EIERKAPSKONTROLL OG FORVALTNINGSREVISJON

IKT INDRE NAMDAL IKS

RAPPORT

Januar 2022

SK1030

Høylandet kommune

FORORD

Revisjon Midt-Norge SA har gjennomført denne eierskapskontrollen og forvaltningsrevisjonen på oppdrag fra Høylandet, Grong, Lierne og Namsskogan kommuners kontrollutvalg i perioden mai 2021 til januar 2022.

Kontrollutvalget skal påse at forvaltningsrevisjon gjennomføres, jf. lov om kommuner og fylkeskommuner (kommuneloven) § 23-2 punkt c). Forvaltningsrevisjon innebærer å gjøre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets eller fylkestingets vedtak og forutsetninger[1].

Revisjonsteamet har bestått av oppdragsansvarlig Margrete Haugum, prosjektmedarbeider Merete Montero og Gunnar Haugum, og kvalitetssikrere Arve Gausen og Tor Arne Stubbe. Revisor har vurdert egen uavhengighet overfor kommunene og selskapet, jf. kommuneloven § 24-4 og forskrift om kontrollutvalg og revisjon kapittel 3.

Forvaltningsrevisjonen er gjennomført i henhold til NKRFs[2] standard for forvaltningsrevisjon og eierskapskontroll, RSK 001 og RSK 002.

Vi vil takke alle som har bidratt med informasjon i prosjektet. En oversikt over tidligere gjennomførte prosjekter finnes på vår hjemmeside www.revisjonmidtnorge.no.

Steinkjer, 27.01.2022

Margrete Haugum

Oppdragsansvarlig revisor

[1] Kommuneloven § 23-3, 1.ledd

[2] Norges Kommunerevisorforbund, www.nkrf.no

SAMMENDRAG

IKT Indre Namdal IKS eies av Høylandet, Grong, Lierne, Namsskogan og Røyrvik kommune. Våren 2021 bestilte fire av de fem eierkommunene en eierskapskontroll av IKT Indre Namdal IKS og en forvaltningsrevisjon av informasjonssikkerhet. Følgende problemstillinger er belyst i prosjektet:

1. Utøver kommunen 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 kommunen?
3. Følger IKT Indre Namdal IKS kravene til håndtering av informasjonssikkerhet?

Det er gjennomført dokumentstudier av protokoller fra representantskapsmøter og styremøter i selskapet, samt dokumentasjon på informasjonssikkerhet i selskapet. Revisor har også undersøkt dokumentasjon på informasjonssikkerhet i noen kommuners kvalitetssystemer. Revisor har også undersøkt eierskapsmeldinger og annen relevant dokumentasjon fra kommunene. Det er gjennomført intervju med eierrepresentantene, kommunedirektører og selskapets daglige leder og sikkerhetsansvarlig.

Eierskapskontroll

Selskapsavtalen er sist vedtatt 12.05.2021 og oppfyller kravene i IKS-loven. Høylandet har en eierskapsmelding fra 28.10.2021 som oppfyller kravene til eierskapsmelding.

Selskapsavtalen regulerer at ordfører er eierrepresentant med varaordfører som vararepresentant. Kommunens delegasjonsreglement hjemler av ordfører representerer kommunen i generalforsamlinger og representantskap hvor det ikke er foretatt valg. Kommunen har ikke hatt eierskap som en del av folkevalgtopplæringen, men har behandlet eierskapsmelding og har planer om å gjennomføre opplæring. Eierrepresentanten for Høylandet kommune har et forutsigbart system for kommunikasjon med kommunestyret, som kan forankres bedre i eierskapsmeldingen.

Representantskapet behandler regnskap og budsjett, men ikke økonomiplan, slik IKS-loven krever. Det er etablert en valgkomite, men den er ikke vedtektsfestet. Det er finnes ikke retningslinjer for valgkomiteens arbeid. Representantskapet velger styre og har besluttet å gjennomføre styreevaluering som grunnlag for å vurdere sammensetningen av styret. Flere av styremedlemmene er kommunedirektører i eierkommunene. Dette kan gi habilitets-utfordringer.

Revisors konklusjon er at det er noen svakheter i Høylandet kommune sin utøvelse av eierskapet i IKT Indre Namdal IKS. Disse svakhetene omfatter:

- Kommunikasjonen mellom eier og eierrepresentant bør forankres bedre i eierskapsmeldingen
- Representantskapet behandler ikke økonomiplan slik IKS-loven sier
- Det mangler retningslinjer for valgkomiteens arbeid
- Det er habilitetsutfordringer knyttet til at kommunedirektører og andre sentralt ansatte i kommunene har styreverv i IKT Indre Namdal IKS
- Ikke alle styrets medlemmer er registrert i styrevervregisteret

Revisor anbefaler Høylandet kommune å:

- Forankre kommunikasjon mellom eier og eierrepresentant i eierskapsmeldingen
- Sørge for at representantskapet behandler økonomiplan
- Sørge for at det utarbeides retningslinjer for valgkomiteens arbeid
- Vurdere utfordringene med kommunedirektørenes inhabilitet

Ansvars- og arbeidsfordeling

Den enkelte kommune er behandlingsansvarlig og har et overordnet ansvar for å overholde personvernprinsippene og regelverket rundt personopplysninger. IKT Indre Namdal IKS er en av flere databehandlere som kommunene har. Personopplysningsloven sier det skal foreligge en databehandleravtale. Det finnes ingen databehandleravtale mellom IKT Indre Namdal IKS og kommunene. Selskapet har tatt tak i dette og startet opp arbeidet med å lage en databehandleravtale.

Revisor finner at dokumentasjon på ivaretakelse av prinsippene for behandling av personopplysninger er svært mangelfull, og at kommunene ikke ivaretar ansvaret sitt som behandlingsansvarlige.

Informasjonssikkerhet

IKT Indre Namdal IKS har sikkerhetsmål og sikkerhetsstrategi for selskapet. Denne omfatter ikke kommunen. Selskapet gjør relevante risikovurderinger og iverksetter sikkerhetstiltak, men risikovurderingene er ikke dokumentert. Selskapet mangler system for internkontroll, men har iverksatt anskaffelse av det.

IKT Indre Namdal IKS har databehandleravtale med sine leverandører, men det mangler databehandleravtale med kommunene. Selskapet har en behandlingsoversikt som er en

bruttoliste for kommunene og selskapet som ble laget i 2018. Den kommunale delen av denne lista er ikke oppdatert. En databehandleravtale vil kunne klargjøre ansvarsforholdene omkring behandlingsoversikten.

Selskapet iverksetter mange tekniske og organisatoriske sikkerhetstiltak, men lite dokumenteres og settes i system. Selskapet framstår som veldig operativt og handlingsorientert. Det er en erkjennelse at selskapet er lite og at det er fornuftig å samarbeide med andre (eksempelvis Atea) om ulike løsninger og tiltak, blant annet for å ha god ressursutnyttelse og et større fagmiljø å støtte seg til. Det er revisors oppfatning at selskapet jobber innenfor et krevende fagområde som stiller store krav til faglig oppdatering og rask støtte til kommunene når det trengs. Med knappe ressurser blir den operative virksomheten og akutte hendelser prioritert i hverdagen, og ikke utviklingsarbeidet.

IKT Indre Namdal IKS har personvernombud.

Konklusjon

Revisor konkluderer med at:

- ansvars- og arbeidsfordelingen mellom den enkelte kommune og IKT Indre Namdal IKS ikke er klarlagt.
- IKT Indre Namdal IKS har svakheter i oppfølging av kravene til informasjonssikkerhet, begrunnet i:
    - Risikovurderinger er ikke dokumentert
    - Selskapet har ikke noe internkontrollsystem
    - Selskapet har databehandleravtaler med leverandører, men mangler databehandleravtaler med kommunene
    - Protokollen over behandlingsaktiviteter er mangelfull og ikke oppdatert
    - Det er gjort tekniske og organisatoriske tiltak innenfor de økonomiske rammene selskapet får, men det mangler dokumentasjon på flere av tiltakene

Anbefalinger

Revisor anbefaler IKT Indre Namdal IKS å:

- sørge for at kravet om databehandleravtale i tråd med personopplysningsloven følges opp. Herunder at arbeids- og ansvarsfordelingen mellom selskapet og eierkommunene blir klarlagt og dokumentert.
- sørge for at kravene i personopplysningsloven oppfylles.

INNHOLDSFORTEGNELSE

Tabell

1 INNLEDNING

I innledningen gjennomgås bestillingen, problemstillinger, metode og bakgrunn for prosjektet. I kapittel 1.5 er det tatt inn en oversikt over sentrale begreper som brukes i rapporten.

1.1 Bestilling

Med bakgrunn i Plan for forvaltningsrevisjon 2020-2024, bestilte kontrollutvalget i Høylandet kommune en eierskapskontroll og forvaltningsrevisjon av IKT Indre Namdal IKS i sitt møte 09.02.2021. Kontrollutvalget vedtok også at de øvrige eierkommunene skulle få en forespørsel om å delta i prosjektet.

Kontrollutvalget i **Røyrvik kommune** behandlet forespørselen om å delta i eierskapskontroll og forvaltningsrevisjon av IKT Indre Namdal IKS i møtet 09.02.2021. Kontrollutvalget besluttet ikke å delta.

Revisor laget en prosjektplan for et mulig felles prosjekt for Høylandet, Grong, Lierne og Namsskogan, datert 25.02.2021. Denne planen lå til grunn for kontrollutvalgenes videre behandling av saken.

Kontrollutvalget i **Høylandet kommune** vedtok den 01.03.2021 prosjektplanen og ba om en oppdatering i forhold til ressursrammen og leveringstidspunkt, hvis forutsetningen om deltakelse fra Høylandet, Grong, Namsskogan og Lierne ble endret.

Kontrollutvalget i **Lierne kommune** vedtok den 9.03.2021 å delta i prosjektet under forutsetning av deltakelse fra Høylandet, Grong, Namsskogan og Lierne og at kontrollutvalget fikk en tilbakemelding på ressursramme og leveringstidspunkt.

I kontrollutvalget i **Grong kommune** den 24.03.2021, ble det besluttet å delta i prosjektet under forutsetning av skisserte ressursramme og deltakelse fra de fire kommunene.

Kontrollutvalget i **Namsskogan kommune** vedtok å delta i prosjektet 17.03.2021 under forutsetning av deltakelse fra de tre andre kommunene og bad om en tilbakemelding på ressursbruken og leveringstidspunkt. Kontrollutvalget behandlet i møtet 19.05.2021 en oppdatert prosjektplan som inneholdt en ressursramme og leveringstidspunkt.

1.2 Problemstillinger

Følgende problemstillinger besvares i rapporten:

4. Utøver kommunen 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 kommunen?
6. Følger IKT Indre Namdal IKS kravene til håndtering av informasjonssikkerhet? Eksempelvis handler dette om:
    - Sikkerhetsmål og sikkerhetsstrategi
    - Risikovurderinger
    - Internkontrollsystem
    - Databehandleravtaler
    - Behandlingsaktiviteter
    - Tekniske og organisatoriske tiltak
    - Personvernombud

IKT Indre Namdal IKS jobber med innføring, drift og utvikling av datasystemer for eier-kommunene og har dermed en tett samhandling med den enkelte kommune. Derfor omhandler den andre problemstillingen grenseflaten mellom selskapet og den enkelte kommune når det gjelder informasjonssikkerhet. På denne måten vil også den enkelte kommune bli involvert i forvaltningsrevisjonen.

I den tredje problemstillingen ble det listet opp eksempler på hva håndtering av informasjons-sikkerhet kan handle om. Underveis i prosjektet ble det klart at noen av disse forholdene ikke er IKT Indre Namdal IKS sitt ansvar. Det har ført til at andre relevante forhold omkring informasjonssikkerhet som berører selskapet er tatt inn.

1.3 Metode

I arbeidet med eierskapskontrollen har vi samlet inn dokumenter fra kommunene for å undersøke hvilke styringssignaler kommunene gir til selskapet. Dette handler i hovedsak om eierskapsmeldinger og kommunestyrenes vedtak om oppnevning av eierrepresentanter. Vi har også hentet ut generalforsamlingsprotokoller fra 2019 og fram til høsten 2021 og gjennomgått disse. Protokollene er dokumentasjon på eiers utøvelse av eierskapet. I tillegg er eier-representantene intervjuet i et digitalt møte. Eierskapsintervjuet med Liernes eierrepresentant ble gjennomført samtidig med eierskapsintervjuet om Brann Midt IKS, fordi de sammenfalt i tid og hadde mange like spørsmål. Det ble laget en felles intervjuguide til eierskapsintervjuene med eierrepresentantene i IKT Indre Namdal IKS og eierrepresentantene har godkjent referatene fra hver sine intervju.

