EIERSKAPSKONTROLL OG FORVALTNINGSREVISJON

IKT INDRE NAMDAL IKS

PROSJEKTPLAN

Høylandet kommune

Februar 2021

Prosjekt-ID

1 SAMMENDRAG AV PROSJEKTPLAN

Problemstilling	1. Utøver Høylandet kommune eierskapet i IKT Indre Namdal IKS i tråd med relevante anbefalinger for eierstyring? 2. Er ansvars- og arbeidsfordelingen for informasjonssikkerheten klarlagt mellom IKT Indre Namdal IKS og Høylandet kommune? 3. Følger IKT Indre Namdal IKS kravene til håndtering av informasjonssikkerhet?
Kilder til kriterier	• Kommunenes sentralforbund sine anbefalinger for god eierstyring • NUES – Norsk utvalg for eierstyring og selskapsledelse – norsk anbefaling om eierstyring og selskapsledelse • Personvernforordningen som er tatt inn i lov om personopplysninger • Veiledere fra Datatilsynet om personvern og GDPR • Avtaler/kontrakter
Metode	• Styringsdokumenter • Dokumentasjon om informasjonssikkerhet • Intervju • Eventuelt andre metoder
Tidsplan	• Antall timer vil avhenge av hvor mange kommuner som deltar i forvaltningsrevisjonen. Anslag 200-300 timer for Høylandet • Levering til sekretær 6 måneder etter at siste kommune har vedtatt prosjektplanen
Prosjektteam	Oppdragsansvarlig revisor: Margrete Haugum, margrete.haugum@revisjonmidtnorge.no Prosjektmedarbeider: Merete Montero, merete.montero@revisjonmidtnorge.no Gunnar Haave Haugum, gunnar.haugum@revisjonmidtnorge.no Styringsgruppe: • Arve Gausen • Tor-Arne Stubbe Revisor vil underveis vurdere å innhente ekstern bistand
Uavhengighets-erklæring	Ingen av de involverte revisorer vil få habilitetsproblemer ved gjennomføringen av prosjektet.

	Oppdragsansvarlig forvaltningsrevisors uavhengighetserklæring er vedlagt prosjektplanen.
Kontaktperson Høylandet kommune	Rådmann eller den som rådmannen delegerer
Kontaktperson i IKT Indre Namdal IKS	Daglig leder

2 MANDAT

I dette kapittelet vil bestillingen bli utdypet og bakgrunnsinformasjon for prosjektet gjennomgått.

2.1 Bestilling

I kontrollutvalget i Høylandet kommune sitt møte den 09.02.2021, sak 2/21 bestilte kontrollutvalget en eierskapskontroll og forvaltningsrevisjon av IKT Indre Namdal IKS. Eierskapskontrollen er prioritert i plan for eierskapskontroll 2020-2024 og forvaltningsrevisjon er prioritert i plan for forvaltningsrevisjon 2020-2024. Kontrollutvalgets føringer for eierskapskontrollen er at den skal undersøke hvordan kommunen utfører sitt eieransvar, om det er oversiktlig hva kommunen betaler for og om kommunen får det den betaler for. Føringer for forvaltningsrevisjonen er om IKT Indre Namdal IKS i samarbeid med deltakerne ivaretar informasjonssikkerheten på en tilfredsstillende måte. Herunder ansvars- og arbeidsfordelingen mellom selskapet og deltakerkommunene når det gjelder informasjonssikkerhet, prosesser og rutiner for å ivareta informasjonssikkerhet og GDPR (personvernregler).

Ettersom IKT Indre Namdal er et interkommunalt selskap er det ønskelig at flere av eier-kommunene deltar i forvaltningsrevisjonen, som vil være felles for kommunene. Eierskaps-kontrollen vil være spesifikk for den enkelte kommune med unntak av eierkommunenes felles utøvelse av eierskapet i representantskapet (tilsvarer generalforsamling i et aksjeselskap) i selskapet.

Temaet forvaltningsrevisjon i selskapet IKT Indre Namdal IKS vil berøre kommunene i sterk grad og derfor vil den enkelte kommune bli involvert i forvaltningsrevisjonen.

2.2 Bakgrunnsinformasjon

2.2.1 IKT Indre Namdal IKS

IKT Indre Namdal IKS er et interkommunalt selskap eid av Høylandet, Røryrvik, Namsskogan, Grong, Lierne og Snåsa. Selskapet forvalter IKT-løsninger for sine eierkommuner. Snåsa har vedtatt å gå ut av selskapet.

