



Namsos kommune

November 2021

FR1195

1 SAMMENDRAG AV PROSJEKTPLAN

Problemstilling	a) Hvordan ivaretar Namsos kommune informasjonssikkerhet? b) Hvordan har kommunen sikret integritet, konfidensialitet og tilgjengelighet for informasjon fra de gamle kommunene?
Kilder til kriterier	Kilder til kriterier er aktuelle lover, for eksempel personopplysningsloven og arkivloven, og tilhørende forskrifter og veiledninger.
Metode	Aktuelle metoder for innsamling av data er intervju og gjennomgang av tilgjengelig dokumentasjon. I tillegg kan det være aktuelt å gjøre undersøkelser knyttet til konkrete datasystemer.
Tidsplan	Prosjektets rammer er: • 400 timer • Levering til sekretær 1. juni 2022
Prosjektteam	Oppdragsansvarlig revisor: Margrete Haugum margrete.haugum@revisjonmidtnorge.no Prosjektmedarbeider: Thomas Furunes thomas.furunes@revisjonmidtnorge.no Styringsgruppe: • Merete Montero • Unni Romstad
Uavhengighetserklæring	Ingen av de involverte revisorer vil få habilitetsproblemer ved gjennomføringen av prosjektet. Oppdragsansvarlig forvaltningsrevisors uavhengighetserklæring er vedlagt prosjektplanen.
Kontaktperson Namsos kommune	Kommunaldirektør i Namsos eller den som kommunedirektøren delegerer

2 OPPDRAGET

I dette kapittelet presenteres bestillingen og bakgrunnsinformasjon for prosjektet.

2.1 Bestilling fra kontrollutvalget

Prosjektet ble bestilt i kontrollutvalgets møte 21. september 2021. Undersøkelsen skal omfatte IKT, datasikkerhet og GDPR. Kontrollutvalget kom med følgende innspill til problemstillinger/spørsmål:

- Sikkerhet, drifting og dublering av system
- Samordning mellom enhetene på bruk av digitale plattformer, effektivisering
- Fremtidig lagring og tilgang. Kompatibilitet av system, rettsdokumentasjon

Kontrollutvalget ønsket å få oversendt en prosjektplan til møte 23. november 2021.

Slik revisor forstår bestillingen er den knyttet til informasjonssikkerhet. Det er redegjort for sammenhengene mellom begrepene i bestillingen i kapittel 2.4. Der begrunnes også hvorfor informasjonssikkerhet løftes opp som et overbyggende begrep.

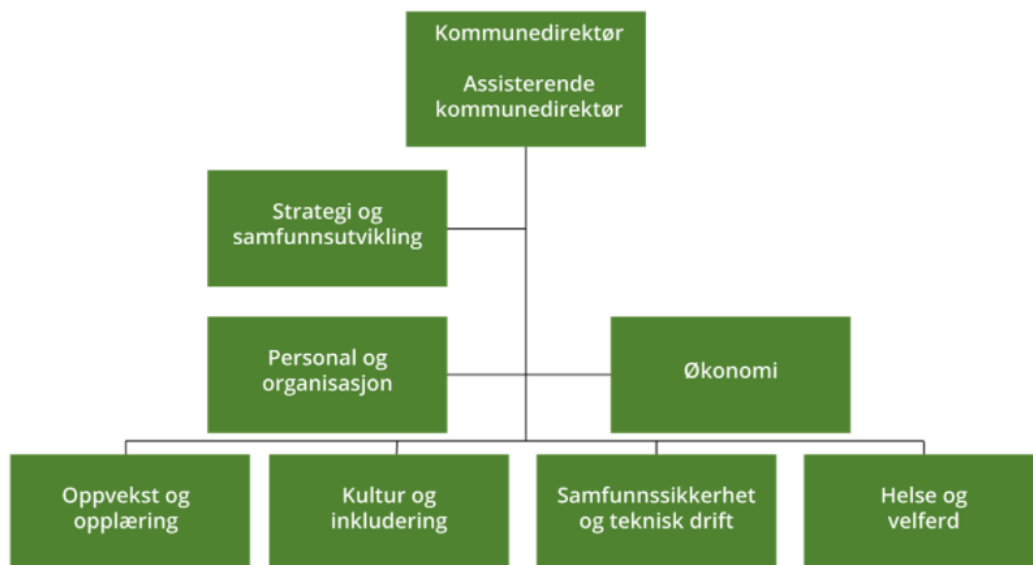
2.2 Bakgrunnsinformasjon

Av helhetlig risiko- og vesentlighetsanalyse fra 2020 fremgår det at antallet henvendelser til IT brukerstøtte har økt betydelig, mens antallet ansatte er stabilt. Antallet henvendelser som ikke lukkes innen akseptabel frist beskrives som økende. Kommunen har et eget arkivdepot. Kommunen legger opp til økt bruk av elektronisk kommunikasjon med innbyggerne. Gjeldende IKT-strategi skulle vært rullert i 2016.

