannes.

Dokumenta skal deretter journalføres i aktuelle sak- og arkivsystem med: 1) Dokumentdato og mottattdato 2) Saks- og dokumentnummer 3) Eventuelle prosesstyringsverdier (om saka er reservert, under behandling, midlertidig journalført etc.) 4) Avsender/ mottaker 5) Klausulering (den som journalfører kommer med forslag til eventuell gradering og hjemmel for dette) 6) Saksbehandler 7) Klassering, ordningsverdi (saksnivå og arkivnøkkel) 8) Dokumentstatus (J = Journalført av arkivet)

Sakarkivet er fullelektronisk og papiroriginalen blir oppbevart i kort periode før makulering. Den som journalfører skal kontrollere om brev inneholder eventuelt vedlegg som det er vist til. Skulle disse mangle skal vedkommende ta kontakt med avsender for ettersending.

All post stilet til Aukra kommune blir åpnet. Dette gjelder også personlig adressert post der personnavn er oppgitt før Aukra kommune.

Feilsendt post blir sendt videre til rette adressat eller returnert til avsender. Det skilles mellom post som skal registreres i kommunens sak- og arkivsystem og post som skal registreres i fagsystem. Post til fagsystem blir viderefordelt til aktuelle enheter for nødvendig registrering.

Eventuell klient/ pasientpost til journalenheten med konsesjonspliktig personregister (PPT-kontor, sosialavdeling og barnevernavdeling) skal førest i egne postjournaler knyttet til fagsystem.

Behandling av e-post
Aukra kommune nytter Microsoft outlook til å sende e-post både internt og eksternt.
E-post til Aukra kommune skal primært sendes til og håndteres av postmottaket på e-postadresse: post@aukra.kommune.no E-post til journalførende enheter utenfor kommunehuset blir sendt videre til disse for journalføring. E-post kan også sendes til den enkelte definert bruker av outlook.

Håndtering av inngående e-post
E-post til sentralt postmottak blir åpnet av serviceavdelingen (arkivforskriften § 3, 2. ledd).
Den ansvarlige for journalføring må ta stilling til om melding, vedlegget eller begge deler er arkivverdig. All arkivverdig e-post skal journalføres i sak- og arkivsystemet (egne rutiner) og blir på den måten fordelt.

Dersom den enkelte saksbehandler mottar e-post som er dokumentasjon i en sak, plikter han å

vurdere om posten er arkivverdig. Arkivverdig post skal han overføre/ eksportere til rette saksmappe eller sende videre til postmottak for journalføring.

Kvittering for mottak av e-post
Aukra kommune nytter ikke automatisk kvittering for mottak av e-post. Det er saksbehandler sitt ansvar å gi tilbakemelding dersom avsender ønsker bekreftelse på mottak av e-post.

Håndtering av utgående e-post
Arkivverdig utgående post skal som hoved regel sendes som ordinær post, men kan i tillegg sendes som e-post, som en foreløpig melding. Kommunen har ordning med utstrakt delegasjon og fullført saksbehandling. Saksbehandler kan selv gjøre dette for sine dokument ved hjelp av funksjonalitet i sak- og arkivsystemet. Saksbehandler er ansvarlig for å kontrollere at sakspost som vedkommende sender som e-post, blir registrert i sak- og arkivsystemet. Hovedregelen er at all utgående sakspost skal opprettes i sak- og arkivsystemet.

Taushetsbelagte opplysninger
Opplysninger som er underlagt lovbestemt taushetsplikt i forhold til offentleglova § 13 og andre lovhjemler skal ikke sendes som e-post. Unntak kan være aktuelt dersom personopplysningene anonymiseres, slik at det ikke er mulig å knytte opplysningene til enkeltpersoner.

E-postrutiner ved saksbehandler sitt fravær
Saksbehandler må sikre at mottatt e-post kan behandles også ved fravær over lengre tid. Dette gjøres ved bruk av funksjon i e-postsystemet for automatisk svar. Med hjelp av fraværsassistenten i outlook legger en inn opplysninger om fraværets lengde og adresse til kommunen sitt postmottak, post@aukra.kommune.no. Det er mulig å legge ulike meldinger til interne og eksterne avsendere.

Arbeidsgiver sin tilgang til ansatte sin e-post og oversikt over bruk av e-postsystemet
Lov om personopplysninger, forskrifter til denne lova, samt Datatilsynets retningslinjer regulerer tilgang til ansatte sin e-post og andre elektroniske dokument, jfr. databrukeravtale for Aukra kommune.

Utgående post – daglig postavlevering
Det er ikke adgang til å produsere dokument uten å knytte denne til en postjournal. All dokumentproduksjon skal skje i sak- og arkivsystem eller fagsystem dersom bruker er knyttet til slike system. Saksbehandler er ansvarlig for registrering av utgående korrespondanse.

Saksbehandler har ansvar for å knytte sine dokument til riktig saksnummer. Eksisterer det ikke sak fra før, skal saksbehandler be arkivet om å opprette en sak. Vedkommende har anledning selv til å reservere sak/ mappe i sak- og arkivsystemet. Status i sak blir da automatisk R (reservert) og saksbehandler skal varsle arkivet om at det er gjort, slik at arkivet får fullført den registrering som er påkrevd.

Når dette er gjort og det er klart for å opprette ny journalpost skal følgende opplysninger registreres av saksbehandler: 1) Tittel/ innhold 2) Adressat 3) Eventuelt unntak for offentlighet og skjerming av enkelte opplysninger 4) Registrere eventuelle vedlegg

Når dokumentet er ferdigstilt, skal saksbehandler endre dokumentstatus fra R (reservert) til F (ferdigstilt av saksbehandler).