Til problemstillingen om ansvars- og arbeidsfordelingen mellom selskapet og den enkelte kommune har vi intervjuet både selskapets ledelse og kommunedirektørene i de fire

kommunene. Dette for å fange opp synspunkter på arbeids- og ansvarsfordelingen fra begge parter. Vi har valgt intervju for å ha muligheten til å stille oppfølgende spørsmål omkring forholdet mellom selskapet og den enkelte kommune, og fordi forholdet mellom kommunene og selskapet kan være forskjellig fra kommune til kommune. Revisor har funnet lite dokumentasjon på ansvars- og arbeidsfordelingen. Revisor har bedt om innsyn i kommunenes kvalitetssystem hvor retningslinjer for GDPR (*general data protection regulation*, nærmere forklart i kapittel 1.5) finnes. Revisor har ikke fått innsyn i Høylandet kommune sitt kvalitetssystem. Til to av kommunene ble det laget noen mer detaljerte, skriftlige spørsmål til andre i kommunen fordi kommunedirektørene henviste til andre som hadde mer detaljkunnskap. Høylandet kommune har ikke svart på spørsmålene. Referat fra intervjuet med kommunedirektøren i Høylandet er ikke godkjent i innen den utvidede fristen som ble gitt. De andre kommunedirektørene har godkjent referatene fra intervjuene. Kommunedirektøren i Høylandet ble i epost 20.01.2022 informert om at revisor ville anse intervjureferatet som godkjent hvis det ikke ble gitt beskjed senest 24.01.2022. Revisor har ikke fått noe svar.

Revisor har også fått tilgang til kvalitetssystemene i Grong, Lierne og Namsskogan og sett nærmere på hvilken dokumentasjon som finnes på GDPR området i kvalitetssystemene.

I forvaltningsrevisjonen av selskapet har revisor hatt et digitalt oppstartsmøte med daglig leder. I tillegg ble det gjennomført er mer omfattende fysisk intervju med daglig leder og selskapets sikkerhetsansvarlige. Intervjuene fulgte en intervjuguide, og referatet er godkjent. Revisor har hentet ut styreprotokoller for perioden 2019 og fram til høsten 2021. I tillegg har enkeltsaker som er relevant for problemstillingene blitt undersøkt nærmere, slik som utviklingsplanen for selskapet. Revisor har også fått tilsendt selskapets GDPR-dokumentasjon som ligger i kvalitetssystemet.

På grunn av lite dokumentasjon, spesielt om ansvars- og arbeidsfordeling, har intervjuene blitt en viktig datakilde. På grunn av den praktiske arbeidsfordelingen mellom selskapet og kommunene, er det mange forhold som kunne vært undersøkt i kommunene, men som ligger utenfor denne revisjonen. Det er revisors oppfatning at vi har et tilstrekkelig datagrunnlag for konklusjoner og anbefalinger. IKT er et område med mange begreper og faguttrykk som gjør at begrepsvaliditeten kan være svekket. Dette handler både for eksempel om hvordan revisor stiller spørsmål og hvordan disse spørsmålene fortolkes av den som skal svare, videre hvordan svaret blir fortolket av intervjuer. Revisjon Midt-Norge har forsøkt å styrke begrepsvaliditeten gjennom å styrke prosjektteamet med en medarbeider med kompetanse på IT-revisjon.

1.4 Bakgrunn

IKT Indre Namdal IKS er et interkommunalt selskap som eies av Grong, Høylandet, Lierne, Namsskogan og Røyrvik kommune. Snåsa kommune var medlem fram til 01.01.2021. Selskapet forvalter IKT-løsninger for sine eierkommuner.

Selskapet ble stiftet i 2003 og har forretningsadresse i Grong kommune og postadresse i Røyrvik kommune. Siste vedtatte selskapsavtale fra 12.05.2021, viser at hver av kommunene har en eierandel på 20 prosent. Sammensetningen av styret framgår av tabell 1.

Tabell 1. Styret og administrativ leder i IKT Indre Namdal IKS

Rolle	**Navn**	**Periode**
Styreleder	Karl Audun Fagerli*	2015
Nestleder	Mildrid Hendbukt-Søbstad	2020
Styremedlem	Tore Kirkedam	2021
Styremedlem	Liv Elden Djokoto	2012
Varamedlem	Bjørn Ståle Aalberg	2020
Varamedlem	Ola Peder Tyldum	2016
Varamedlem	Tone Røttesmo	2016
Daglig leder	Stein Vidar Aspnes	2014

*Fagerli har også hatt andre roller i styret Kilde: www.brreg.no

IKT Indre Namdal IKS har fra høsten 2021 fire ansatte. To av eierkommunene kjøper tjenester fra selskapet ut over selskapets virksomhet for å styrke kommunenes IT-ressurser.

Ifølge selskapets hjemmeside har selskapets oppgaver 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, ved siden av drift og videreutvikling av eksisterende løsninger. Selskapet utfører også andre tjenester for kommunene ved behov.

I årsmeldingen for 2018 informeres det om at det 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, oppgraderinger, utvikling, brukerstøtte og feilretting. Selskapet bruker også mye tid på bistand til 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.

I selskapets årsmelding for 2018 står det at kommunene og IKT Indre Namdal IKS, gjennomførte et fellesprosjekt om GDPR, hvor de har innarbeidet en rekke styringsdokumenter som er nødvendige for etterlevelse av de nye kravene i personvernlovgivingen.

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

> 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 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.

1.5 Begreper

Personopplysningsloven inneholder en del begreper som det kan være nyttig å ha oversikt over. Under er noen av begrepsdefinisjonene fra personvernforordningen gjengitt.

GDPR – general data protection regulation. Dette er en forkortelse for personvernforordningen som er en lov som EU har vedtatt. Den er tatt inn i den norske lov om personopplysninger. I stedet for paragrafer henviser forordningen til artikler.

Personopplysning – enhver opplysning om en identifisert eller identifiserbar fysisk person (den registrerte). En identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, for eksempel et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet.

Behandling – enhver operasjon eller rekke av operasjoner hvor personopplysninger inngår, enten automatisert eller ikke, for eksempel innsamling, registrering, omorganisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.

Register – enhver strukturert samling av personopplysninger som er tilgjengelig etter særlige kriterier, enten samlingen er plassert sentralt, er desentralisert eller spredt på et funksjonelt eller geografisk grunnlag.

Behandlingsansvarlig – en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.

Databehandler – en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige.

Integritet og konfidensialitet – personopplysninger skal behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak.

Dataminimering – personopplysninger som samles inn skal være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for.

Lovlighet, rettferdighet og åpenhet -behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte.

Formålsbegrensning – personopplysninger skal samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene.

1.6 Rapportens oppbygging

Denne rapporten er en eierskapskontroll av kommunen og en forvaltningsrevisjon av selskapet IKT Indre Namdal IKS. Eierskapskontrollen er unik for den enkelte kommune, mens forvaltningsrevisjonen er lik. Det betyr at rapporten finnes i fire versjoner med hver sin eierskapskontroll rettet mot den enkelte kommune. Eierskapskontrollen er rapportens kapittel 2. Konklusjon og anbefalinger i eierskapskontrollen er plassert sist i dette kapitlet.

Det første kapittelet er en innledning som redegjør for bestillingsprosessen, problemstilling og metode.

Kapittel 3 ser på ansvars- og arbeidsfordelingen mellom selskapet og kommunene.

Kapittel 4 er forvaltningsrevisjon av IKT Indre Namdal IKS og omhandler informasjons-sikkerhet.

Kapittel 5 er en redegjørelse for høring hos både eierrepresentanten og selskapet. Kommune-direktørene har også fått rapporten på høring fordi kapittel 3 berører deres ansvarsområde.

Kapittel 6 er konklusjon og anbefalinger knyttet til forvaltningsrevisjonen.

2 EIERSKAPSKONTROLL HØYLANDET

Dette kapitlet handler om Høylandet kommune sitt eierskap i IKT Indre Namdal IKS.

2.1 Problemstilling

Problemstillingen om eierskap er følgende:

> *Utøver Høylandet kommune eierskapet i IKT Indre Namdal IKS i tråd med relevante anbefalinger for eierstyring?*

2.2 Vurderingskriterier

Vurderingskriterier til eierskapskontrollen er hentet fra kommuneloven og KS sine anbefalinger om eierstyring, selskapsledelse og kontroll (2020). I tillegg gir også lov om interkommunale selskap (IKS-loven) av 29. januar 1999 nr. 6 føringer for IKS som selskapsform. Utledningen av revisjonskriteriene finnes i vedlegg ett.

Styringsdokumenter

- Det skal foreligge en selskapsavtale som minst angir informasjon som IKS-loven krever.
- Kommuner skal minst en gang i valgperioden utarbeide en eierskapsmelding som skal vedtas av kommunestyret. Den skal inneholde: prinsipper for eierstyring, oversikt over eierskap, formål med eierskapet.
- Selskapsinformasjonen i eierskapsmeldingen bør revideres årlig med oppdatert selskapsinformasjon.

Eierrepresentasjon

- Kommunestyret skal oppnevne sentrale folkevalgte til representanter og vara-representanter til representantskapet for fire år.
- Kommunen bør gjennomføre opplæring om eierskap for kommunestyrerepresentantene i løpet av de seks første månedene av valgperioden.
- Det bør etableres forutsigbare kommunikasjonsformer mellom eier (kommunestyret) og eierrepresentant som forankres i eierskapsmeldingen.

Representantskapet

- Representantskapet skal behandle selskapets regnskap, budsjett og økonomiplan.
- Representantskapet skal velge et styre og bør sikre at styrets kompetanse er tilpasset det enkelte selskaps formål og virksomhet.

- Representantskapet bør vedtektsfeste bruk av valgkomite og vedta retningslinjer for valgkomiteens arbeid.
- Eier bør ha et system for å unngå inhabilitet og unngå at sentrale folkevalgte og administrative ledere velges som styremedlemmer der kommunen har eierinteresser.
- Eier bør sikre at styrets medlemmer er registrert i styrevervregister.

2.3 Utøvelse av eierskapet i Høylandet kommune

2.3.1 Styringsdokument

Selskapsavtale

IKT Indre Namdal IKS ble opprettet 18.06.2003. Selskapsavtalen ble sist revidert 12.05.2021 og foreligger nå som versjon 8. Selskapsavtalen ble sist revidert i forbindelse med at Snåsa kommune gikk ut av samarbeidet. Den reviderte selskapsavtalen trer i kraft når alle eierne har vedtatt den og signert (§ 28 i selskapsavtalen). Kommunestyret på Høylandet vedtok ny selskapsavtale 27.05.2021, sak 0033/21. Den er også vedtatt av de andre eierne.

Tabell 2 oppsummer IKS-lovens krav til selskapsavtale og den andre kolonnen viser hvilke bestemmelser i selskapsavtalen som svarer på kravene.

Tabell 2. Krav til innhold i selskapsavtalen

Krav til innhold i selskapsavtalen, jf. IKS-loven § 4	**Bestemmelse i selskapsavtalen**
Selskapets foretaksnavn	§ 1 Navn
Angivelse av deltakere	§ 1 Navn
Selskapets formål	§ 4 Formål og ansvarsområde
Den kommune der selskapet har sitt hovedkontor	§ 3 Hovedkontor
Antall styremedlemmer	§ 11 Styret
Deltakernes innskuddsplikt og plikt til å foreta andre ytelser overfor selskapet	§ 6 Ansvarsfordeling
Den enkelte deltakers eierandel i selskapet og den enkelte deltakers ansvarsandel i selskapet dersom denne avviker fra eierandelen	§ 5 Eierandel
Antall medlemmer av representantskapet og hvor mange medlemmer den enkelte deltaker oppnevner	§ 8 Representantskapet

Eierskapsmelding

Høylandet kommunestyre vedtok eierskapsmelding 28.10.2021, sak 58/2021. Forrige behandling av eierskapsmeldingen var 01.04.2020.

Eierskapsmeldingen har et kapittel om kommunens eierskapspolitikk, her skilles det mellom eierskapspolitikk og eierstrategi.

- *Eierskapspolitikken* er de overordnede premissene som kommunen legger til grunn for forvaltningen av sine selskaper eller eierandeler. Politiske temaer kan for eksempel være premisser for valg av styremedlemmer, premisser for valg av selskaps-organisering og premisser for hvordan eierstyringen skal skje. Dette er prinsipper og retningslinjer for kommunens eierskap.
- *Eierstrategi* er de prioriteringer, tiltak og resultatkrav kommunen har overfor det enkelte selskap for å sikre at selskapet ivaretar de målsettingene som eierne har satt.

Kapitlet om eierskapspolitikk omhandler prinsipper for kommunen som eier, prinsipper for selskaper der kommunen er eier og prinsipper for selskapets styrer.

Eierskapsmeldingen har en oversikt over de selskapene som kommunen har eierinteresser i. I forbindelse med hvert selskap er det gjort vurderinger av kommunens eierskap, herunder kommunens formål med eierskapet.

Høylandet kommunes formål med eierskapet i IKT Indre Namdal IKS er effektivisering av tjenesteproduksjon. Selskapet innehar både viktig kompetanse som alle kommuner drar nytte av og gir kommunen mye bedre økonomiske vilkår på drift og innkjøp enn om kommunen hadde stått alene.

I saksframlegget går det fram at det legges opp til en rutine der administrasjonen kommer med eventuelle innspill overfor kommunens representant i styret før hvert representantskapsmøte, basert på den eierstrategien som er gjeldende for de ulike selskapene.

Ordfører forteller at kommunen har ambisjoner om årlige eierskapsmeldinger, men har ikke fått det til hvert år. I den siste versjoner er det tatt inn et kapittel om eierskapsstrategi, hvor det går fram hva kommunen ønsker med de ulike eierskapene. Ordfører ønsker mer bevissthet omkring mål og mening med eierskapene. Det er kommuneadministrasjonen som har skrevet eierskapsmeldingen.