Nåværende Namsos kommune er en sammenslåing av tidligere Namsos kommune, Namdalseid kommune og Fosnes kommune. Kommunesammenslåingen skjedde fra 1. januar 2020. I den forbindelse er datasystemene i den nye kommunen samordnet.

2.3 Kommunens organisering

I figur 1 er kommunens organisasjonskart gjengitt.



Kilde: Namsos kommunes hjemmeside

Figur 1. Organisasjonskart Namsos kommune

Informasjonssikkerhet berører hele kommuneorganisasjonen ettersom en stor del av kommunenes arbeid er digitalisert, og ansatte trenger både teknisk infrastruktur og programmer (applikasjoner) for å utføre arbeidet. Kommunens arbeid dokumenteres i digitale systemer og arkivfunksjonen i kommunen er kjernen for å ta vare på og gjøre det mulig å finne igjen informasjon. Samtidig er det et krav om å minimere lagringen og sikret at bare de som skal ha tilgang får det og at lagret informasjon er ekte.

Det framgår av kommunenes nettside at kommunen har personvernombud og personvernerklæring. I stabsfunksjonen personal og organisasjon er det et eget dokumentcenter. Det går ikke klart fram hvor i organisasjonen informasjonssikkerhetsarbeidet er.

2.4 Informasjonssikkerhet

Informasjonssikkerhet og datasikkerhet er nært beslektede begreper. Datasikkerhet omhandler den elektroniske behandlingen av data, mens informasjonssikkerhet er et litt videre begrep som også inkluderer data oppbevart i papirform. Den nye personvernforordningen, forkortet til GDPR, trådte i kraft 25.05.2018. Den gjelder all elektronisk databehandling av personopplysninger og ikke-elektronisk behandling av personopplysninger når de er satt i register. I GDPR-regelverket står informasjonssikkerhet sentralt og bestemmelsene er på mange områder overførbare til annen informasjon enn bare personopplysninger.

Informasjonssikkerhet handler om at informasjons generelt og spesielt personopplysninger må sikres på en tilfredsstillende måte. Informasjonssikkerhet handler om:

- Integritet – nøyaktige og fullstendige opplysninger sikret mot uautorisert endring
- Konfidensialitet – sikre at kun autoriserte brukere har tilgang
- Tilgjengelighet – sikre at opplysningene er tilgjengelig for autoriserte personer ved behov

For å ivareta informasjonssikkerheten stilles det større krav til dokumentasjon av prosesser, sikkerhetsløsninger, IT-systemer og opplæring av ansatte. GDPR-regelverket skjerper kravene til internkontroll. Personvernforordningen stiller strengere krav enn tidligere til håndtering av avvik.

Det kan listes opp ulike krav som skal ivaretas og noen eksempler er gjengitt under:

- Krav til konfigurering av IT-systemer
- Krav om signering av taushetserklæring
- Krav om fysisk sikring
- Opplæring av ansatte
- Sikring av konfidensialitet
- Sikring av integritet
- Tilgjengelighet og backup løsninger
- Jevnlige sikkerhetsrevisjoner
- Prosedyrer for avvikshåndtering
- Tilgangsstyring og logging av autorisert og uautorisert bruk
- Databehandleravtaler
- Personvernombud

3 PROSJEKTDESIGN

I dette kapitlet presenteres problemstillingene i forvaltningsrevisjonen, kilder til revisjonskriterier og metode for innsamling av data.

3.1 Avgrensing

Prosjektet handler om informasjonssikkerhet i Namsos kommune etter sammenslåingen av kommunene Namsos, Namdalseid og Fosnes. Sammenslåingen av kommunene medførte at tre selvstendige enheter med hver sine datasystemer skulle bli til et felles system. En slik overgang kan være forbundet med risiko og revisor vil se nærmere på hvordan informasjonssikkerheten ble ivaretatt i sammenslåingen. Forvaltningsrevisjonen avgrenses til å se på informasjonssikkerheten i den nye kommunen og ikke hvordan dette ble løst i de tidligere kommunene.

Prosjektet er avgrenset til informasjonssikkerhet internt i Namsos kommune og omhandler ikke tjenester som Namsos kommune leverer til nabokommuner.

Forvaltningsrevisjonen ser heller ikke på hvordan informasjonssikkerhet ivaretas fra et brukerperspektiv, det vil si for den enkelte ansatte eller for innbyggerne.

3.2 Problemstillinger

Revisjonen foreslår følgende problemstillinger:

- a) Hvordan ivaretar Namsos kommune informasjonssikkerhet?
- b) Hvordan har kommunen sikret integritet, konfidensialitet og tilgjengelighet for informasjon fra de gamle kommunene?