Registrering av interne dokument
I kraft av arkivforskriften § 2-6 vurderer kommunen selv hvilke interne dokument som skal registreres i journalen. Aukra kommune definerer seg som flere organ og har følgende journalføringsrutiner for interne dokument: 1) Internpost skal behandles som eksternpost 2) For korrespondanse mellom enhetene som er tilknyttet samme Noark-base, nytter en dokumenttypene X og N. Er den ene enheten ikke knyttet opp mot basen, nytter en dokumenttypene U og I som for ekstern korrespondanse.

3.3 Kommunerevisjonens vurdering og anbefaling

Hovedformålet med undersøkelsen har vært å undersøke om Aukra kommunes behandling av inn- og utgående post er i samsvar med bestemmelsen i forvaltningsloven, offentlighetsloven og arkivloven med tilhørende forskrifter. Prosjektet har hatt utgangspunkt i postbehandlingen ved felles postmottak som ble etablert 1.7.2015.

Arkivtjenesten mottar dokumenter, stempler mottatt, skanner og legger dokument i importsentral for aktuell avdeling. Den enkelte avdeling har ansvar for videre håndtering, inkludert vurdering og fastsettelse av hjemmel for å unnta dokumentet offentlighet.

Aukra kommune har utarbeidet dokumenthåndteringsrutiner som omhandler mottak og åpning av vanlig post, og arkivbegrensning. Når kommunen mottar saksdokumenter på annet medium, sørger en for at slike dokumenter skannes og arkiveres. Kommunen har et elektronisk arkiv og journalfører saksdokumenter i journal før de går til saksbehandling. Dette gjelder også hastesaker.

Aukra kommune har avklart hvordan kommunen skal forholde seg til elektronisk kommunikasjon, og gjennom dette forebygge risiko og informere brukere om risiko ved bruk av elektronisk kommunikasjon.

All post stilet til Aukra kommune blir åpnet. Dette gjelder også personlig adressert post der personnavn er nevnt før Aukra kommune. Kommunerevisjonen viser til arkivforskriften § 3-1, 2. ledd som bestemmer at post hvor mottakers navn er angitt før kommunenavn defineres som personlig post. Slik post skal som hovedregel leveres uåpnet til saksbehandler. Personlig post kan åpnes av kommunen/ arkivpersonalet når den enkelte saksbehandler har gitt skriftlig fullmakt til dette.

Anbefaling: Aukra kommune bør endre praksis gjeldende post hvor mottakers navn er angitt før kommunenavn. Slik post skal sendes uåpnet til navngitt mottaker.

4 Oppsummering, samlede vurderinger og anbefalinger

Aukra kommune har nylig etablert et helhetlig kvalitetssystem: Kvalitetslosen.

Aukra kommune har ikke egen plan og strategi for informasjonssikkerhet, men kommunen har dokumenter som sier noe om databruk og taushetsplikt. Aukra kommune har startet arbeidet med en kvalitetshåndbok, og har laget en kvalitetsplakat som viser kva kommunen har arbeidet med når det gjeld overordnet internkontroll.

Kommunen gikk inn i et interkommunalt samarbeid på IKT-området fra 1.1.2014, og driftsansvaret ble lagt til ROR-IKT. ROR-IKT ble etablert etter vedtak i medlemskommunene

Aukra, Midsund, Molde, Rauma og Vestnes. Bakgrunnen for etableringen var erkjennelsen av at kommunene måtte stå sammen om å løse utfordringene på IKT-området og for å dempe utviklingen i driftskostnadene ved å ta ut stordriftsfordeler.

I intervju framkom det at det skal startes et arbeid med å utarbeide plan for informasjons-sikkerhet, og at det gjennom dette skal utarbeides rutiner for informasjonssikkerhet. ROR-IKT har utarbeidet dokumenter som vil ha innvirkning på dette arbeidet.

Oppgaver knyttet til IKT var fram til og med 2013 lagt til Personalavdeling, fra 2014 er dette ivaretatt av ROR-IKT. I 2014 ble det lyst ut stilling i Aukra kommune som rådgiver for digitaletjenester, inkludert oppgaver knyttet til Kvalitetslosen og informasjonssikkerhet. Det er ikke klart definert hva dette arbeidet omfatter. Stillingen ble besatt høsten 2014, og stillingsinnehaver har hittil hatt hovedfokus på innføring av Kvalitetslosen. Stillingsinnehaver har deltatt på kurs og har startet et arbeid med å avklare oppgaver knyttet til informasjonssikkerhet.

Tjenestenivåavtale mellom ROR-IKT og Aukra kommune gir avklaringer av ansvars- og myndighetsforhold i Aukra kommune gjeldende informasjonssikkerhet. Det er blant annet avklart at rådmann i Aukra kommune er behandlingsansvarlig iht personopplysningsloven. Aukra kommune har ansvar for å bekjentgjøre tjenestenivåavtalen og sikre etterlevelse av denne i egen organisasjon. Avtalen og innholdet i denne er i liten grad kjent og implementert i Aukra kommune. Det framgår ikke av delegasjonsskriv hvordan og hvem som ivaretar arbeid med informasjonssikkerhet. Informasjonssikkerhet er ikke omtalt i politisk- eller administrativt delegasjonsskriv.