2.3.2 Eierrepresentasjon

Valg av eierrepresentant

Det er fastslått i selskapsavtalens § 8 at representantskapet skal bestå av eiernes ordførere og at eiernes varaordførere er medlemmenes personlige varamedlemmer. Valget gjelder for den kommunale valgperioden. Videre står det at eierne har instruksjonsmyndighet overfor sine representanter i representantskapet, mens representantskapet har instruksjons- og omgjøringsmyndighet overfor styret.

Eierrepresentanten opplever det ikke som noe problem at selskapsavtalen har bestemmelser om hvem som skal representere eierkommunene.

Eierrepresentanten forteller at kommunen bruker å fordele verv i en sak i starten av valgperioden. Eierrepresentanten er usikker på om det velges representant til representantskapet i IKT Indre Namdal IKS. Revisor har ikke funnet at det er valgt representant og vararepresentant(er) i sak 65/19 Valg av nemnder, utvalg og råd i perioden 2019-2023. I denne saken er det valgt representant og vararepresentanter til andre interkommunale selskaper som kommunen deltar i.

I høringssvaret opplyser eierrepresentanten at kommunens delegeringsreglement, vedtatt 22.09.2020, sak 56/20, har en bestemmelse om at ordfører gis fullmakt til å representere kommunen ved generalforsamlinger, årsmøter hvor kommunen har eierinteresser som eier eller aktør, og er kommunens representant i representantskapsmøter. Dette gjelder der kommunestyret ikke har gjort særskilte vedtak eller valg.

Opplæring

Eierrepresentanten forteller at kommunen hadde folkevalgtopplæring i starten av perioden, hvor det ble lagt vekt på det kommunale årshjulet og rollen som politiker fordi det var mange nye politikere. De planla mer folkevalgtopplæring året etterpå hvor eierskap var en del av innholdet. Dette ble utsatt på grunn av pandemien og målet er å gjennomføre opplæringen tidlig i 2022.

I saksframlegget til sak 58/2021 om eierskapsmeldingen, går det fram at formannskapet/ kommunestyret ikke har fått gjennomarbeidet den eierskapspolitikken som nå framlegges tilstrekkelig, da den i stor grad er kopiert fra andre kommuner. Det foreslås at kommunestyret i 2022 setter av en dag til gjennomgang av kommunens eierskap, eierskapspolitikk og eierskapsstrategi. Da vil eierskapsmeldingen bli evaluert/bearbeidet og både administrasjonen og politisk nivå vil kunne ende opp med et dokument som bedre gjenspeiler det Høylandet kommune egentlig ønsker med sitt eierskap.

Eierrepresentanten presiserer i høringssvaret at kommunen har et klart formål med de ulike interkommunale selskapene de deltar i, og at dette er beskrevet i formålet til det enkelte selskap og i de sakene hvor kommunestyret har vedtatt å bli med i det interkommunale selskapet. I eierskapsstrategien arbeides det med form og retning for videre utvikling.

Kommunikasjonsformer mellom eier og eierrepresentant

I eierskapsmeldingen beskrives under kommunestyrets rolle at det er viktig for god oppfølging og ivaretakelse av det demokratiske eierskapet at det etableres gode systemer som sikrer at eierrepresentanten har tilstrekkelig kunnskap som hva som er kommunestyrets syn på saker som gjelder selskapet. Dette for å sikre at representanten kan ivareta eiers reelle interesser ved behandling av en sak.

Formannskapet er ifølge eierskapsmeldingen tillagt rollen som kommunens eierskapsutvalg, herunder å være politisk styringsgruppe i arbeidet med å utforme overordnede og selskaps-spesifikke eierstrategier. I denne rollen vil formannskapet være et saksforberedende organ som etter behov vil involvere berørte aktører, samt fremme forslag til eierstrategier til kommunestyret.

Et av eierskapsprinsippene i eierskapsmeldingen er at politisk vedtatt eierstrategi binder kommunenes deltakere i generalforsamling og representantskap. Videre skal eierrepresent-anten i sitt tillitsverv sørge for at kommunens eierinteresser/vedtak/intensjon blir ivaretatt av den enkelte virksomhet. I tillegg skal eierrepresentanten utøve sin rolle innenfor vedtatte føringer fra formannskap/kommunestyre, herunder holde seg oppdatert på hva som er de til enhver tid gjeldende føringer. Representanten har et selvstendig ansvar for å innhente informasjon og avklare kommunens mål og strategier knyttet til virksomheten.

Eierrepresentanten forteller at hun orienterer i folkevalgte organ hvis det er større saker i selskapet, slik som da Snåsa gikk ut av IKT Indre Namdal IKS. Hvis det passer inn i forhold til møter i formannskapet eller kommunestyret, drøftes de utsendte sakene i forkant av representantskapsmøter, forteller eierrepresentanten. Hvis dette ikke passer inn, sendes sakene i epost til politikerne og de får mulighet til å gi innspill. Eierrepresentanten erfarer at det kommer lite signaler. Eierrepresentanten har aldri opplevd å få bundet mandat.

I høringssvaret presiserer eierrepresentanten at innkallinger og saklister til representantskap og generalforsamlinger blir sendt kommunestyremedlemmene per epost. Referater fra representantskapsmøter og generalforsamlinger blir gjort kjent for kommunestyret og i tillegg etterstrebes det å orientere formannskapet og kommunestyret muntlig om diskusjonene som har foregått i møtene.

I kommunens budsjettbehandling diskuteres selskapet og eierskapet.

Det er ikke rutine for at eierrepresentanten orienterer fra alle representantskapsmøtene, forteller eierrepresentanten. Protokoller sendes på epost eller legges ut på politikernes dataløsning for politiske saker.

2.3.3 Representantskapet

Revisor har lagt til grunn representantskapsmøter fra 2019 og framover. Det avholdes normalt ett representantskapsmøte hvert år i april. Dette er gjennomført 02.04.2019, 27.04.2020 og 28.04.2021. Det er gjennomført ett ekstraordinært representantskapsmøte 25.08.2020. Det ekstraordinære representantskapsmøtet behandlet en sak om reduksjon av kostnader i 2021 og en sak om godkjenning av låneopptak for finansiering av prosjektet *Oppgradere sak og arkivløsning Elements*.

I representantskapsbehandlingen i 2019 ble det drøftet et større IKT-samarbeid i framtiden og Snåsa orienterte om kommunestyrevedtak hvor dato for uttreden av IKT Indre Namdal IKS var flyttet fra 01.01.2020 til 01.01.2021.

Eierrepresentanten opplever at representantskapsmøtene er gode og informative møter med gode diskusjoner. Det er grundige saksframlegg med fyldige beskrivelser av aktivitet og prioriteringer. Selskapet har en stor kostnad og leverer en viktig tjeneste til kommunene.

Eierrepresentanten forteller at kommunene er både enige og uenige i saker, spesielt om prioritering og fordeling av kostnader. Det er ingen store diskusjoner om de store trekkene og dagens eiere er noenlunde samstemte.

Regnskap, budsjett og økonomiplan

Det framgår av representantskapsprotokollene at årsmelding og regnskap er faste poster i representantskapsmøtene. Revisjonsberetningen er også vedlagt sammen med årsmeldingen og regnskapet. I representantskapsprotokollen er innstillingen fra daglig leder gjengitt, samt styrets behandling av saken, før representantskapsbehandlingen.

I 2021 vedtas den økonomiske rammen for 2022 til kroner 22,5 millioner. Dette er en kostnadsramme som hvert år følges opp med en ny sak om rammer for låneopptak og tilskudd fra deltakerne. Representantskapet behandler ingen økonomiplan ut over budsjett for kommende år.

I saken om rammer for låneopptak og tilskudd fra deltakerne, beslutter representantskapet at selskapet ikke skal ta opp lån over kroner 10 millioner. Denne låneramma er gitt i selskaps-avtalens § 17. I tillegg vedtas det at tilskudd fra deltakerne skjer ved refusjon av utgifter. I selskapsavtalens § 6 heter det at eierne betaler årlig midler til driften av selskapet i samsvar med vedtak i representantskapet. Videre at grunnlaget for beregning av driftstilskuddet skal

være folketallet ved siste årsskifte og en fordelingsnøkkel som blir fastlagt av representantskapet. Representantskapet i 2021 vedtok at tilskudd fra deltakerne fordeles i hovedsak etter prinsippet om at 50 prosent av utgiftene fordeles likt, mens resterende fordeles etter folketall. Det kan i enkelttilfeller være avtalt andre fordelingsmodeller basert på antall brukere eller lokasjoner.

Høylandets eierrepresentant synes det er viktig å gi føringer når det kommer til økonomiske rammer og prioriteringer.

I hvert ordinære representantskap behandles en sak om overordnede mål og retningslinjer for driften kommende år, kalt utviklingsstrategi for driftsplattformen. I 2021 omfattet den perioden 2020-2024, etter en revidering i 2020. I behandlingen av denne saken i 2021 bestiller representantskapet et strategimøte med ordførere, rådmenn/kommunedirektører og administrasjonen i selskapet, hvor målsettingen er å utvikle samarbeidet mellom kommunene og selskapet videre. Denne saken synliggjør planer for prosjekter med innføring av ulike datasystemer/ applikasjoner. Det framgår av protokollen at daglig leders innstilling og styrets behandling av saken er grunnlaget for det som legges fram for representantskapet.

Utviklingsstrategien omhandler driftsplattformen innen IKT de neste 5 årene for IKT Indre Namdal IKS. Konklusjonen i utviklingsstrategien er at:

> For at IKT Indre Namdal IKS skal kunne tilby en sikker, stabil, skalerbar og kostnadseffektiv IKT plattform skal følgende ligge til grunn:
>
> - Lokal løsning videreføres som kjerneløsning, og selskapet skal fortrinnsvis eie hardware, men vurdere fortløpende ut fra blant annet utvikling innen skyløsninger
> - Skytjenester skal prioriteres ved oppgradering eller anskaffelse av fagapplikasjoner
> - Selskapet skal ha kontakt med andre nødvendige selskaper for å sikre en framtidsrettet IKT-løsning, som ivaretar kommunens digitaliserings ønsker. (Utviklingsstrategi 2020)

Valgkomite

Selskapsavtalens § 11 første ledd andre punktum sier at representantskapet velger en valgnemnd på to personer som forbereder valget.

I representantskapet i 2019 besluttet representantskapet å redusere antall medlemmer i valgnemnda fra tre til to medlemmer. I 2020 valgte representantskapet ordfører i Grong kommune og ordfører i Namsskogan kommune som medlemmer i valgnemnda for to år og ordfører i Grong kommune ble valgt til leder av valgnemnda for to år.

I protokollen fra 2021 er det referert fra behandlingen av valget at valgkomiteen oppfordrer styret til å gjennomføre en styreevaluering i forkant av neste representantskapsmøte for å sikre riktig kompetanse inn i styret.

I styreinstruksen fra 11.11.2020 går det fram at styret skal minimum en gang per år evaluere sitt eget arbeid og eventuelt foreslå forbedringer eller behov for endring i styresammensetningen for representantskapet.

Valg av styre

Selskapsavtalens § 11 slår fast at styret velges av representantskapet. Styret skal ha 3-5 medlemmer som velges for 2 år. Representantskapet velger leder og nestleder blant styrets medlemmer for 1 år. Varamedlemmer velges i rekkefølge.

Det framgår av protokollene fra representantskapet at det hvert år gjennomføres valg til styret.

I 2021 ble Mildrid Hendbukt-Søbstad og Tore Kirkedam valgt til styremedlemmer for 2021-2023. Karl Audun Fagerli ble valgt til styreleder for 2021-2022. Mildrid Hendbukt-Søbstad ble valgt til nestleder for 2021-2022. Det opplyses i tillegg at Karl Audun Fagerli og Liv Elden Djokoto tidligere er valgt for perioden 2020-2022. Tre varamedlemmer er valgt for perioden 2020-2022.

Valgnemnda har vurdert å gå ned til tre styremedlemmer eller å øke til fem styremedlemmer for å ivareta forhold som kompetanse, kjønnsbalanse og eksterne styremedlemmer. I dag er det to menn og to kvinner i styret.

Eierrepresentanten forteller at valgkomiteen innstiller til representantskapet, som velger styret. Kjønnsfordeling i styret har vært tema, både blant styremedlemmer og varamedlemmer. Eierrepresentant opplever at de har et dedikert styre og som har gjort en innsats for selskapet.

Et av medlemmene i valgnemnda forteller at valgnemnda snakker med de som sitter i styret og de som går ut, for å få innspill til aktuelle styrekandidater. Valgnemnda tenker kontinuitet og ønsker at minst en kommunedirektør skal sitte i styret fordi kunnskap om kommunenes behov er viktig i styret. Det er andre styremedlemmer og varamedlemmer som er fra andre faggrupper.

System for habilitetsvurdering

Selskapsavtalens § 12 om styrets møter sier i andre ledd at kommunelovens regler i § 11-10 om habilitet skal gjelde ved behandling av saker i styret og i representantskapet. Kommunelovens § 11-10 handler om *folkevalgtes inhabilitet*.

I styreinstruksen som er datert 11.11.2020 står det at kommunelovens regler om habilitet skal gjelde ved behandling av saker i styret, med henvisning til selskapsavtalens § 12.