Informasjonssikkerhet

Det meste av lovkrav knyttet til informasjonssikkerhet er gitt i lov om personopplysninger, som inneholder EUs personvernforordning. Ut over lov om personopplysninger er forhold omkring informasjonssikkerhet i mindre grad lovregulert, men gitt i standarder som for eksempel ISO 27000-serien og COSO. Omtalen av informasjonssikkerhet i kapittel 2.4 viser noen av de forholdene som inngår i revisjonen.

Informasjonssikkerhet i kommunesammenslåingen

Denne problemstillingen omhandler hvordan kommunen jobbet med å lage felles informasjonssystem og hvordan informasjonssikkerheten ble sikret i overgangen fra tre til en kommune. Det er også aktuelt å undersøke tilgjengeligheten av dokumenter fra de gamle systemene. I denne problemstillingen inngår også å se på bruken av ulike applikasjoner og overgang til felles applikasjoner.

3.3 Kilder til kriterier

Aktuelle kilder for kriterier vil være personopplysningsloven og arkivloven med tilhørende forskrifter. Kriterier vil også kunne utledes fra veiledere utarbeidet av Datatilsynet og Arkivverket. Det kan også være aktuelt å undersøke om kommunen følger opp egne retningslinjer.

3.4 Metoder for innsamling av data

Hovedkilder for innsamling av data vil være intervju med aktuelle personer i kommunen og gjennomgang av politiske vedtak, utarbeidede rutiner og gjennomgang av datasystemer. Personopplysningsloven stiller krav til dokumentasjon som er aktuelle data i forvaltningsrevisjon.

Steinkjer 4. november 2021

Margrete Haugum

Oppdragsansvarlig revisor

VEDLEGG 1: UAVHENGIGHETSERKLÆRING

PM Revisjon Midt-Norge	
Prosjekt nr: FR1195	Kommune: Namsos
Vurdering av uavhengighet - revisors egen vurdering i forbindelse med forvaltningsrevisjonsprosjekt: IKT, datasikkerhet, GDPR - Informasjonssikkerhet	

Hovedreferanse: Kommuneloven § 24-4 Forskrift om kontrollutvalg og revisjon kapittel 3 RS 200 --- Formål og generelle prinsipper for revisjon av regnskaper pkt. 4 RS 220 -- Vilkår for revisjonsoppdrag pkt. 4, 12-13 RS 300 -- Planlegging av revisjon av regnskaper pkt. 6 Standard for forvaltningsrevisjon RSK 001 pkt. 8

Ansettelsesforhold:	Undertegnede har ikke ansettelsesforhold i andre stillinger enn Revisjon Midt-Norge SA
Medlem i styrende Organer	Undertegnede er ikke medlem av styrende organ i noen virksomhet som ovenfor nevnte kommune deltar i.
Delta eller inneha funksjoner i annen virksomhet, som kan føre til interessekonflikt eller svekket tillit	Undertegnede deltar ikke i eller innehar funksjoner i annen virksomhet som kan føre til interessekonflikt eller svekket tillit til rollen som revisor.
Nærstående	Undertegnede har ikke nærstående som har tilknytning til ovenfor nevnte kommune som har betydning for uavhengighet og objektivitet.
Rådgivnings- eller andre tjenester som er egnet til å påvirke revisors habilitet	Før slike tjenester utføres foretas en vurdering av rådgivningens eller tjenestens art i forhold til revisors uavhengighet og objektivitet. Dersom vurderingen konkluderer med at utførelse av slik tjeneste kommer i konflikt med bestemmelsen i forskriften § 18, skal revisor ikke utføre tjenesten. Hvert enkelt tilfelle må vurderes særskilt. Revisor besvarer løpende spørsmål/henvendelser som er å betrakte som veiledning og bistand og ikke revisjon. Paragrafen sier at også slike veiledninger må skje med varsomhet og på en måte som ikke binder opp revisors senere revisjons- og kontrollvurderinger. Undertegnede har ikke ytet rådgivnings- eller andre tjenester overfor ovenfor nevnte kommune som kommer i konflikt med denne bestemmelsen.
Tjenesten under kommunens egne ledelses- og kontrolloppgaver	Undertegnede har ikke ytet tjenester overfor ovenfor nevnte kommune som hører inn under kommunens egne ledelses- og kontrolloppgaver.
Opptre som fullmektig for den revisjonspliktige	Undertegnede opptre ikke som fullmektig for ovenfor nevnte kommune.
Andre særegne forhold	Undertegnede kjenner ikke til andre særegne forhold som er egnet til å svekke tilliten til uavhengighet og objektivitet.

Steinkjer 2.11.2021



Margrete Haugum
Oppdragsansvarlig forvaltningsrevisor



Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no