Alle medarbeidere i Aukra kommune som har tilgang til informasjonssystemene, skal lese gjennom og signere en databrukeravtale. Gjennom inngåelse av databrukeravtale bekrefter den enkelte ansatt at han/ hun er kjent med sikkerhetsreglene ved behandling av personopplysninger, og IT-sikkerhetsreglene for Aukra kommune. Den ansatt forplikter seg til å følge bestemmelsene. Kommunen har ikke system for å gjennomgå og revidere tiltak som er innført for å hindre uautorisert bruk av informasjonssystemene. Aukra kommune har ikke system som sikrer at alle ansatte jevnlig går gjennom tiltakene og får oppdatert kunnskap på området.

Aukra kommune avventer sitt arbeid med informasjonssikkerhet. Dette gjøres fordi kommunen ønsker å samordne dette med det arbeid som ROR-IKT skal gjennomføre. I følge digitaliseringsstrategien som ROR-IKT har utarbeida, skal det etableres en faggruppe som skal jobbe med informasjonssikkerhet. Dokumenter utarbeidet av ROR-IKT tilsier at ansvar for informasjonssikkerhet må ivaretas av den enkelte kommune.

Intervjuer og dokumentgjennomgang viser at Aukra kommune har startet arbeid med informasjonssikkerhet. Det gjenstår imidlertid arbeid før kommunen har en tilfredsstillende informasjonssikkerhet.

All post stilet til Aukra kommune blir åpnet. Dette gjelder også personlig adressert post der personnavn er nevnt før Aukra kommune. Aukra kommune bør endre praksis, og sende post uåpnet til navngitt mottaker. Alternativt kan kommunen inngå avtale med den enkelte saksbehandler om at kommunen kan åpne personlig adressert post.

Anbefalinger
Med utgangspunkt i de funn som er gjort i denne undersøkelsen gir revisjonen følgende anbefalinger knyttet til informasjonssikkerhet:

1. Aukra kommune bør sikre at det utarbeides sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet og implementere dette i egen organisasjon.

2. Aukra kommune bør klargjøre arbeidsdeling gjeldende informasjonssikkerhet med ROR-IKT.

3. Aukra kommune bør utarbeidet en enkel oversikt over de personopplysninger som behandles i kommunen. Oversikten bør gjøres kjent for de med ansvar for informasjonssikkerhet og aktuelle ansatte i organisasjonen.

4. Aukra kommune bør utarbeide rutiner for sikkerhetsrevisjon, og gjennomføre jevnlige sikkerhetsrevisjoner.

5. Aukra kommune bør utarbeide og implementere rutiner for melding av avvik fra bestemmelser om informasjonssikkerhet. Ledelsen bør formidle klare forventninger om at det meldes avvik knyttet til informasjonssikkerhet.

6. Aukra kommune bør utarbeide oppdatert organisasjonskartet i forhold til behandlingsansvaret etter personopplysningsloven, og gjennom dette tydeliggjør ansvarslinjene knyttet til informasjonssikkerhet.

7. Aukra kommune bør gjennomgå og revidere tiltak som er innført for å hindre uautorisert bruk av informasjonssystemene. Aukra kommune bør innføre system som sikrer at alle ansatte jevnlig går gjennom disse tiltakene.

8. Aukra kommune bør utarbeide dokument(er) som tydeliggjør tiltak som skal hindre uautorisert innsyn. Videre bør det utarbeides system som sikrer implementering og vedlikehold av slik kunnskap.

9. Aukra kommune bør gjennomgås og revideres tiltak som skal hindre uautorisert endring av personopplysninger. Aukra kommune bør innføre system som sikrer at alle ansatte jevnlig får vedlikeholde og oppdatere kunnskap om dette.

På området posthåndtering i Aukra kommune gis en anbefaling:

10. Aukra kommune bør endre praksis gjeldende post hvor mottakers navn er angitt før kommunenavn. Slik post skal sendes uåpnet til navngitt mottaker.

Molde, 9. november 2015

Einar Andersen
oppdragsansvarlig forvaltningsrevisor

Anny Sønderland
forvaltningsrevisor

Referanser og kilder

- Lov om behandling av personopplysninger (personopplysningsloven) 1.1.2001
- Forskrift om behandling av personopplysninger (personopplysningsforskriften) 1.1.2001
- En veileder om internkontroll og informasjonssikkerhet, Datatilsynet (november 2009)
- Veiledning i informasjonssikkerhet for kommuner og fylkeskommuner, Datatilsynet (januar 2005)
- Risikovurdering av informasjonssystemer, Datatilsynet (februar 2002)
- Sikkerhetsbestemmelsene i personopplysningsforskriften, Datatilsynet (desember 2000)
- Anbefalinger til God IT-skikk (GITS)
- COBIT – Control Objectives for Information and Related Technology

- Internkontroll i Aukra kommune (Politisk sak vedrørende valg av internkontrollsystem)
- Databrukeravtale
- Erklæring om teieplikt
- Kvalitetshandbok for Aukra kommune
- Kvalitetsplakat
- ROS-analyse for kommunehuset
- Digitaliseringsstrategi
- Rutiner for arkivering av personalmapper
- Rutiner for elektronisk personalarkiv
- Barnehagemapper
- Elevmapper
- Normen
- Prosedyrar knytt til informasjostryggleik
- Leiaren sitt ansvar i Kvalitetslosen
- Manual for avviksbehandling for leiarar
- Manual for avvikmelding for tilsette
- Deltakarliste superbrukaropplæring kvalitetslosen
- Referansegruppe kvalitetslosen
- Program superbukaropplæring avvik
- Program opplæring i risikostyring
- Internopplæring av dei tilsette
- Delegeringsreglementet
- Rutiner for felles postmottak
- Rutine postmottak, journalføring
- Sjekkpunktliste til offentlegsvurdering
- Fagsystem systemansvarleg (ROR-IKT)
- Organisasjonsskisse (ROR-IKT)
- SLA (tenestenivåavtale) (ROR-IKT)
- Arkivplan for Aukra kommune
- Rettleiar ePhorte