Selskapets formål er:

> *Selskapet skal i samråd med eierne arbeide for å utvikle bruken av systemer for informasjons- og kommunikasjonsteknologi tjenester hos eierne. Selskapet skal på vegne av eierne være juridisk avtalepart overfor leverandører i den hensikt å oppnå rabatter og storkundefordeler. Selskapet skal utvikle egen kompetanse på bruken av felles applikasjoner, tilby eierne brukerstøtte og tilpasninger av valgte systemer og være en pådriver i bruken av EDB-løsninger. Selskapet skal være eiernes kontaktledd mot leverandørene ut fra at eierne tegner avtaler med selskapet om bruk av valgte applikasjoner. Selskapet skal være utviklingspart for eierne på de valgte tekniske løsninger. Selskapet kan etter nærmere vedtak*

av styret prise visse tjenester og således ha egne inntekter. Selskapet har anledning til å ta på seg konsulentoppdrag for andre, når oppdragsgiver betaler for tjenesten og det ikke går ut over selskapets hovedoppgaver. Til gjennomføring av spesielle prosjekt utenom selskapets ordinære arbeidsoppgaver, blir det søkt finansiering mellom medlemmene eller andre som spesielt ønsker prosjektet gjennomført. Selskapet kan delta i samarbeid med andre selskap/organisasjoner.

Selskapet ble stiftet i 2003 og har forretningsadresse i Grong kommune og postadresse i Røyrvik kommune. I følge selskapsregistreringen i brønnøysundregisteret har eierkommunene en like store eierandeler i selskapet, 16 2/3 prosent.

Ifølge selskapets hjemmeside har oppgavene siden oppstarten av selskapet i stor grad vært knyttet til prosjekter for innføring av nye fellesløsninger for eierkommunene. Innføring av nye løsninger er fortsatt en stor del av selskapets arbeidsoppgaver, men også drift og videreutvikling av eksisterende løsninger. Selskapet utfører også enkeltvise tjenester for kommunene ved behov.

I årsmeldingen for 2018 informeres det om at fra oppstarten av selskapet ble jobbet med prosjekter for innføring av fellesløsninger for kommunene. Nå er en stor del av de 50 systemene med tilhørende støttesystemer fellesløsninger. Selskapets aktivitet har endret seg til å bli mer en driftsorganisasjon med hovedvekt på drift av eksisterende løsninger. Utfordringen for selskapet er å ha ressurser til å gjennomføre nye prosjekter, samtidig som eksisterende løsninger skal driftes og vedlikeholdes. Trenden de siste årene har vært at kravet til informasjonsdeling mellom ulike fagapplikasjoner har økt, noe som kompliserer prosjektgjennomføringen. Den daglige driften av eksisterende løsninger omfatter vedlikehold/oppgradering, utvikling, brukerstøtte og feilretting. Selskapet bruker også mye tid på bistand av brukere og superbrukere i kommunene på ulike løsninger. I tillegg til drift av fellesløsninger har selskapet driftet lokal infrastruktur for to av kommunene gjennom en avtale om fast tjenestekjøp.

Når det gjelder GDPR står det i årsmeldingen at i 2018 har kommunene og IKT Indre Namdal IKS gjennomført et fellesprosjekt hvor man har innarbeidet en rekke styringsdokumenter som er nødvendige for etterlevelse av de nye kravene.

Årsmeldingen for 2018 refererer til selskapsavtalens §4 når det gjelder ansvarsområde. Her heter det:

> Selskapet skal i samråd med eierne arbeide for å utvikle bruken av systemer for informasjons- og kommunikasjonsteknologitjenester hos eierne. Selskapet skal på vegne av eierne være juridisk avtalepart overfor leverandører i den hensikt å oppnå rabatter og storkundefordeler. Selskapet skal utvikle egen kompetanse på bruken av felles applikasjoner, tilby eierne brukerstøtte og tilpasninger av valgte systemer og være en pådriver i bruken av EDBløsninger. Selskapet skal være eiernes kontaktledd mot

leverandørene ut fra at eierne tegner avtaler med selskapet om bruk av valgte applikasjoner. Selskapet skal være utviklingspart for eierne på de valgte tekniske løsninger.

Selskapet kan etter nærmere vedtak av styret prise visse tjenester og således ha egne inntekter. Selskapet har anledning til å ta på seg konsulentoppdrag for andre, når oppdragsgiver betaler for tjenesten og det ikke går ut over selskapets hovedoppgaver.