Styret i IKT Indre Namdal IKS har i flere år bestått av en eller flere kommunedirektører. Dagens styre består av fire medlemmer hvorav to er kommunedirektører og en har vært kommunedirektør. Fire av de fem eierkommunene er representert i styret. I protokollene fra 2019 og 2021 er det ikke behandlet enkeltsaker knyttet til noen av de kommunene som styrerepresentantene kommer fra. Den eneste kommunen som det er behandlet saker i tilknytning til, er Snåsa kommune sin uttreden av selskapet. I den undersøkte perioden har ingen av styrerepresentantene hatt et ansettelsesforhold til Snåsa kommune.

Eierrepresentanten forteller at representantskapet har tidligere diskutert habilitetsspørsmål, men ikke de siste årene.

Styrevervregisteret

KS sin anbefaling om registrering i styrevervregisteret er basert på at kommuner og fylkeskommuner er avhengig av allmennhetens tillit når det gjelder både forvaltning og styring. Åpenhet rundt hvilke roller lokalpolitikere og ledelsen i kommunene har er viktig for å unngå mistanke om rolleblanding.

Selskapet som sådan er ikke registret i styrevervregisteret, men noen av styrerepresentantene og vararepresentantene er registrert i styrevervregisteret. Dette går fram av tabellen under.

Tabell 3. Registrerte i styrevervregisteret på IKT Indre Namdal IKS.

Rolle	**Navn**	**Registrert/ ikke registrert**
Styreleder	Karl Audun Fagerli*	Registrert
Nestleder	Mildrid Hendbukt-Søbstad	Registrert
Styremedlem	Tore Kirkedam	Ikke registrert
Styremedlem	Liv Elden Djokoto	Registrert
Varamedlem	Bjørn Ståle Aalberg	Registrert
Varamedlem	Ola Peder Tyldum	Ikke registrert
Varamedlem	Tone Røttesmo	Ikke registrert
Daglig leder	Stein Vidar Aspnes	Registrert

Kilde: Styrevervregisteret

2.4 Vurdering

2.4.1 Styringsdokumenter

Selskapsavtale

Vurderingskriteriet er at selskapsavtalen skal minst inneholde den informasjonen som IKS-loven krever.

Revisor vurderer at selskapsavtalen inneholder de kravene som IKS-loven setter.

Eierskapsmelding

Vurderingskriteriet er at kommunen minst en gang i valgperioden skal utarbeide en eierskapsmelding som skal vedtas av kommunestyret. Den skal inneholde prinsipper for eierstyring, oversikt over eierskap og formål med eierskapet. Selskapsinformasjonen i eierskapsmeldingen bør revideres årlig med oppdatert selskapsinformasjon.

Revisor vurderer Høylandet kommune har en eierskapsmelding i henhold til lov og anbefalinger.

2.4.2 Eierrepresentasjon

Oppnevning

Vurderingskriteriet er at kommunestyret skal oppnevne sentrale folkevalgte til representanter og vararepresentanter til representantskapet for fire år.

Revisor finner at Høylandet kommune ikke har valgt representant til representantskapet i IKT Indre Namdal IKS, men at delegeringsreglementet som ble vedtatt 22.09.2020, sak 56/20 hjemler at ordfører representerer kommunen i representantskapet når det ikke er foretatt særskilt valg.

Revisor vurderer at kommunens delegeringsreglement hjemler at ordfører er eierrepresentant i IKT Indre Namdal IKS.

Opplæring

Vurderingskriteriet er at kommunen bør gjennomføre opplæring om eierskap for kommune-styrerepresentantene i løpet av de seks første månedene av valgperioden.

Eierskap var ikke en del av folkevalgtopplæringen kommunen hadde i starten av valgperioden. I behandlingen av eierskapsmeldingen går det fram at kommunen planlegger en større gjennomgang på eierskap.

Revisor vurderer at kommunen har gjennom behandling av eierskapsmeldingen har vært opptatt av eierskap og kommunen har planer om å gjennomføre opplæring i eierskap for kommunestyrerepresentantene.

Kommunikasjonsformer mellom eier og eierrepresentant

Vurderingskriteriet er at det bør etableres forutsigbare kommunikasjonsformer mellom eier og eierrepresentant, som er forankret i eierskapsmeldingen.

Revisor finner at eierrepresentanten har en praksis med å sende innkallinger og saklister per epost til kommunestyrets medlemmer og protokoller gjøres kjent for kommunestyret. Eierskapsmeldingen sier at det er viktig at det etableres system for å sikre at eierrepresentanten kan ivareta eiers reelle interesser ved behandling av en sak. Eierskapsmeldingen sier ikke noe om hvordan dette systemet er, eller hvordan eier skal få tilbakemeldinger.

Revisor vurderer eierrepresentanten har et forutsigbart system for kommunikasjon med kommunestyret, som bør forankres som eierprinsipper i eierskapsmeldingen.

2.4.3 Representantskapet

Regnskap, budsjett, økonomiplan

Vurderingskriteriet er at representantskapet skal behandle selskapets regnskap, budsjett og økonomiplan.

Revisor finner at representantskapet i perioden 2019-2021 har behandlet regnskap og budsjett. Representantskapet har ikke behandlet økonomiplan, noe som ikke er i samsvar med kravene i IKS-lovens § 20.

Revisor vurderer at selskapet har behandlet regnskap og budsjett, men ikke økonomiplan.

Valgkomite

Vurderingskriteriet er at representantskapet bør vedtektsfeste bruk av valgkomite og vedta retningslinjer for valgkomiteens arbeid.

Revisor finner at bruk av valgkomite er vedtektsfestet, men det finnes ingen retningslinjer for valgkomiteen. I 2021 har valgkomiteen bedt styret gjøre en styreevaluering, slik at styret selv kan formidle behovet for kompetanse til valgkomiteen. Det at eierne blir enig om retningslinjer for valgkomiteens arbeid, bidrar til å avklare hva som forventes av valgkomiteen blant eierrepresentantene og valgkomiteen selv.

Revisor vurderer at valgkomite er vedtektsfestet, men at det ikke finnes noen retningslinjer for valgkomiteens arbeid.

Valg av styre

Vurderingskriteriet er at representantskapet skal velge et styre og bør sikre at styrets kompetanse er tilpasset det enkelte selskaps formål og virksomhet.

Revisor finner at representantskapet velger styre. I forbindelse med valg av styre i 2021 har valgkomiteen bedt om at det gjøres en styreevaluering med tanke på å undersøke om det er kompetanse styret mangler. Styreevaluering som grunnlag for å endre sammensetningen av styret er også nedfelt i styreinstruksen fra 11.11.2020.

Revisor vurderer at representantskapet velger styre og har besluttet å gjennomføre styre-evaluering som grunnlag for å vurdere sammensetningen av styret.

Habilitet

Vurderingskriteriet er at eier bør ha et system for å unngå inhabilitet og unngå at sentrale folkevalgte og administrative ledere velges som styremedlemmer der kommunen har eier-interesser.

Revisor finner at ordførere velges til eierrepresentanter, og at varaordførere og andre politikere velges til vararepresentanter. Selskapets styreinstruks henviser til kommunelovens regler i § 11-10 om habilitet ved behandling av saker i styret. Om inhabilitet for selskapets ansatte og medlemmer av selskapets styrende organer gjelder kommuneloven § 13-3 og § 11-10 tilsvarende. § 13-3 omhandler ansattes inhabilitet og § 11-10 omhandler folkevalgtes inhabilitet. Når det gjelder ansattes inhabilitet gjelder forvaltningslovens regler.

Revisor finner at sentrale administrative ledere velges som styremedlemmer i IKT Indre Namdal IKS. IKS-loven tillater at kommunalt ansatte kan velges til styremedlemmer i interkommunale selskaper. Det kan likevel oppstå habilitetsutfordringer.

KS sin anbefaling (nr. 15) om habilitet anbefaler at kommunedirektører ikke bør sitte i styrer i selskaper. I IKT Indre Namdal IKS er det valgt en ordning som er frarådet av KS. Det er flere grunner til at KS fraråder at kommunedirektører sitter som medlemmer av styre.

For det første kan det oppstå inhabilitet i saker som selskapet skal behandle. Inhabilitet for ansatte og medlemmer av styrende organer i interkommunale selskaper er regulert i IKS-loven. Kommunedirektør kan bli inhabil til å behandle saker i styret, som han har håndtert som ansatt i kommunen. Videre vil det generelt sett kunne være utfordrende å tenke selskapets beste ved saker som har økonomisk betydning, når det kanskje vil øke kommunens budsjett

ved større overføringer til selskapet. Eksempelvis behovet for investering i sikkerhetstiltak. Samtidig er det slik at de tjenestene selskapet yter overfor eierkommunene i stor grad griper inn i kommunens virksomhet. Med dette perspektivet ser revisor at det kan være stor nytte i at kommunedirektører er medlemmer av styret, fordi de kjenner behovet for tjenestene godt. Samtidig er det slik at informasjonssikkerhetsarbeidet er avhengig av en helhetlig tilnærming fra ledelsens side. Habilitetsutfordringene kan bli veldig synlige hvis kommunene blir uenige. Skal de ivareta sin egen kommunes behov eller selskapets behov? Som alternativ, kan kommunedirektørenes innflytelse ivaretas gjennom et eget rådgivende utvalg til styret i selskapet.

For det andre kan inhabilitet oppstå når kommunen skal behandle en sak hvor selskapet er part. Denne situasjonen er regulert i kommuneloven og forvaltningsloven. Personer i de kommunale selskapenes eierorganer og styrer må alltid vurdere sin egen habilitet i forhold til sakene som skal behandles, og bør si fra til organet dersom det kan foreligge forhold som kan lede til inhabilitet. Kommunene har ikke dokumentert en juridisk vurdering av habilitet knyttet til at kommunedirektør er styremedlem i IKT Indre Namdal. Dette gjelder både for eiersaker generelt og i saker som omhandler IKT Indre Namdal spesielt til kommunestyret. Forvaltningsloven fastslår at en person er inhabil når han er medlem av styret for et selskap som er part i saken. Ingen kommunalt ansatte skal håndtere saker i kommunen som gjelder et selskap der de selv er styremedlem. Dette gjelder uansett om selskapet er privat eid eller helt eller delvis offentlig eid. Kommunedirektøren kan bli inhabil til å tilrettelegge saker for kommunestyret.

Et aktuelt eksempel er kommunestyrets budsjettbehandling, hvor kommunedirektøren har vært med å fremme et forslag til budsjett for selskapet, som kommunedirektøren skal fremme videre til sitt eget kommunestyre.

Det er representantskapet som velger styret og som bør ha et bevisst forhold til habilitetsutfordringene. Det bør gjøres en juridisk vurdering omkring hvilke saker fra selskapet, som kan gjøre kommunedirektøren inhabil. Hvis det blir for mange saker så anbefaler KS ikke å velge kommunedirektøren som styrerepresentant. Dette skaper åpenhet om habilitet ved valg av styremedlemmer. Det er opp til den enkelte eier, kommunestyret å bestemme om dette er greit eller ikke. Hvis kommunedirektøren finnes inhabil, må setterådmann hentes inn utenfor organisasjonen.

Et tredje forhold er at det kan oppstå en skjevhet mellom kommunene hvis noen, men ikke alle kommunedirektørene er like involvert i selskapet.

Revisor finner ikke at det er gjort habilitetsvurderinger som er protokollført i selskapets representantskapsprotokoller eller styreprotokoller de siste tre årene. Kommunedirektører og andre sentralt ansatte i kommunene som styremedlemmer gir habilitetsutfordringer som bør unngås.

Revisor vurderer at det ikke er gjort habilitetsvurderinger omkring at kommunedirektører er medlemmer i styret og vil påpeke at det kan oppstå situasjoner som kan gi habilitets-utfordringer.

Styrevervregisteret

Vurderingskriteriet er at eier bør sikre at styrets medlemmer er registrert i styrevervregister.

Revisor vurderer at ikke alle av styrets medlemmer og varamedlemmer er registrert i styrevervregisteret.

2.5 Konklusjon

Revisors konklusjon er at det er noen svakheter i Høylandet kommune sin utøvelse av eierskapet i IKT Indre Namdal IKS. Disse svakhetene omfatter:

- Kommunikasjonen mellom eier og eierrepresentant bør forankres bedre i eierskapsmeldingen
- Representantskapet behandler ikke økonomiplan slik IKS-loven sier
- Det mangler retningslinjer for valgkomiteens arbeid
- Det er habilitetsutfordringer knyttet til at kommunedirektører og andre sentralt ansatte i kommunene har styreverv i IKT Indre Namdal IKS
- Ikke alle styrets medlemmer er registrert i styrevervregisteret

2.6 Anbefaling

Revisor anbefaler Høylandet kommune å:

- Forankre kommunikasjon mellom eier og eierrepresentant i eierskapsmeldingen
- Sørge for at representantskapet behandler økonomiplan
- Sørge for at det utarbeides retningslinjer for valgkomiteens arbeid
- Vurdere utfordringene med kommunedirektørenes inhabilitet

3 ANSVARS- OG ARBEIDSFORDELING

Dette kapitlet handler om ansvars- og arbeidsfordelingen mellom kommunene og IKT Indre Namdal IKS når det gjelder informasjonssikkerhet. I henhold til personopplysningsloven er kommunene behandlingsansvarlig fordi de bestemmer formålet med behandlingen av personopplysninger. IKT Indre Namdal IKS er å betrakte som en databehandler fordi selskapet behandler personopplysningene på vegne av kommunene. IKT Indre Namdal IKS er behandlingsansvarlig for personopplysninger i egen organisasjon, eksempelvis personalsystemet for de ansatte. Denne rollen berøres ikke i dette kapitlet.