Vedlegg 1: Høringsuttalelse fra rådmann

Aukra kommune

Andersen Einar

Vår ref.:	Dykkar ref.:	Saksbehandlar:	Dato:
2015/858-12/060		Aaslaug Søreide	05.11.2015

Svar på utkast til høyringsrapport - Forvaltningsrevisjon om informasjonstryggleik

Vi viser til høyringsbrevet gjeldande «Forvaltningsrevisjonsrapport om Informasjonssikkerhet i Aukra kommune» og kan i hovudsak seie oss einig i dei utfordringane som den omhandlar.

Vi arbeider med å få på plass fleire av dei anbefalte punkta som er nemnt i rapporten. Mykje er under arbeid og også planlagt gjennomført dette året og i 2016.

Rådmannen legg vekt på å få nemnte anbefalingar på plass i Aukra kommune.

Med helsing

Ingrid Husøy Rimstad
Rådmann

Aaslaug Søreide
Servicesjef

Postadresse	Besøksadresse	Telefon	Bank
Aukraringen 25	Aukraringen 25	71 17 15 00	9650.26.60192
6480 Aukra	**Org.nr.** 964 981 337	**Telefaks**	**Bankkto. skatt**
E-post: post@aukra.kommune.no	www.aukra.kommune.no	71 17 15 01	6345 06 15473

Vedlegg 2: Problemstilling og revisjonskriterier

Tema 1: Informasjonssikkerhet i Aukra kommune

Problemstilling
Har Aukra kommune tilfredsstillende informasjonssikkerhet, som sikrer krav til konfidensialitet, integritet og tilgjengelighet?

Revisjonskriterier

1. ***Aukra kommune har etablert sikkerhetsledelse, sikkerhetsmål og sikkerhetsstrategi***
   Personopplysningsforskriften § 2-3 stiller krav om at det er etablert en sikkerhetsledelse:

   «Den som har den daglige ledelsen av virksomheten som den behandlingsansvarlige driver, har ansvar for at bestemmelsene i dette kapittelet følges».

   Kommentar fra Datatilsynet:
   Bestemmelsen understreker at det er den behandlingsansvarlige, ved virksomhetens daglige ledelse, som skal sørge for tilfredsstillende informasjonssikkerhet, jf. personopplysningsloven § 13, og dermed har ansvar for at bestemmelsene i dette kapittelet følges.

   Virksomhetens ledelse skal utøve dette ansvaret blant annet ved å beskrive virksomhetens sikkerhetsmål. Sikkerhetsmål vil omfatte beslutninger om til hva, og hvordan informasjonsteknologi skal benyttes i virksomheten. Eksempler på slike beslutninger kan være valg av hvilke behandlinger av personopplysninger som skal skje med elektroniske hjelpemidler, hvordan virksomheten forholder seg til opplysninger som må sikres både med hensyn til konfidensialitet og tilgjengelighet, og føringer for medarbeideres eventuelle private bruk av informasjonssystemet.

   Videre skal virksomhetens ledelse beskrive valg og prioriteringer i sikkerhetsarbeidet i en sikkerhetsstrategi. Sikkerhetsstrategien vil omfatte grunnleggende beslutninger om organisering og gjennomføring av sikkerhetsarbeidet. Eksempler på slike beslutninger kan være fordeling av arbeidsoppgaver for drift og informasjonssikkerhet mellom ledelse, drifts- og sikkerhetspersonell og den enkelte bruker, eventuelt krav til at konfidensielle personopplysninger behandles i informasjonssystem uten tilkobling til eksterne datanett, og bruk av leverandører for å få utført sikkerhetsoppgaver.

   Virksomhetens ledelse skal jevnlig, eksempelvis årlig, gjennomgå sikkerhetsmål og strategi. Slik ledelsesgjennomgang vil ha som formål å vurdere hvorvidt de beslutninger som er tatt, er i samsvar med virksomhetens behov for informasjonsteknologi og informasjonssikkerhet. Gjennomgangen vil danne grunnlag for eventuelle endringer av sikkerhetsmål eller strategi. Praktisk kan ledelsesgjennomgang gjennomføres innenfor rammen av årlig økonomi- eller virksomhetsplanlegging.

2. ***Aukra kommune har tilstrekkelig oversikt over personopplysninger som behandles***
   Personopplysningsforskriften § 2-4 stiller krav om at kommunen har tilstrekkelig oversikt over de personopplysninger som behandles:

   «Det skal føres oversikt over hva slags personopplysninger som behandles».

Kommentar fra Datatilsynet:
Bestemmelsen pålegger den behandlingsansvarlige å holde oversikt over de personopplysninger som behandles med elektroniske hjelpemidler, sammen med angivelse av hvilke opplysninger det er nødvendig å sikre konfidensialitet, tilgjengelighet eller integritet for. Oversikten benyttes som del av grunnlaget for risikovurderingen.