Til gjennomføring av spesielle prosjekt utenom selskapets ordinære arbeidsoppgaver, blir det søkt finansiering mellom medlemmene eller andre som spesielt ønsker prosjektet gjennomført.

Selskapet kan delta i samarbeid med andre selskap/organisasjoner.

2.2.2 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 overførbar til annen informasjon enn bare personopplysninger.

Informasjonssikkerhet handler om at 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 skjerper kravene til intern-kontroll. Personvernforordningen stiller strengere krav enn tidligere til håndtering av avvik.

Det kan listes opp ulike krav som skal ivaretas:

- 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

- Vurdere sikkerhet hos leverandører og andre som opplysninger overføres til
- Risikovurdering av informasjonssystemer

I personvernforordningen skilles det på rollene som behandlingsansvarlig og databehandler.

Behandlingsansvarlig – den eller de virksomhetene som bestemmer formålet med behandlingen av personopplysningene og hvilke hjelpemidler som skal brukes (hvorfor og hvordan personopplysningene skal brukes). I dette tilfellet vil det være den enkelte kommune.

Databehandler – virksomheter som behandler personopplysninger på vegne av den behandlingsansvarlige. I dette tilfellet vil det blant annet være IKT Indre Namdal IKS og leverandører av applikasjoner[1].

Artikkel 5 i personvernforordningen stiller opp grunnkrav for å behandle personopplysninger. Det er tre prinsipielle krav: Lovlig, rettferdig og åpenhet. Det stilles krav til at registreringen skal ha et formål og at det finnes en hjemmel for dette formålet. De opplysningene som skal registreres skal være *tilstrekkelig og relevante*. Det betyr at det ikke skal behandles flere opplysninger enn nødvendig og ikke lagres lengre enn nødvendig. Opplysningene skal være korrekte og oppdatert og de skal være tilstrekkelig sikret. Gjennom internkontroll skal man dokumentere at reglene følges. Alle offentlige virksomheter skal ha personvernombud.

Personvernforordningen stiller følgende dokumentasjonskrav til behandlingsansvarlig og databehandlere:

Tabell 1. Dokumentasjonskrav

Behandlingsansvarlig	**Databehandler**
Vedlikeholde oversikt over behandlinger	Vedlikeholde oversikt over behandlinger
Risikovurdering og tilfredsstillende teknisk og organisatoriske tiltak.	Risikovurdering og tilfredsstillende tekniske og organisatoriske tiltak
Etterleve og demonstrere etterlevelse av personvernprinsippene	
Konsekvensutredning dersom høy risiko	
Innebygd personvern	

[1] Applikasjon er en programvare som benytter datamaskinens ressurser til en oppgave som brukeren ønsker utført, for eksempel tekstbehandlere, regneark og nettlesere.

Ut over kravene til dokumentasjon stilles det også en rekke krav til rutiner og retningslinjer.

- Kartlegging av personopplysninger
- Identifisere formålet med behandlingen
- Hjemmelsgrunnlag for behandlingen
- Vurdere om formålet er i samsvar med hjemmelen
- Vurdering av opplysningers kvalitet
- Retting og sletting av personopplysninger
- Oppfyllelse av informasjonsplikt ved innhenting av opplysninger
- Innsyn
- Utlevering av opplysninger
- Overføring av opplysninger til tredjeland
- Inngåelse av databehandleravtale
- Gjennomføring av kontrolltiltak overfor ansatte
- Innsyn i epost
- Bruk av epost, post på mobil, makulering og utskrift
- Avviksmeldinger og oppfølging
- Inngåelse av taushetserklæringer
- Gjennomføring av risikovurderinger
- Tilgang og avvikling av tilganger til IT-systemer

Noen av disse kravene ligger til både behandlingsansvarlig og databehandler. Samtidig er det slik at IKT Indre Namdal IKS ivaretar oppgaver for kommunene, noe som stiller krav til en tydelig ansvarsfordeling mellom selskapet og den enkelte kommune.

2.3 Selskapets og kommunens organisering

I følge hjemmesiden har selskapet tre ansatte med kontorsted Røyrvik og Snåsa.

På hjemmesiden til Høylandet kommune finnes det en personvernerklæring www.hoylandet.kommune.no/tjenester/administrasjon/personvernombud. Det opplyses om at Marit Grannes ved servicekontoret er personvernombud. Det går videre fram at rådmannen er IKT-ansvarlig.