3.1 Problemstilling

Følgende problemstilling besvares:

> *Er ansvars- og arbeidsfordelingen for informasjonssikkerheten klarlagt mellom IKT Indre Namdal IKS og kommunene?*

Denne problemstillingen besvares ved bruk av revisjonskriterier og en beskrivende del av noe av dokumentasjonen kommunene har innenfor informasjonssikkerhet. Prosjektet er ingen revisjon av kommunens arbeid med informasjonssikkerhet og derfor er det laget en beskrivende del av kommunenes arbeid som kan berøre ansvars- og arbeidsfordelingen.

3.2 Revisjonskriterier

Det er utarbeidet et revisjonskriterium for denne problemstillingen. Dette er utledet i vedlegg en.

- Det skal foreligge en databehandleravtale mellom kommunen som behandlingsansvarlig og IKT Indre Namdal IKS som databehandler

Behandlingsansvarlig er kommunene fordi de bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes. IKT Indre Namdal IKS er databehandler sammen med flere, eksempelvis leverandører av applikasjoner.

Artikkel 5 i personvernforordningen gir den behandlingsansvarlige ansvaret for å dokumentere at prinsippene for behandling av personopplysninger er ivaretatt. Kommunenes håndtering av prinsippene for behandling av personopplysninger er beskrevet for å gi en mer helhetlig framstilling av ansvars- og arbeidsfordelingen. Det samme er sikkerhetsmål og sikkerhetsstrategi i kommunene.

3.3 Ansvars- og arbeidsfordeling mellom kommunene og selskapet

Selskapsavtalen mellom IKT Indre Namdal IKS og kommunene i fellesskap, sier noe om formålet til selskapet og ansvarsområdet i § 4, ansvarsfordeling i § 6 og personvern og bruk av forvaltningsloven og offentlighetsloven i § 15.

Følgende deler av § 4 berører ansvars- og arbeidsfordeling mellom selskapet og kommunene, nærmere bestemt hva selskapet skal gjøre på vegne av kommunene.

- Selskapet skal i samråd med eierne arbeide for å **utvikle bruken av systemer** for informasjons- og kommunikasjonsteknologi i 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 tilpasning til 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 en **utviklingspart for eierne** på de valgte tekniske løsninger.

(revisors uthevinger)

Paragraf 6 om ansvarsfordeling handler om det økonomiske ansvaret kommunene har som eiere av selskapet. Eierne betaler årlig inn midler til drift av selskapet i samsvar med vedtak i representantskapet. Dette dekker også utgifter til lisenser, tjenester og lignende kostnader som er generert av tredjepart eller av selskapet selv.

I § 15 om personvern og bruk av forvaltningsloven og offentlighetsloven, går det fram at selskapet skal følge rutiner og saksbehandlingsregler som er vanlig for å ivareta personvernet.

IKT Indre Namdal IKS har en utviklingsstrategi for perioden 2020-2024, som er vedtatt i representantskapet 27.04.2020, sak 07/20. Denne utviklingsstrategien ble også behandlet i representantskapsmøtet 28.04.2021 uten noen revidering. I selskapets utviklingsstrategi (s. 12) opplyses det at flere applikasjoner blir erstattet med webløsninger, spesielt en del tjenester som kommunene benytter utenom IKT Indre Namdal IKS. Skolene har tatt i bruk mange tjenester via internett de siste årene. For skole er de aller fleste applikasjoner skyløsninger i dag.

Daglig leder forteller at noe er nedskrevet om ansvarsfordeling, mens andre deler er en praksis de har. Regelverket om GDPR tvinger frem spørsmålet om ansvarsfordeling, hva skal selskapet gjøre for kommunene, og hva kommunene selv må gjøre.

Daglig leder forteller at PCer er kommunenes eget ansvar. Kommunene kjøper inn og setter opp PCer. Kommunene kan styre mye selv, isolert til sin egen kommune. I praksis gjør selskapet det meste, kommunene justerer ikke applikasjoner selv. Bunnen i systemet er styrt av selskapet, med automatiske oppdatering av applikasjoner og systemer.

3.3.1 Databehandleravtale

Det er ingen databehandleravtale mellom selskapet og den enkelte kommune. Daglig leder tok opp spørsmålet under GDPR-prosjektet. Selskapsavtalen sier ikke noe om databehandling. Daglig leder forteller at de er usikre på hvordan de skal løse dette. Daglig leder foreslo å lage et generelt dokument om databehandling, men tror ikke det er holdbart juridisk sett.

Daglig leder forteller at selskapet i etterkant av intervjuet har avtalt med en ekstern konsulent om å bistå selskapet med å etablere en databehandleravtale mellom selskapet og kommunene. I høringssvaret opplyser selskapet at det er engasjert en ekstern konsulent til å bistå i arbeidet og det ble gjennomført et oppstartsmøte 15.12.2021og per 05.01.2022 er prosessen i gang.

Revisor har spurt kommunedirektørene om ansvarsforholdet mellom kommunene og selskapet og under er svarene fra kommunene gjengitt.

Grong

Kommunen har ansvar for infrastruktur internt, forteller kommunedirektøren i Grong, og selskapet har ansvaret for strukturell IKT. Hvis for eksempel infrastrukturproblemer meldes inn til selskapet, vil kommunen få beskjed om at det er en lokal oppgave, og at de må finne løsninger selv. Det er kommunen som har bygd opp lokal struktur. Hvis kommunen ikke har tilstrekkelig kompetanse, må de kjøpe tjenester fra Atea.

Driftsansvar for fellesløsninger ligger til selskapet. Kommunen må sørge for opplæring. Selskapet er forhandlingspart og tar kontraktsforhandlinger på vegne av kommunene. Da kommunen skulle skifte domene, var selskapet ansvarlig for prosjektet, mens det var lokale IT-ansatte som utførte selve jobben. Kommunen bruker selskapet som rådgivere.

Kommunedirektøren forteller at kommunen får varsler fra selskapet når uønskede eposter kommer gjennom brannmuren. Selskapet skal øke kompetansen på sikkerhet. Selskapet hadde dataangrep i mars 2021, som krevde mye kompetanse. Da måtte de kjøpe konsulent-hjelp fra Atea.

Kommunedirektøren forteller at det er etablert en felles serviceportal for melding av avvik; TMS helpdesk[3]. Den er felles for selskapet og kommunene. Der blir oppgavene fordelt etter hvem som har ansvaret.

Kommunen har ingen rutine for samhandling med selskapet ut over selskapsavtalen.

Høylandet

Kommunedirektøren forteller at kommunen har databehandleravtaler med mange leverandører, men er usikker på om det foreligger en databehandleravtale med selskapet. Det er laget rutiner for samhandling mellom selskapet og kommunen for enkelte applikasjoner, eksempelvis Elements. Det har vært tett samarbeid mellom kommunene om rutinearbeidet, men rutinene må også tilpasses den enkelte kommune sin organisering.

Kommunedirektøren i Høylandet forteller at det er utfordringer med samhandlingen mellom kommunen(e) og selskapet når det skal innføres nye satsinger. Ansvaret ligger både på selskapet og kommunedirektør. Det er uklart for kommunen hvor store ressurser som kreves for å ta i bruk nye applikasjoner og i perioder kan dette skape kapasitetsutfordringer. Kommunene må ha ressurser til å gjennomføre det som er vedtatt i selskapet. Kommunedirektøren trekker fram innføring av nytt sak- og arkivsystem som en krevende prosess og som var en stor oppgave både for selskapet og kommunene.

Selskapet har vært frempå de siste årene og påpekt viktighet av datasikkerhet, forteller kommunedirektøren. I 2021 har selskapet prioritert økt stillingsressurs for å arbeide systematisk med informasjonssikkerhet. Det er inngått avtaler, noe er startet opp og mer er planlagt. Kommunen ser behovet for å jobbe videre med informasjonssikkerhet.

Kommunedirektøren forteller at kommunen er ilagt overtredelsesgebyr av Datatilsynet. Denne saken omhandler en applikasjon som helsestasjonen brukte, hvor de ansatte fikk opp kryptert informasjon som ikke angikk kommunen. Denne applikasjonen er ikke en del av det som leveres gjennom IKT Indre Namdal. Ansatte varslet til nærmeste ledelse. Det ble gitt beskjed om at ansatte ikke skulle gå inn på området. Det tok for lang tid før det ble tatt tak i fra ledelsen. Kommunen meldte fra til Datatilsynet at de hadde tilgang til informasjonen og at det var en systemfeil hos CGM. Det hadde da gått mange måneder siden kommunen oppdaget det. Kommunen fikk kritikk for to forhold: de var for sein til å rapportere og de skulle rapportert direkte til CGM, slik at de kunne lukke feilen. Kommunen opplevde det som urettferdig at kommunen skulle få smekk, når det var CGM sin feil.

[3] TMS helpdesk – *Technet management system*, er en applikasjon for henvendelser fra brukere.

Høylandet kjøper IT-support fra Overhalla IT og kommunedirektøren ser behovet for en rolleavklaring mellom Overhalla IT, IKT Indre Namdal og kommunen. Det er spesielt viktig at ansatte er kjent med arbeidsfordelingen. Kommunedirektøren forteller at det er en avtale med Overhalla IT, men er ikke sikker på om det er en databehandleravtale. Videre forteller kommunedirektøren at de ser at de ikke klarer å følge med på den digitale utviklingen innenfor alle områder. I 2021 ble det opprettet en stilling som fagleder for digitalisering med overordnet ansvar for helhetlig satsing innenfor digitalisering.

Lierne

Lierne kommune kjøper de fleste tjenestene fra selskapet, forteller rådmannen. Kommunen har en egen IT-konsulent som er førstelinjetjeneste. Selskapet tilbyr ikke førstelinjetjeneste, så dette må kommunen ordne selv. Kommunen har ikke rutinebeskrivelser for samhandling med selskapet. For hvert enkelt prosjekt går det fram av styrets igangsettelsesvedtak hvem som er prosjektleder og hvor mye ressurser kommunen skal bistå med.

Rådmannen henviser til at årsmeldingen har en oversikt over samarbeidsprosjektene og denne listen gir en oversikt over hvilke saker selskapet skal håndtere for kommunene. Representantskapet vedtar nye prosjekter som tilføyes listen. Rådmannen forteller at kommunen har ansvaret for alt selskapet ikke skal ta ansvar for, og selskapet har fått ansvaret for alt som ikke er igjen i kommunen.

Rådmannen forteller at kommunene var bevisst på å ha en tydelig grense mellom selskapet og eierne fra første dag. Deltakerkommunene har litt ulike IT-ressurser og noen av eierne kjøper tjenester fra selskapet og andre har egen førstelinjetjeneste.

I Lierne sin sikkerhetsstrategi står det under punktet om kontrakter at alle formaliteter mellom kommunene og leverandører skal være formulert i formelle kontrakter og skal inkludere relevante sikkerhetskrav. Det skal være en egen avtale mellom IKT Indre Namdal IKS og Lierne kommune, samt mellom Lierne kommune og Lierne Utvikling AS og eventuelt andre relevante samarbeidsparter som behandler personopplysninger. Revisor har etterspurt, men ikke fått oversendt noen avtale mellom IKT Indre Namdal IKS og Lierne kommune.

Namsskogan

Kommunedirektøren i Namsskogan forteller at arbeidsfordelingen mellom kommunen og selskapet har vært diskutert i forbindelse med prosjekter. Både daglig leder og styret er oppmerksom på hva som er selskapets oppgave og hva som er kommunens. Det er noen området hvor kommunen selv har ansvaret, da leier Namsskogan kommune inn ansatte fra selskapet. Kommunedirektøren forteller at det er for dårlige rutiner på å dokumentere tidsbruken for den enkelte kommune. Kommunen har ikke god nok kontroll på hvor mye

vedkommende skal jobbe for kommunen og har stilt spørsmål ved om kommunen får det den betaler for.

Kommunedirektøren tror ikke det finnes rutiner for samhandling med selskapet, bortsett fra at det kan finnes noe på avgrensede områder. Kommunedirektøren tror det er klar ansvarsfordeling ved dataangrep, men det er ikke sikkert kommunedirektøren har det helt klart. Selskapet er flink til å følge opp dette.

3.4 Vurdering

3.4.1 Databehandleravtale

Revisjonskriteriet er at det skal foreligge en databehandleravtale mellom kommunen som behandlingsansvarlig og IKT Indre Namdal IKS som databehandler.

Revisor finner at det ikke er utarbeidet noen databehandler avtale eller noe annet avtaleverk som avklarer hva som er kommunenes ansvar og IKT Indre Namdal IKS sitt ansvar. IKT Indre Namdal IKS har satt i gang en prosess med utarbeidelse av en databehandleravtale. Kravet om databehandleravtale ble veldig tydelig med innføringen av lov om personopplysninger i 2018. Det har vært en arbeids- og ansvarsfordeling mellom selskapet og kommunene som har blitt til underveis og som ikke har blitt utfordret med ulike oppfatninger.