Den behandlingsansvarlige skal fastlegge kriterier for den risiko som kan aksepteres, eller eventuelt må reduseres ved hjelp av sikkerhetstiltak. Slike beslutninger kan overprøves i de tilfeller der Datatilsynet ikke finner informasjonssikkerheten tilfredsstillende, jf. § 2-2.

Den behandlingsansvarlige skal klarlegge sannsynlighet for, og konsekvens av sikkerhetsbrudd ved hjelp av risikovurdering. Begrepet "risikovurdering" er valgt i stedet for den mer formelle betegnelsen "risikoanalyse". Dette for å signalisere at arbeidet med å avdekke risiko ikke bør være mer omfattende eller formalisert en strengt tatt nødvendig.

Begrepet "risikovurdering" er også valgt i stedet for "sårbarhetsanalyse" som normalt benyttes kun til å beskrive vurdering av motstandsdyktighet mot uønskede hendelser.

Risikovurdering skal gjennomføres før behandling av personopplysninger med elektroniske hjelpemidler settes i gang, og deretter ved endringer med betydning for informasjonssikkerheten. Dette kan være endringer som følger av beslutninger hos den behandlingsansvarlige, eller hendelser den behandlingsansvarlige ikke har herredømme over, eksempelvis endringer i trusselbildet, feil i standard programvare eller lignende.

Risikovurdering kan utføres med utgangspunkt i norsk standard *NS-5814, Krav til risikoanalyser*. Resultat av risikovurdering skal sammenlignes med de fastlagte kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger. Resultatet benyttes som del av grunnlaget for valg av de konkrete sikkerhetstiltak som må etableres.

3. Aukra kommune gjennomfører jevnlig sikkerhetsrevisjon

Personopplysningsforskriften § 2-5 stiller krav om at det gjennomføres jevnlig sikkerhets revisjon:

«Sikkerhetsrevisjon av bruk av informasjonssystemet skal gjennomføres jevnlig».

Kommentar fra Datatilsynet:
Bestemmelsen pålegger den behandlingsansvarlige jevnlig, eksempelvis årlig, å etterprøve sikkerhetsarbeidet for å verifisere 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. Slik revisjon må ikke blandes sammen med ledelsens gjennomgang av sikkerhetsmål og strategi, jf. § 2-3, hvor formålet er å vurdere ledelsens beslutninger opp mot virksomhetens behov for informasjonsteknologi og informasjonssikkerhet. Resultatet fra sikkerhetsrevisjonen vil imidlertid være del av grunnlaget for slike gjennomganger.

Sikkerhetsrevisjon er et viktig grunnlag for kontinuerlig forbedring av informasjonssikkerheten. Praktisk kan sikkerhetsrevisjoner gjennomføres etter de samme fremgangsmåter som benyttes i HMS-arbeidet, jf. forskrift 6. desember 1996 nr. 1127 om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter (internkontrollforskriften).

4. Aukra kommune har etablert avviksbehandlingssystem og behandler sikkerhetsbrudd som avvik

Personopplysningsforskriften § 2-6 stiller krav om at det er etablert avviksbehandlings-system:

«Bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd, skal behandles som avvik».

Kommentar fra Datatilsynet:
Bestemmelsen pålegger den behandlingsansvarlige å behandle uønskede hendelser i informasjonssystemet med formål å gjenopprette normal tilstand og å hindre med formål å gjenopprette normal tilstand og å hindre gjentagelse. Avviksbehandling iverksettes ved sikkerhetsbrudd og/eller når oppgaver er utført i strid med de rutiner som er besluttet.

Avviksbehandling vil normalt omfatte rapportering, strakstiltak, permanent korrigering av avvik og oppfølging av korrigerende tiltak over tid for å vurdere om dette fungerer etter sin hensikt. For de tilfeller der avviksbehandlingen har avdekket uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig, skal Datatilsynet meddeles resultatet fra avviksbehandlingen.

5. Aukra kommune har en klar organisering med etablerte ansvars- og myndighetsforhold

Personopplysningsforskriften § 2-7 stiller krav om en klar organisering med etablerte ansvars- og myndighetsforhold:

«Det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjons-systemet».

Kommentar fra Datatilsynet:
Bestemmelsen pålegger den behandlingsansvarlige å organisere arbeidet med informasjonssystemet slik at tilfredsstillende informasjonssikkerhet oppnås. Det skal etableres klare ansvars- og myndighetsforhold med utgangspunkt i beslutninger tatt av virksomhetens ledelse. Ansvars- og myndighetsforhold skal dokumenteres og gjøres kjent for virksomhetens medarbeidere.

Det er viktig at ansvar og myndighet relatert til drift av informasjonssystemet (driftsledelse) og for oppfølging av sikkerhetsarbeid (sikkerhetsledelse), er klarlagt. Disse funksjoner er henholdsvis ”utøvende” og ”kontrollerende” og bør ideelt sett tillegges forskjellige medarbeidere i virksomheten. For mindre virksomheter kan det likevel være nødvendig å legge begge funksjoner til en og samme person. Arbeidsoppgaver for sikkerhetsleder vil normalt omfatte forberedelse av ledelsesgjennomganger, gjennomføring av sikkerhetsrevisjoner samt kontroll med risikovurdering og avviksbehandling.

Den behandlingsansvarlige pålegges videre å konfigurere informasjonssystemet slik at tilfredsstillende informasjonssikkerhet oppnås. Med ”konfigurasjon” menes informasjonssystemets utforming, det vil si utstyr og program samt sammenkoblinger mellom disse. Informasjonssystemet konfigureres med utgangspunkt i beslutninger tatt av virksomhetens ledelse. Konfigurasjonen skal dokumenteres.