3 PROSJEKTDESIGN

I dette kapitlet presenteres revisors forslag til forvaltningsrevisjonsprosjekt med avgrensninger, problemstillinger, kilder til revisjonskriterier og metode.

3.1 Avgrensing

Prosjektet er sammensatt av en eierskapskontroll og en forvaltningsrevisjon. Eierskaps-kontrollen retter seg mot Høylandet kommune som eier og utøvelsen av eierskapet i representantskapet sammen med de andre eierne. Eierskapskontrollen tar utgangspunkt i Kommunenes Sentralforbund sine anbefalinger for god eierstyring og det gjøres et utvalg av anbefalingene som er relevant for interkommunale selskaper.

Forvaltningsrevisjonen tar utgangspunkt i GDPR. Kravene til informasjonssikkerhet er ivaretatt i regelverket om GDPR og vil derfor ikke bare handle om personopplysninger, men om hele informasjonssystemet.

Ansvaret for GDPR ligger hos kommunene og således vil forvaltningsrevisjonen også berøre kommunen som den ansvarlige. I tillegg er det litt uklart for revisor hvordan oppgave- og ansvarsfordelingen er mellom hver enkelt kommune og selskapet.

3.2 Problemstillinger

4. Utøver Høylandet kommune eierskapet i IKT Indre Namdal IKS i tråd med relevante anbefalinger for eierstyring?
5. Er ansvars- og arbeidsfordelingen for informasjonssikkerheten klarlagt mellom IKT Indre Namdal IKS og Høylandet kommune?
6. Følger IKT Indre Namdal IKS kravene til håndtering av informasjonssikkerhet? Eksempelvis kan dette handle om:
    - Kartlegging av personopplysninger
    - Tilgangsstyring og -kontroll
    - Databehandleravtaler (kommune-selskap-leverandør)
    - Avviksmelding og oppfølginger
    - Opplæring av ansatte
    - Taushetserklæringer
    - Risikovurdering
    - Internkontroll og dokumentasjonskrav

3.3 Kilder til kriterier

Følgende kilder til revisjonskriterier legges til grunn for arbeidet.

- Kommunenes sentralforbund sine anbefalinger for god eierstyring

- NUES – Norsk utvalg for eierstyring og selskapsledelse – norsk anbefaling om eierstyring og selskapsledelse
- Personvernforordningen som er tatt inn i lov om personopplysninger
- Veiledere fra Datatilsynet om personvern og GDPR
- Avtaler/kontrakter

3.4 Metoder for innsamling av data

Til eierskapskontrollen vil det bli hentet data fra styringsdokumenter i selskapet og kommunens styringsdokumenter og politiske vedtak. Det er aktuelt å innhente dokumentasjon fra representantskapsmøter og styremøter for de to siste årene. Det vil også bli gjennomført intervjuer med kommunens eierrepresentant. Dette er skriftlig dokumenter som antas å beskrive forhold som problemstillingene etterspør.

I forvaltningsrevisjonen av selskapet tas det utgangspunkt i selskapets dokumentasjon knyttet til informasjonssikkerhet og oppfylling av kravene i GDPR. Aktuelle dokumenter er retningslinjer og rutinebeskrivelse, avviksmeldinger, logger for tilgangsstyring, databehandleravtaler og andre relevante dokumenter. Det blir gjennomført intervju med daglig leder og eventuelt de andre ansatte i selskapet.

Etter datainnsamlingen hos selskapet er det naturlig å følge opp med intervju med rådmannen og personvernombudet i kommunen og eventuelt innsamling av dokumentasjon fra den enkelte kommune. Dette for å undersøke arbeids- og ansvarsfordelingen mellom selskapet og kommunen, for dermed å undersøke om alle kravene blir ivaretatt.

Revisor vil vurdere andre metoder for å undersøke informasjonssikkerhet underveis i arbeidet.

Steinkjer 25.02.2021

Margrete Haugum

Oppdragsansvarlig revisor

VEDLEGG 1: UAVHENGIGHETSERKLÆRING

Prosjekt nr:	**Kommune:** Høylandet kommune med flere
Vurdering av uavhengighet - revisors egenvurdering i forbindelse med forvaltningsrevisjonsprosjekt: IKT Indre Namdal IKS	

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 utøvelse 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 opptrer 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 25.02.2021
Margrete Haugum
Styringsgruppe

Revisjon

Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no