Revisor vurderer at det ikke finnes noen databehandleravtale mellom selskapet og kommunene, men at selskapet har satt i gang en prosess for å få på plass en databehandleravtale.

3.5 Kommunenes dokumentasjon på GDPR

Dette er et beskrivende kapittel som ser på kommunenes dokumentasjon innenfor GDPR med spesiell vekt på ivaretakelsen av prinsippene for behandling av personopplysninger, sikkerhetsmål og sikkerhetsstrategier. Beskrivelsen er basert på intervjuene med kommunedirektørene og daglig leder i selskapet. Revisor har også hatt tilgang til kvalitetssystemet for tre av kommunene.

3.5.1 Prinsipper for behandling av personopplysninger

Prinsipper for behandling av personopplysninger handler om at kommunen som behandlingsansvarlig må dokumentere at prinsippene for behandling av personopplysninger overholdes. Prinsipper for behandling av personopplysninger handler om:

- Lovlighet, rettferdighet og åpenhet

- Formålsbegrensning - personopplysninger skal kun behandles for spesifikke, uttrykkelige, angitte og legitime formål
- Dataminimering - begrense mengden innsamlede personopplysninger til det som er nødvendig
- Riktighet - personopplysningene skal være korrekte
- Lagringsbegrensning
- Integritet og konfidensialitet
- Behandlingsansvarlig skal ta ansvar for å sikre regeletterlevelse

I 2018 deltok alle kommunene og selskapet på en felles opplæring i GDPR. Rådmannen i Lierne forteller at de i forbindelse med GDPR-opplæring konkluderte med at det var kommunens ansvar å sørge for dokumentasjon og rutiner.

I forbindelse med denne opplæringen startet kommunene å lage en behandlingsoversikt for å svare ut prinsippene for behandling av personopplysninger. Revisor har fått en oversikt fra selskapet som viser alle applikasjoner og systemer som selskapet er i berøring med. Det er skilt mellom hvilke applikasjoner selskapet er behandlingsansvarlig for og hvilke applikasjoner kommunene er behandlingsansvarlig for (jf. kapittel 4.3.5). I kommunenes kvalitetssystem finnes en lignende oppbygd matrise med oversikt over funksjonsområder. Etter revisors vurdering tyder det på at de oversiktene som ligger i kvalitetssystemet er maler fra kvalitetssystemet eller oppstarten på en utfylling. Alle matrisene som er funnet er ufullstendig. Når status på dokumentet er undersøkt viser det at de ikke er revidert i henhold til fristene som ligger i kvalitetssystemet. I flere tilfeller er ikke dokumentene revidert siden 2018.

Revisor har fått tilgang til kvalitetssystemet i tre av fire kommuner. I Namsskogan sitt kvalitetssystem finnes det om lag 50 protokoller som beskriver prinsippene for behandling av personopplysninger i den enkelte applikasjon. Namsskogan har protokoller for mange applikasjoner og dermed er mye av dokumentasjonen på plass, men dokumentene er ikke revidert og nye applikasjoner er ikke tatt inn. Ledelsen i Grong kommune forteller at mange protokoller ble laget i fellesskap da de deltok på opplæring. Revisor har ikke funnet protokoller i Grong kommune sitt kvalitetssystem. Det er heller ikke funnet protokoller i Lierne sitt kvalitetssystem og revisor har ikke fått tilgang til å undersøke Høylandet sitt kvalitetssystem.

I kvalitetssystemene er det muligheter for å registrere avvik innenfor GDPR. Revisor har funnet at avvik registreres i to av de tre kommunene.

3.5.2 Sikkerhetsmål og sikkerhetsstrategi

IKT Indre Namdal IKS har sikkerhetsmål og sikkerhetsstrategi som er omtalt nærmere i kapittel 4.3.1. I noen av sikkerhetsmålene omtales ansvarsforholdet mellom selskapet og kommunen. Daglig leder uttaler at dersom kommunene brukte malene ukritisk, burde de skrive avvik med en gang dokumentet ble tatt i bruk, fordi de må tilpasses virksomheten.

I de tre kommunene hvor revisor har fått tilgang til kvalitetssystemet, finnes det dokumenter på sikkerhetsmål, sikkerhetsorganisasjon og sikkerhetsstrategi. Noen omtaler disse tre dokumentene som sikkerhetshåndboka. Sikkerhetsorganisasjonen er fylt ut for alle kommunene. Sikkerhetsmål og sikkerhetsstrategi er utformet i varierende grad. I noen tilfeller finnes det dokumenter som ikke er oppdatert i henhold til kravene som ligger i kvalitetssystemet. For selve sikkerhetsstrategien ligger det en mal i kvalitetssystemet. Innholdet i de tre kommunene sine systemer er i stor grad likt og revisor vurderer at det er mye av malen som ligger der som tekst. Dette er blant annet basert på at for eksempel brannmur, som er selskapets ansvar, er omtalt i kommunens sikkerhetsstrategi uten å henvise til selskapet. I fortsettelsen følger litt mer informasjon fra den enkelte kommune.

Grong

Kommunen har ikke gjennomført risikovurderinger innenfor GDPR, forteller kommunedirektøren. Kommunen har gjennomført en overordnet generell ROS-analyse, der IKT kanskje var en del av den. Det gjøres risikovurderinger knyttet til de ulike fagapplikasjonene og disse journalføres.

I kvalitetssystemet er målet med informasjonssikkerhetsarbeidet i Grong beskrevet slik:

- Medarbeidere i kommunen skal ha en sikker adferd ved behandling av person- og helseopplysninger bygd på kunnskap, holdninger samt gode og dokumenterte rutiner og styringssystemer for håndtering av risiko.
- Kommunen skal tilrettelegge robuste systemtekniske løsninger som sikrer personopplysningenes integritet og god tilgjengelighet til opplysningene samtidig som nødvendige sikkerhetskrav og -standarder oppfylles.
- Personopplysninger skal være tilgjengelige kun for de som er autoriserte (need to know).
- Oppkopling mot nettverk, eksternes tilgang til kommunens IT-løsninger, samt bruk av partnere, leverandører og databehandlere skal kun gjennomføres etter at nødvendige sikkerhetsbehov er kartlagt, dokumentert og ivaretatt.
- Transportabelt IT-utstyr og/eller lagringsmedier med personopplysninger, skal sikres spesielt.

(revidert mars 2021)

Det ligger inne i kvalitetssystemet at ledelsen årlig skal gjennomgå sikkerhetsmål, strategi og organisering av informasjonssystemet og kontrollere om disse er i samsvar med virksomhetens behov. Personalsjefen i Grong kommune opplyser at egenkontroll og ledelsens gjennomgang ikke har vært gjennomført i 2021. Videre informerer personalsjefen i en epost at egenkontroll og ledelsens gjennomgang har ikke vært gjennomført etter at nytt system for GDPR ble innført, det vil si fra 2018. Det vil si gjennomført i henhold til de beskrivelser som finnes i prosedyren for egenkontroll og ledelsen gjennomgang. Det er også enighet i kommuneledelsen at systemarbeidet på GDPR må heves og reimplementeres.

Utvalgte deler av sikkerhetsstrategien som berører forholdet til IKT Indre Namdal IKS er:

- Register/datasystemer som leverandører drifter på vegne av kommunen skal sikres gjennom en Databehandleravtale.
- Brannmurer og tilsvarende sikkerhetsbarrierer skal nyttes for å oppnå et sikkert skille mellom kommunen og eksterne nett.
- Alle fellessystemer og fagsystemer skal utarbeides og ivaretas av sikkerhetskopirutinene som IT avdelingen er ansvarlig for.

Lierne

Rådmannen forteller at kommunen har gjennomført risikovurderinger og at kommunen har vært opptatt av dette det siste halvåret.

I dokumentet sikkerhetsmål finnes det 14 sikkerhetsmål. Eksempler på to av målene er:

- Det skal være mulig å spore uønskede hendelser, ved brudd eller mistanke om brudd på personvern.
- Uønskede hendelser skal meldes inn i Compilo, og behandles av leder.

Namsskogan

Kommunedirektøren forteller at det er utført helhetlig ROS-analyse (risiko og sårbarhetsanalyse) som omhandler datainnbrudd og andre uønskede hendelser innen IKT. I 2018 ble det også gjennomført en ROS-analyse innenfor GDPR og det foreligger rutiner for informasjonssikkerhet i kvalitetssystemet Compilo.

Sikkerhetsmål for Namsskogan er:

- Namsskogan kommune skal støtte og sikre at alle ansatte i kommunen vet hvordan behandling av personopplysninger skal foregå i daglig drift, og for å sikre allmenne tillit til behandling og omdømme i det offentlige rom.
- Organisasjonen og alle ansatte skal forebygge og avgrense konsekvensene av uønskede hendelser som kan medføre at informasjon kommer på avveie.

- Namsskogan kommunes overordnede mål er å verne kommunen sin informasjons-behandling mot interne og eksterne trusler av tilsiktet og utilsiktet art. Namsskogan kommune skal sikre den registrerte sine rettigheter og hindre at grunnleggende personvern blir krenket.

3.5.3 Oppsummering

Kommunene er behandlingsansvarlige og skal dermed dokumentere at de følger prinsippene for behandling av personopplysninger. Revisor finner at dokumentasjon på ivaretakelse av prinsippene for behandling av personopplysninger er svært mangelfull. Selskapet har en oversikt, men det er den enkelte kommune som har ansvaret for å dokumentere at prinsippene overholdes. Artikkel 5 i forordningene gir kommunene ansvaret.

Kommunene har sikkerhetsmål, sikkerhetsorganisasjon og sikkerhetsstrategi, men det ligger ikke risikovurderinger til grunn i alle kommunene. Når det gjelder sikkerhetsstrategiene synes disse å følge en mal, både når det gjelder overskrifter og innhold eller en kombinasjon av en mal og felles innhold for kommunene. Etter revisors oppfatning inneholder sikkerhetsstrategien forhold som i arbeidsfordelingen ligger til IKT Indre Namdal IKS, eksempelvis brannmurer og sikkerhetskopiering. Det framgår ikke av sikkerhetsstrategien hvilken rolle IKT Indre Namdal IKS har i kommunenes sikkerhetsstrategi. Kommunenes dokumenter er ikke oppdaterte.

4 INFORMASJONSSIKKERHET I IKT INDRE NAMDAL IKS

Dette kapitlet handler om hvordan IKT Indre Namdal IKS håndterer kravene til informasjonssikkerhet i rollen som databehandler.

4.1 Problemstilling

Følgende problemstilling besvares:

Følger IKT Indre Namdal IKS kravene til håndtering av informasjonssikkerhet?

4.2 Revisjonskriterier

Følgende revisjonskriterier er utledet for problemstillingen om informasjonssikkerhet. Revisjonskriteriene er utledet i vedlegg en.

- Databehandler skal ha sikkerhetsmål og sikkerhetsstrategi.
- Databehandler skal dokumentere vurderingen av risiko og gjennomførte og planlagte sikkerhetstiltak.
- Databehandler skal ha et internkontrollsystem som bygger på risikovurderinger.
- Det skal finnes databehandleravtaler med det innholdet personvernforordningen krever.
- Databehandler skal føre protokoll over alle kategorier av behandlingsaktiviteter som er utført på vegne av behandlingsansvarlig.
- Databehandler skal ha gjennomført egnede tekniske tiltak.
- Databehandler skal ha gjennomført egnede organisatoriske tiltak.
- Databehandler skal ha personvernombud.

4.3 Informasjonssikkerhet i IKT Indre Namdal IKS

I denne delen presenteres data omkring informasjonssikkerhet i IKT Indre Namdal IKS. På noen områder er arbeidet tett koblet til det som gjøres i kommunene og da blir kommunes del av arbeidet beskrevet generelt for å gi en mer helhetlig framstilling.

4.3.1 Sikkerhetsmål og sikkerhetsstrategi

IKT Indre Namdal IKS utarbeidet sikkerhetsmål, sikkerhetsstrategi og oversikt over sikkerhetsorganisasjon og ansvar i forbindelse med studium ved Høgskolen i Innlandet i 2018. Daglig leder forteller at dokumentene er selskapets dokumenter, basert på maler i Compilo. De ble utarbeidet i GDPR-prosjektet og kommunene har egne varianter. Selskapet måtte skrive om malene, fordi de ikke passet for selskapet. Dersom kommunene brukte malene ukritisk, burde de skrive avvik med en gang dokumentet ble tatt i bruk, fordi de må tilpasses virksomheten.

Sikkerhetsorganisasjon og ansvar

Behandlingsansvarlig er ansvarlig for informasjonssikkerheten og daglig leder har denne rollen. Selskapet har en sikkerhetsansvarlig som er en av de interne konsulentene. Vedkommende har det overordnede operative ansvaret for informasjonssikkerheten i selskapet. Det er en rolle som ansvarlig for teknisk løsning (systemansvarlig) som ivaretas av daglig leder. Rollen personvernombud ivaretas av en av de andre konsulentene. Ansvarsområdet og myndighet for disse rollene er beskrevet samt ansvaret til alle ansatte.