Ved valg av konfigurasjon skal virksomhetens behov for informasjonssikkerhet tillegges vekt, i tillegg til vurdering av økonomi og behov for funksjonalitet.

Eksempelvis vil slik vurdering omfatte etablering av sikkerhetsbarrierer, bruk av nettverkssegmentering for å skille forskjellige behandlinger av personopplysninger fra hverandre i informasjonssystemet eller lignende.

Den behandlingsansvarlige pålegges å beslutte hvordan arbeidet med informasjonssystemet skal foregå. Slike beslutninger må gjøres kjent for virksomhetens medarbeidere i form av rutiner for bruk. Rutiner må ha et omfang og en detaljeringsgrad som sikrer at arbeidsoppgaver utføres med tilfredsstillende sikkerhet som resultat, og at de utføres likt hver gang de repeteres.

6. ***Aukra kommune har fysisk sikring mot uautorisert tilgang***
Personopplysningsforskriften § 2-10 stiller krav om fysisk sikring mot uautorisert tilgang:

«Det skal treffes tiltak mot uautorisert adgang til utstyr som brukes for å behandle personopplysninger...».

Kommentar fra Datatilsynet:
Bestemmelsen pålegger den behandlingsansvarlige å hindre uautorisert adgang til utstyr benyttet for behandling av personopplysninger eller med betydning for informasjonssikkerheten. Eksempelvis skal tjener og klientmaskiner, og utstyr benyttet som sikkerhetsbarrierer i virksomhetens datanett, fysisk sikres mot uautorisert adgang.

Fysisk sikring kan gjennomføres ved tilsyn/vakt, låsing/skjerming av det enkelte utstyr eller låsing/skjerming av lokaler. Tilsyn/vakt etableres eksempelvis ved hjelp av resepsjonstjeneste og ledsagelse av uautorisert personell (besøkende). Låsing/skjerming av utstyr oppnås eksempelvis ved fysiske sikkerhetsmekanismer integrert i utstyret. For låsing/skjerming av lokaler er det som hovedregel tilstrekkelig å etablere normal bygningsmessig sikkerhet.

7. Aukra kommune har tiltak mot uautorisert innsyn
Personopplysningsforskriften § 2-11 stiller krav om tiltak mot uautorisert innsyn:

«Det skal treffes tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig».

Kommentar fra Datatilsynet:
Begrepet konfidensialitet i denne bestemmelsen er ikke sammenfallende med konfidensialitetsbegrepet i sikkerhetsinstruksen. Bestemmelsen pålegger den behandlingsansvarlige å hindre uautorisert innsyn i personopplysninger. Også informasjon om informasjonssystemet og om sikkerhetstiltak skal sikres mot uautorisert tilgang når dette kan få betydning for informasjonssikkerheten.

Valg av hvilke opplysninger som det skal sikres konfidensialitet for, og hvilke sikkerhetstiltak som må etableres, følger av resultatet av risikovurderingen. Den behandlingsansvarlige skal ved kryptering eller på annen møte sørge for nødvendig konfidensialitet ved overføring av personopplysninger i offentlige telenett.

Reglene for kryptering gjelder også for overføring via private datalinjer som er utenfor det området virksomheten har sikret mot uautorisert adgang, jf. § 2-10. I slike tilfeller skal kryptering velges som nødvendig erstatning for konfidensialitetssikring som normalt oppnås ved fysisk sikring. Eksempel på annen sikring enn kryptering kan være anonymisering eller oppsplitting av teksten slik at teksten kun gir mening når en har tilgang til hele teksten.

Det skal tydelig fremgå om et lagringsmedium (harddisk, magnetbånd, kompaktdisk, diskett eller lignende) inneholder personopplysninger som det er nødvendig å sikre konfidensialitet for. Bestemmelsen inneholder ingen detaljerte krav til utforming eller metode. Den behandlingsansvarlige må selv velge merking som gir tilstrekkelig informasjon om konfidensialitetsbehovet, eksempelvis ved utveksling av lagringsmedia eller for å vurdere behovet for sletting av personopplysninger.

Bestemmelsen pålegger den behandlingsansvarlige å sørge for sletting av personopplysninger fra lagringsmedium som ikke lenger benyttes for behandling av personopplysningene. Bestemmelsen inneholder ingen detaljerte krav til metode. Valg av metode for sletting vil blant annet avhenge av om lagringsmediet skal benyttes til annen behandling av personopplysninger eller avhendes.

Ved avhending av lagringsmedia skal personopplysninger slettes fullstendig og permanent fra lagringsmediet, slik at det ikke er mulig, selv ved bruk av tekniske hjelpemiddeler, å gjenopprette tilgang til opplysningene. Som alternativ til sletting kan det være nødvendig å destruere lagringsmediet fysisk.

8. Aukra kommune sikrer tilgang til personopplysninger

Personopplysningsforskriften § 2-12 stiller krav om at kommunen sikrer tilgang til personopplysninger:

«Det skal treffes tiltak for å sikre tilgang til personopplysninger hvor tilgjengelighet er nødvendig».

Kommentar fra Datatilsynet:
Bestemmelsen pålegger den behandlingsansvarlige å sikre nødvendig innsyn i opplysninger slik at behandling av personopplysninger kan gjennomføres som besluttet. Det skal også sikres tilgang til informasjon om informasjonssystemet og om sikkerhetstiltak når dette er nødvendig for sikkerhetsarbeidet. Valg av hvilke opplysninger som det skal sikres tilgjengelighet for, og hvilke sikkerhetstiltak som må etableres, følger av resultatet av risikovurderingen.

For personopplysninger som det skal sikres tilgjengelighet for, må den behandlingsansvarlige forberede alternativ behandling for de tilfeller informasjonssystemet ikke er tilgjengelig. Alternativ behandling kan gjennomføres ved duplisering av utstyr/ program, eller ved hjelp av manuelle behandlingsrutiner.

Den behandlingsansvarlige skal reservekopiere (ta "backup" av) personopplysningene. Kravet til reservekopiering gjelder også for annen informasjon når dette er nødvendig for sikkerhetsarbeidet, eksempelvis for program og innstillinger av program, benyttet i sikkerhetstiltak.

9. Aukra kommune har tiltak mot uautorisert endring av personopplysninger

Personopplysningsforskriften § 2-13 stiller krav om tiltak mot uautorisert endring av personopplysninger:

«*Det skal treffes tiltak mot uautorisert endring av personopplysninger der integritet er nødvendig*».

Kommentar fra Datatilsynet:
Bestemmelsen pålegger den behandlingsansvarlige å hindre utilsiktet endring av personopplysninger. Også informasjon om informasjonssystemet og om sikkerhetstiltak skal sikres mot uautorisert endring når dette er nødvendig for informasjonssikkerheten.

Valg av hvilke opplysninger som det skal sikres integritet for, og hvilke sikkerhetstiltak som må etableres, følger av resultatet av risikovurderingen. Den behandlingsansvarlige skal sørge for beskyttelse mot ødeleggende program, eksempelvis "datavirus" eller "malicious software". Slike program kan påvirke integritet for program benyttet for behandling av personopplysninger eller i sikkerhetstiltak, og medføre driftsforstyrrelser og gjøre informasjonssystemet utilgjengelig.

Tema 2: Posthåndtering

Forvaltningsloven
Forvaltningsloven § 18 (partenes adgang til å gjøre seg kjent med sakens dokumenter):

> *«En part har rett til å gjøre seg kjent med sakens dokumenter, for så vidt ikke annet følger av reglene i §§ 18 til 19. Dersom en mindreårig er part i saken og blir representert av verge, gjelder dette også den mindreårige selv. Retten til innsyn gjelder også etter at det er truffet vedtak i saken. En mindreårig under 15 år skal ikke gjøres kjent med opplysninger som er underlagt lovbestemt taushetsplikt.*
> *Når det er adgang til å gjøre unntak fra innsyn, skal forvaltningsorganet likevel vurdere å gi helt eller delvis innsyn. Innsyn bør gis dersom hensynet til parten veier tyngre enn behovet for unntak».*

Det er større rettigheter til innsyn som part i sak. For å kunne gjøre seg kjent med dokumentene må de være tilgjengelig for parten når han eller hun ber om innsyn. Hvis ikke saksbehandler er på jobb (ferie, permisjon e.l.) er det vesentlig at andre kan greie å finne frem til dokumentene.

Forvaltningsloven § 23 (formene for enkeltvedtak):

> *«Et enkeltvedtak skal være skriftlig om ikke dette av praktiske grunner vil være særlig byrdefullt for forvaltningsorganet».*

Dette kan være vedtak som forplikter kommunen i en eller annen form, og det er viktig at slike dokumenter blir journalført og kommer inn i kommunens arkiv. Dokumenter som ikke er journalført er på en måte" ikke-eksisterende dokumenter" – det er kun kjent for noen få.

Forvaltningsloven § 27 (underretning om vedtaket):

> *«Det forvaltningsorgan som har truffet vedtaket, skal sørge for at partene underrettes om vedtaket så snart som mulig. … I regelen gis underretning skriftlig. Er det særlig byrdefullt for forvaltningsorganet å gi skriftlig underretning, eller haster saken, kan underretning gis muntlig eller på annen måte. I så fall kan en part kreve å få vedtaket skriftlig bekreftet…».*

eForvaltningsforskriften
eForvaltningsforskriften § 1 (forskriftens formål og anvendelsesområde):

> *«Forskriftens formål er å legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen. Den skal fremme forutsigbarhet og fleksibilitet og legge til rette for samordning av sikre og hensiktsmessige tekniske løsninger. Forskriften skal legge til rette for at enhver på en enkel måte kan utøve sine rettigheter og oppfylle sine plikter overfor det offentlige.*
> *Forskriften gjelder for elektronisk kommunikasjon med forvaltningen og for elektronisk saksbehandling og kommunikasjon i forvaltningen når ikke annet er bestemt i lov eller i medhold av lov.*
> *Denne forskrift gir ikke grunnlag for å gjøre unntak fra de alminnelige reglene om forsvarlig saksbehandling i forvaltningsloven».*

Når forvaltningsorganet legger til rette for elektronisk kommunikasjon, kan det oppstå ny risiko knyttet til formidling av slike opplysninger. Det kan ikke forventes at brukerne selv er kjent med, eller har forutsetninger for å vurdere følgende av den risiko for uberettiget innsyn, eller at opplysninger kommer på avveie, som måtte forekomme i forbindelse med elektronisk kommunikasjon.

eForvaltningsforskriften pålegger derfor forvaltningsorganet et særlig ansvar for å forebygge slik risiko og å informere brukerne om eventuell risiko ved bruk av elektronisk kommunikasjon. Viktig at man har stadfestet i dokumenthåndteringsrutinene sine hvordan kommunen skal forholde seg til elektronisk kommunikasjon, enten det er epost, facebook, elektroniske skjema osv. Man skal ikke sende sensitive opplysninger pr. e-post uten kryptering.