Sikkerhetsmål

Formålet med sikkerhetsmålene er å støtte og sikre at alle ansatte i selskapet vet hvordan behandling av personopplysninger skal foregå i daglig drift, for å sikre allmenn tillit til behandling og omdømme i det offentlige rom. Sikkerhetsmålene gjelder for alle ansatte i organisasjonen. Ansvaret for sikkerhetsmålene er hos behandlingsansvarlig i selskapet. Det er definert 15 sikkerhetsmål. To eksempel er gitt under.

- Tilgang til system og informasjon for uvedkommende skal forhindres, ved logiske og fysiske sperrer
- Det skal være mulig å spore uønskede hendelser, ved brudd eller mistanke om brudd på personvern

Sikkerhetsstrategi

Formålet med sikkerhetsstrategien er å konkretisere arbeidet med informasjonssystemet og informasjonssikkerheten. Sikkerhetsstrategien har utgangspunkt i sikkerhetsmålene og er en overordnet beskrivelse av ansvars- og myndighetsforhold, forhold til partnere og leverandører samt organisatoriske og tekniske sikkerhetstiltak. Ansvaret ligger hos behandlingsansvarlig, som er daglig leder for selskapet.

Sikkerhetsstrategien er bygd opp med følgende hovedpunkter:

- Kontrakter
- Egenkontroll
- Systemer/behandlinger
- Kommunikasjonsløsninger
- Sikkerhetskopiering
- Generell taushetserklæring
- Opplæring
- Konsekvenser av sikkerhetsbrudd
  Fysisk sikkerhet
- Soneinndeling og adgangskontroll
- Adganger til informasjonssystemer/ behandlinger

- Dokumentsikkerhet
- Konfigurasjonskontroll
- Endringskontroll
- Beredskap
- Tiltak for å hindre uhell/kriser
- Avviksbehandling
- Systemteknisk sikkerhet
- Krav til dokumentasjon av beskyttelsesbehov
- Oversikt over teknisk løsning
- Strategi for systemteknisk sikkerhet
- Datakommunikasjon
- Infrastruktur
- Systemeier/systemansvarlig
- Leverandør/partnere
- Innkjøp av hardware/software
- Hjemmekontorløsninger
- Tilgangskontroll
- Adgangskontroll
- Dokumentsikkerhet

I styremøte 11.11.2020, sak 67/20 datasikkerhet, redegjorde daglig leder for arbeidet med datasikkerhet. Det ble orientert om økt bemanning innenfor sikkerhet fra 2021, økende behov for å arbeide med sikkerhet, kommune CSIRT, Atea IRT og endepunkt sikkerhet.

- *Kommune CSIRT* er et nyopprettet rådgivende organ for å hjelpe kommune med forebyggende arbeid og bistand ved angrep. Som medlemmer vil selskapet og kommunene bli sikret informasjon og kunnskap om et oppdatert trusselbilde.
- *Atea IRT, Incident Response Team*, er en tilleggstjeneste til driftsavtalen med Atea. Med tilleggsavtalen er selskapet garantert rask bistand ved eventuelle angrep. Det inngår også forebyggende arbeid og Atea er operasjonell part ved en hendelse.
- *Endepunktsikkerhet.* Dette handler om behovet for antivirus og andre sikkerhetstiltak framover.

Styret vedtok å be om en handlingsplan for sikkerhet innen utgangen av første halvår 2021 og at den blir en del av selskapets overordnede handlingsplan.

I representantskapsmøtet 28.04.2021, sak 04/21 overordnede mål og retningslinjer for 2021, vedtok representantskapet å inngå avtale med Atea IRT i 2021 og endepunktsikkerhet i 2022.

4.3.2 Risikovurderinger

Prosedyre for akseptabel risiko

I selskapets GDPR-dokumentasjon er det en prosedyre for fastsetting av akseptabel risiko, hvor formålet er å etablere en standard for hvor mye risiko en organisasjon kan akseptere innenfor personvern og informasjonssikkerhet. Akseptabel risiko blir vurdert ved årlig revisjon, for å vurdere om den skal endres som følge av endringer i organisasjon, infrastruktur, registrerte hendelser eller policy. Behandlingsansvarlig skal fastsette akseptabel risiko basert på felles kriteriesett for sannsynlighet og konsekvens. Kriteriesettet er en del av prosedyren. Høyest akseptable risiko er satt til ni, hvor en er lavest og 25 er høyest.

Erfaringer med risikoer

Daglig leder og sikkerhetsansvarlig er samstemt i at brukerne av IKT-systemene er den største risikoen. Selskapet har ikke opplæringsansvar overfor brukere. Nyansatte skal få opplæring av kommunene. Daglig leder ser at selskapet har behov for å sende ut informasjon om sikkerhet og systematisere opplæringen av nyansatte. Det forelå et forslag om å ta i bruk et skybasert program, Jungelmap, hvor ansatte skulle få korte sekvenser på epost med opplæring omkring sikkerhet og bruk av office. Dette programmet er ikke anskaffet.

Når det oppstår eksterne trusler, setter selskapet i verk tiltak for å unngå skader. Det kan for eksempel sendes ut felles epost om kjente phishing-kampanjer. Selskapet informerer ansatte i kommunene om endringer og hvorfor de gjøres, forteller daglig leder. Ansatte i kommunene henvender seg til selskapet om phishing, med spørsmål om eposter er grei og informerer om hva de har fått og slettet.

I 2018-2019 hadde selskapet flere ransom-angrep utelukkende på terminalservere. Første gang brukte de mye tid for å finne ut av det. De neste tre til fire gangene gikk det raskere å finne ut hvem som var angrepet, slette alt og hentet frem backup.

I mars 2021 var det angrep på mailserver, forteller daglig leder. Selskapet trodde de hadde håndtert det fort, men det viste seg at angrepet var startet før varslet kom. Selskapet kjørte alle sjekkene som var anbefalt. Det ble oppdaget aktivitet på serveren natten før varselet, som var et skript som kunne aktiveres senere. Selskapet hadde ikke datatap.

I sikkerhetsstrategien står det i forbindelse med konfigurasjonskontroll at systemeier har ansvaret for å utarbeide og vedlikeholde oversikt over utstyr, programvare og system-konfigurasjon. Ansvaret kan delegeres til systemansvarlig.

Daglig leder forteller at selskapet ikke har kartlagt IKT-utstyr som selskapet bruker og heller ikke kommunenes utstyr. Daglig leder tviler på at kommunene har kartlagt sitt utstyr. Selskapet

har et system hvor PCer er registret sammen med hva som er installert på dem. Dette systemet ble anskaffet i forbindelse med en lisensrevisjon. Daglig leder er usikker på om selskapet får beholde systemet på grunn av økonomiske innstramninger. I dette systemet har selskapet oversikt over nettverksadresser på alle enheter, så lenge kommunene registrerer dem. Dette omfatter bare faste adresser.

Selskapet administrerer brukerlisenser i hovedsak på Microsoft 365. Selskapet har god kontroll over egne brukerlisenser og rapporterer til leverandør en gang i året, mens kommunene har en gjennomgang av sine brukere i Microsoft CSP[4] to ganger i året, forteller daglig leder. Ansatte får ikke logget på PCer uten lisens. Det er også noen datacenterlisenser. For administrasjon og helse er det en entrepriseavtale med servere og en del brukerlisenser inkludert i avtalen. De øvrige brukerlisensene er på en CSP-avtale. Lisenser justeres nesten ukentlig, og kommunene tildeler lisenser gjennom autorisasjonsportalen. Selskapet er ansvarlig for drift av løsningen, mens kommunene administrerer brukerne.

Daglig leder forteller at selskapet ikke har noe konfigurasjonskart som viser selskapets IKT-infrastruktur. Dette er dokumentasjon som skal utarbeides av den nye sikkerhetsstillingen. Selskapet har gjort mye praktisk bra og systemdokumentasjonen er i orden. Overordnet dokumentasjon er ikke prioritert. Selskapet skal sammen med Atea lage mal for prinsippskisser og beskrive infrastruktur og hvordan ulike deler henger sammen. Dokumentasjonen må være laget slik at alle forstår og kan brukes i GDPR-arbeidet. En slik dokumentasjon vil beskrive hvor data ligger, backup-rutiner og hvor lenge det lagres. Selskapet skal lage detaljerte tegninger for eget bruk.

For noen år siden ønsket selskapet midler til å gjennomføre penetrasjonstester, men fikk ikke det. Nå har selskapet inngått en avtale med Atea som sikrer at selskapet vil bli prioritert og få hjelp raskt hvis det skjer noe. Atea kan bistå i hele håndteringen av en hendelse både i forhold til Datatilsynet, media og det tekniske. Avalen ble inngått sommeren 2021 og det skal være månedlige statusmøter. I statusmøtene gjennomgås de siste oppdateringene på selskapets systemer og det utformes en liste over prioriterte tiltak.

Atea har direkte overvåkning av selskapets system. Atea håndterer brannmurer i en egen driftsavtale. NTE overvåker internettlinje og kommunikasjon mellom alle kommuner og datarom på Steinkjer.

[4] Microsoft CSP (cloud solution provider)

4.3.3 Internkontrollsystem

Selskapet er opptatt av sikkerhet, forteller daglig leder. Det de mangler er dokumentasjon på hvordan internkontrollsystemet fungerer. De siste to årene har selskapet gjort flere tiltak som har løftet sikkerheten betydelig, slik som

- Segmentere nettverk
- Logging av aktivitet
- Ikke lokale administratorrettigheter
- Personlige administratorkontoer, ikke felles
- To-faktor tilgang

Uten et internkontrollsystem er det vanskelig å prioritere arbeidet med internkontroll. Hvis selskapet hadde et internkontrollsystem, ville de startet med å få på plass dokumentasjon av internkontrollen for selskapet. Det må også lages en avtale med kommunene som beskriver ansvarsfordelingen.

Daglig leder opplyser i etterkant av intervjuet at styret bevilget midler til å anskaffe et oppgaveorientert internkontrollsystem som følger GDPR, ISO 27001 og ISO 27002. Selskapet har fått en demobruker og vil undersøke funksjonaliteten før avtale inngås. I høringssvaret opplyses det at selskapet har gjort ytterligere vurderinger av løsningen og avtale vil bli inngått i januar 2022.

4.3.4 Databehandleravtaler

Daglig leder forteller at selskapet inngår databehandleravtaler med leverandørene om systemer. Noen leverandører ønsker avtaler direkte med kommunene, mens andre vil ha avtale med selskapet. Det varierer hvor medgjørlig leverandørene er. Leverandørene ønsker også å benytte egne standardavtaler. I de tilfellene leverandørene ønsker databehandleravtale med selskapet, signerer selskapet uten å være behandlingsansvarlig. Selskapet sliter med å finne løsning på dette. Daglig leder opplyser at det er satt i gang et arbeid med databehandler-avtale mellom selskapet og kommunene. Det er uklart hva utfallet blir. Enten lages det en generell avtale mellom selskapet og kommunene som viderefører behandlingsansvaret eller at den enkelte leverandør må inngå avtaler direkte med kommunene.

Selskapet har databehandleravtale med Atea. Den er korrekt. Det mangler en generell avtale mellom selskapet og kommunen, med Atea som tredjepart.

Databehandleravtalene med leverandørene blir oppdatert ved endringer eller tilleggs-bestillinger, forteller daglig leder.

4.3.5 Behandlingsaktiviteter

IKT Indre Namdal har en behandlingsoversikt, sist ajourført 11.10.2021. I denne oversikten står ESA8 som sak- og arkivsystem. Det er opplyst fra kommunene at de tok i bruk Elements som sak- og arkivsystem i juni 2021. I høringssvaret fra selskapet presiseres det at denne behandlingsoversikten ble laget i 2018 sammen med kommunene. I oversikten er applikasjoner som kun brukes av kommunene markert og ESA8 er en av dem.

I oversikten har hver applikasjon (fagsystem/arkivsystem) sin linje. For hver applikasjon er formålet beskrevet, om det registreres personopplysninger, sensitive personopplysninger eller ikke personopplysninger, høyeste score på ROS-analyse, hjemmel for behandling og om det finnes en databehandleravtale. Kolonnen for ROS-analyse er ikke utfylt. I behandlings-oversikten er det 136 applikasjoner, hvorav 28 berører selskapet og de resterende er knyttet til kommunene.

Daglig leder vet ikke om kommunene bruker behandlingsoversikten og tror at det er forskjell på hvor mye kommunene har arbeidet med GDPR etter at de gjennomførte prosjektet.

Behandlingsoversikten sier ikke noe om dataminimering (ikke lagre mer data en nødvendig) og det er ikke fastsatt noen policy på lagringstid. Selskapet har retningslinjer for hvor ofte de skal ta back-up av data, men har ikke oversikt over hvor lenge data skal tas vare på. Selskapets erfaring er at kommunene kvitter seg med gamle data når systemer blir skiftet ut, bortsett fra det som de er pliktig å ta vare på ifølge arkivloven.

Da det skulle byttes skoleadministrativt system for noen år siden, gikk leverandøren konkurs før de hadde skiftet system. Kommunene hadde papirarkiv og skulle ta ansvaret for å rydde opp. De måtte ha en kassasjonsplan fra arkivet, men arbeidet stoppet opp og det ble besluttet å slette data fra systemet, og data skal finnes på papir. Daglig leder forteller at ulike prosjekter det siste året har gjort at arkivarene i kommunene forstår bedre hva som ligger i deres rolle opp mot IKT-systemene. I forbindelse med overgangen til nytt sak- og arkivsystem ble det laget en plan for denne overgangen.