Arkivloven med forskrifter
Arkivloven § 1 (føremål):

> *«Føremålet med denne lova er å tryggja arkiv som har monaleg kulturelt eller forskningsmessig verde eller som inneheld rettsleg eller viktig forvaltningsmessig Dokumentasjon, slik at desse kan verta tekne vare på og gjorde tilgjengeliege for ettertida».*

Arkivene som kommunene lager inneholder rettslig og forvaltningsmessig dokumentasjon og det er derfor viktig at disse arkivene blir både dannet og bevart riktig. Det overordnede arkivansvaret ligger hos administrasjonssjefen jfr. kommuneloven § 23.

Bestemmelser om kommunale arkiv er gitt i arkivloven og forskrift om offentlig arkiv. Under gjengis hovedbestemmelser fra arkivforskriften.

Arkivforskriften § 2-6 (journalføring og anna registrering):

> *«Eit offentleg organ skal ha ein eller fleire journalar for registrering av dokument i dei sakene organet opprettar. I journalen skal ein registrere alle inngåande og utgåande dokument som etter offenleglova § 4 må reknast som saksdokument for organet, dersom dei er gjenstand for saksbehandling og har verdi som dokumentasjon.*
> *…*
> *Journalar skal førast elektronisk eller på papir. Dersom journalen inngår i eit elektronisk arkiv- eller saksbehandlingssystem, skal ein på en enkel måte kunne hente ut og gjere tilgengeleg dei journalopplysningane som allmenta har krav på å få innsyn i…».*

De meste av dokumentene som enten kommer inn til kommunen, eller som kommunen sender ut, blir vanligvis journalført av arkivtjenesten. Journalføring skal gjøres slik at man kan identifisere dokumentene og det er en rekke opplysninger som skal med slik som avsender/ mottaker, dato, opplysninger om innhold m.m.

Arkivforskriften § 3-1 (mottak og opning av vanleg post):

> *«Inngåande post skal leverast til arkivtenesta. Dersom arkivfunksjonane er desentraliserte, i delarkiv eller eigne journalførande einingar, må ein fastsetje kva for eining av arkivtenesta som skal motta post som er adressert til organet utan nærmare spesifikasjon.*

> *Personleg adressert post, dvs. brev der personnamnet er nemnt før namnet på organet, skal leverast uopna til adressaten, med mindre organet har inngått avtale med adressaten om at arkivtenesta kan opne slik post. Dersom brevet viser seg å vere eit saksdokument for organet, skal det straks returnerast til arkivtenesta og behandlast som post til organet. Dette gjeld også post som er adressert til den politiske leiinga i eit organ».*

Inngående post skal leveres og åpnes av arkivtjenesten, dette gjelder også telefaks, e-post eller lignende som er stilet til organet. I forbindelse med poståpning skal det gjennomføres arkivbegrensning, som betyr at man vurderer hva som skal journalføres/ ikke journalføres.

Kommunen bør ha rutiner på hvordan dokumentbehandlingen foregår og hvem som er ansvarlig for hva i forbindelse med produksjon av egne dokumenter og ved mottak av dokumenter utenfra. Det er også viktig å merke seg at begrepet *dokument* er teknologinøytralt i lovverket så hvilken informasjonsbærer innholdet kommer på er uvesentlig, det er innholdet som teller.

Når man journalfører dokumenter og samler dokumentene sammen til saker lager man arkiv. Når man gjør dette kan man følge opp saksbehandlingen og sørge for at inngående dokumenter blir besvart til riktig tid og at utgående dokumenter blir kvalitetssikret og bekreftet at de er sendt.

Arkivforskriften § 3-3 (behandling av dokument på ulike medium)
Hvis en kommune har papirarkiv og ikke elektronisk arkiv, og mottar saksdokumenter på annet medium enn papir, må kommunen sørge for at slike dokumenter skrives ut på papir.

Arkivforskriften § 3-5 (registrering og fordeling):

> *«Saksdokument skal registrerast i journalen før dei går til saksbehandling. Dette gjeld også for hastesaker, sjølv om desse kan vere underlagde særskilde behandlingsprosedyrar».*

Dette er viktig for å dokumentere og ha oversikt over hvilke dokumenter kommunen har mottatt til saksbehandling.

Arkivforskriften § 3-8 (avskriving og arkivlegging):

> *«Når saksbehandlingen er avsluttet og svarbrev er ekspedert, skal alle dokumenter i saken tilbake til arkivtjenesten».*

Arkivforskriften § 3-9 (kopibok):

> *«Organet skal normalt lage kopibok som inneheld kopi av alle utgåande dokument. Riksarkivaren kan fastsetje, gjennom generelle føresegner eller enkeltvedtak, at elektronisk arkiv på visse vilkår kan erstatte kopiboka, jf. § 2-13».*

Organet skal normalt lage kopibok. Den skal inneholde kopi av alle undertegnede dokumenter som er sendt ut fra organet. Det er vanlig at man har en perm hvor man setter inn kopiene fortløpende. Kommunen må ha rutiner på hvem det er som skal sørge for at dette kommer i kopiboka. Kommuner som har elektroniske lagrede saksdokumenter kan på visse vilkår nytte dette i stede for kopibok.