Selskapet har ingen egen oversikt over hvor det ligger lagret personopplysninger ut over det som finnes i behandlingsoversikten. Daglig leder ønsker en bedre oversikt og hvordan dette er koblet til to-faktor autentisering.

4.3.6 Tekniske og organisatoriske tiltak

Sikkerhetsstrategien omhandler både fysiske og organisatoriske tiltak. Presentasjonen av de tekniske og organisatoriske tiltakene bygger på beskrivelsen som ligger i sikkerhetsstrategien og informasjon fra intervjuet med selskapet.

Systemteknisk sikkerhet

Et punkt omtaler systemteknisk sikkerhet. Betydningen av tilgjengelighet, konfidensialitet og integritet er avhengig av det enkelte system og den informasjonen som blir behandlet i systemet. Det skilles mellom tre ulike beskyttelsesbehov:

- Høy - gjelder bare system og informasjon der uønskede hendelser kan være kritiske for organisasjonen eller den registrerte.
- Middels - gjelder system og informasjon med beskyttelsesbehov.
- Lav - kan gjelde alle system og informasjon med lite eller ingen behov for beskyttelse.

Ulike delsystem kan ha ulikt beskyttelsesbehov. Løsningen skal være i henhold til de krav som stilles fra Datatilsynet når det gjelder åpent og lukket segment med nødvendige brannmurer for å hindre at uautoriserte får tilgang til sensitive data.

Det skal være tilgangskontroll slik at tilgangen til systemer som inneholder personopplysninger skal være styrt. Sensitive personopplysninger skal i tillegg beskyttes av brukernavn og passord, samt to-faktor autentisering der det er mulig.

I sikkerhetsstrategien står det også at systemansvarlig er ansvarlig for at det finnes oppdatert dokumentasjon over infrastruktur. Her går det fram at selskapets nett skal deles inn i soner hvor det er definert hvilke soner som kommuniserer med andre interne eller eksterne soner. Brannmurer og tilsvarende sikkerhetsbarrierer skal benyttes for å oppnå et sikkert skille mellom kommunene og eksterne nett. All kommunikasjon rutes via sikkerhetsbarrierer. Ved behandling av sensitive personopplysninger skal det være to sikkerhetsbarrierer mellom sikker sone og eksternt nett. Det skal være elektronisk overvåkning av nettverkstrafikken mot virksomhetskritiske systemer og nettverk i selskapet. Support fra leverandører over ekstern linje skal benytte VPN-løsning[5] med kryptering eller annen sikker kommunikasjon.

Backup

Daglig leder forteller at selskapet sitt datasenter er på Steinkjer. Kommunene kan ha egne servere, men det meste er på vei til å fases ut eller er faset ut. Datasenteret på Steinkjer tar daglig backup av alt. Det lagres først på hurtiglager og overføres til backup-enhet. En gang i måneden tas det ut backup på tape som oppbevares adskilt fra serverrommet. Selskapet har ikke oversikt over hvordan backup foregår i fagsystemene, men dette står beskrevet i avtalene med de ulike leverandørene. Selskapet kjenner ikke de tekniske detaljene og må forholde seg

[5] VPN-løsning, VPN betyr virtuelt privat nettverk. Det innebærer en kryptering av all datatrafikk før den forlater PCen og sendes til en server et annet sted hvor den dekrypteres og forlater serveren til det tiltenkte målet som om PCen skulle befunnet det der.

til avtalene. I høringssvaret presiseres det at dette ikke gjelder alle fagsystemer. Fagsystem som er installert og driftet i IKT Indre Namdal IKS sin infrastruktur blir håndtert i selskapets backup-løsning. Applikasjoner som leveres som en tjeneste (skyløsning) har ikke selskapet detaljerte opplysninger om backup, men i avtalen med leverandøren går det fram at leverandøren påtar seg ansvar for sikkerhet og backup.

Brannmurer

Selskapet har to sentrale brannmurer på Steinkjer for alle kommunene. All trafikk går via dem. Der håndteres skillet mellom intern og sikker sone. Helse er på sikker sone og har ikke internett og får ikke til å flytte filer inn og ut av sikker sone. Det er det bare administrator som kan. Det er ikke mulig å kopiere tekst eller ta skjermbilder.

Kryptering

Selskapet har ingen kryptering ut over det som eventuelt ligger i systemene. Alt som ligger i Microsoft, er kryptert.

Sikkerhetsoppdateringer

Alt selskapet gjør er for at systemene skal være sikre og i drift, forteller daglig leder. I perioder kan det være ustabilt. Endringstakten har økt betydelig og nå får selskapet jevnlig mange varsel om sårbarheter med høg kritikalitet. Noen ganger avventes ikke sikkerhetsoppdateringer selv om det kan gå ut over oppetid på applikasjonene. Selskapet bruker mye ressurser på dette i tillegg til å rydde opp i uønskede konsekvenser som følge av bruken av løsninger. Daglig leder mener at dette er den nye normalen.

Overvåkning

Selskapet har tilgang til hele infrastrukturen og alle systemer og kan følge med på at servere, linjer og tjenester fungerer. Atea har også overvåkning av selskapets IKT-infrastruktur, men selskapet har ikke direkte tilgang til denne overvåkningen. Selskapet har egen overvåkning på noen servere som for eksempel kan varsle om lite lagringsplass, manglende nettverkstilgang og lignende problemer.

Gjennom kundeportalen kan selskapet se hvilke tjenester som er oppegående. Brannmurene varsler om det er ting som ikke er greit, det samme gjør antivirus. Daglig leder og sikkerhetsansvarlig får brannmur-rapporter. Det genereres 15-20 rapporter hver natt til mandag, med oversikt over hva som har skjedd siste uke. Etter hvert danner det seg et bilde av hva som er normal bruk av systemene og rapportene viser hva brannmuren har stoppet av uønsket adferd.

Leverandørene gir selskapet informasjon om sikkerhetsutfordringer og kjente sårbarheter på alle systemer. Hvis selskapet får beskjed om en kjent sårbarhet på et system som selskapet drifter, meldes det inn en sak til Atea og de undersøker om dette gjelder selskapets system.

Selskapet kjøper DDoS-tjeneste[6] fra NTE. DDoS stopper og filtrerer bort hvis det er store mengder trafikk som ikke er normal. På NTE er det døgnvakt som får varsel om betydningsfulle ting som skjer. Det har vært lite av dette i det siste, forteller daglig leder.

Informasjon til kommunen

Kommunedirektørene får informasjon fra selskapet hvis det oppstår store sårbarheter, slik at de vet hva som foregår. Daglig leder forteller at de gjør en vurdering av nytten av å informere og hvem som er rett mottaker. Sikkerhet er en fast sak i styremøtene (omtalt i kapittel 4.3.1) og daglig leder informerer da om hva selskapet gjør konkret.

Sikkerhetsmåling

Selskapet har ingen egne målinger på sikkerhetsnivået, men har en hatt dialog med Atea og den overvåkningen de gjør. Daglig leder informerer om at de etter intervjuet med revisjonen har mottatt rapporter fra et internt sårbarhets-scan. Dette er et av tiltakene som ligger i Atea IRT-avtalen. Rapporten viste at *overall business risk* var lav. Det ble avdekket mange sårbarheter, men veldig få med høg kritikalitet. Ingen av systemene som ble rapportert som kritisk eller høy er veldig kritiske for selskapet. Daglig leder vil jobbe for å finansiere en ukentlig scanning på sikkerhetsnivået.

Avvik fra arkivverket

En av kommunene har fått avvik fra Arkivverket. Dette skyldtes muligheter for tilgang mellom kommunenes arkiver. Daglig leder forteller at det tidligere saksbehandlingssystemet hadde felles arkivkjerne for kommunene. I praksis har kommunene vært adskilt gjennom bruker-tilganger. Hver kommune avgjør hvem som skal ha brukertilgang i det felles arkivet. I teorien kunne en administrator i en kommune gi tilganger til ansatte i en annen kommune. I tilsynet ble det også påpekt at det var felles løpenummerserie i saksbehandlingssystemet. Avviket er lukket og kommunene har tatt i bruk nytt sak- og arkivsystem.

Brukertilganger

[6] DDoS-tjeneste. DDoS står for *distributed denial of service* eller distribuert tjenestenekt. En tjeneste som beskytter mot DDoS angrep ved å bryte tilgjengeligheten til informasjonen. Et DDoS-angrep kjennetegnes ved at et nett av datamaskiner oversvømmer en nettside eller en annen ressurs på nettet, for å hindre at legitime brukere får tilgang til tjenesten (nettvett.no/ddos-angrep/, lastet ned 17.12.2021).

Lisenser er omtalt i kapittel 4.3.2 og henger sammen med at en bruker må han en lisens for å få tilgang til datasystemet. Det er kommunene som håndterer brukertilganger gjennom en egen autorisasjonsportal. Selskapet fakturerer kommunene to ganger i året for bruken av lisenser. I forkant sendes det ut en liste over antall brukere og kommunene bruker å se over lista slik at den stemmer. Kommunen har egeninteresse av ikke å betale for flere lisenser enn hva de bruker. Selskapet har mulighet til å ta ut oversikter over ansattes tilganger til applikasjoner. Det arbeides med en ny løsning som skal erstatte autorisasjonsportalen.

Beredskap

Om beredskap står det at ansvar og håndtering av hendelser skal være avklart i organisasjons-kart og stillingsomtaler. Videre at effektiv håndtering skal sikres gjennom rutiner som er tilgjengelig for relevante personer. Hendelser skal handteres i tråd med alvoret i hendelsen. Varslingsrutiner skal eksistere der både relevant personell i selskapet, og andre relevante partnere inngår. Drift og plan for å gjenopprette normaldrift skal finnes.

Dokumentsikkerhet

Sikkerhetsstrategien stiller krav til dokumentasjon av beskyttelsesbehov. Det omfatter blant annet å vedlikeholde en oversikt over behandling av personopplysninger.

Om dokumentsikkerhet står det at alle selskapets rutiner og avvik finnes i kvalitetssystemet KSS. Videre at alle prosedyrer og dokumenter skal revideres en gang per år i samsvar med kravene i internkontrollforskriften.

Selskapet har utfordringer med å sette ting i system og dokumentere, forteller daglig leder. Det skjer mange endringer og det vil være behov for selskapets tjenester framover.

Taushetserklæring

Daglig leder forteller at ansatte i selskapet har signert taushetserklæring som en del av arbeidsavtalen. Dette gjelder uavhengig av hvilken kommune de arbeider med. Kommunene har egne taushetserklæringer.

Avvik

Selskapet har ikke avvikssystem, forteller daglig leder. I selskapets helpdesk dokumenteres avvik knyttet til applikasjonene. Kommunene bruker Compilo som avvikssystem. Selskapet har kun GDPR-modul i Compilo.

Ressurser og samarbeid

Det er utredet et større samarbeid med Steinkjer og videre er Nærøysund og Namsos forespurt om samarbeid. I utredningen med Steinkjer ble ulike løsninger og felles ressurser undersøkt. Selskapet har mye som er likt med Steinkjer og de har også Atea som samarbeidspart, noe som vil forenkle et nærmere samarbeid. Utredningen var på et overordnet nivå og det ble reist spørsmål om viljen til samarbeid på tjenestenivå, men det ble ikke gått videre med undersøkelser om dette. Så langt har det ikke vært noen interesse fra Nærøysund eller Namsos, mest sannsynlig fordi de har vært opptatt med kommunesammenslåing. Tilgangen på ressurser i kommunene er den største utfordringen for å gjennomføre prosjekter.

I høringssvaret presiseres det at selskapet er avhengig av nøkkelpersoner i kommunene for å gjennomføre prosjekter. Nøkkelpersoner har ofte flere roller i egen kommune, og det kan derfor by på utfordringer å prioritere tid til slike oppgaver. Selskapet må derfor sette frister for å sikre nødvendig framdrift for fellesskapet. Selskapet opplever at kommunene har begrensede ressurser til å følge med utviklingen innenfor det enkelte fag. Med dagens utviklingstakt kommer det stadig nye løsninger og muligheter i markedet. Kommunene må følge med på denne utviklingen, ettersom selskapet verken har ressurser eller kompetanse til å vurdere hva som er relevant og nødvendig innenfor det enkelte fagfelt. Personvernombud

Av dokumentet sikkerhetsorganisasjon og ansvar går det fram at en av de ansatte konsulentene er personvernrådgiver. Beskrivelsen av ansvarsområdet for personvernrådgiver viser at dette er rollen til personvernombudet.

4.4 Vurdering

4.4.1 Sikkerhetsmål og sikkerhetsstrategi

Revisjonskriteriet er at databehandler skal ha sikkerhetsmål og sikkerhetsstrategi.

Revisor finner at IKT Indre Namdal IKS har sikkerhetsmål og sikkerhetsstrategi for selskapet. Denne bygger på malen i Compilo og er tilpasset selskapet og omhandler selskapet og ikke kommunene.

Revisor vurderer at IKT Indre Namdal IKS har sikkerhetsmål og sikkerhetsstrategi.

4.4.2 Risikovurderinger

Revisjonskriterier sier at databehandler skal dokumentere vurderingen av risiko og gjennomførte og planlagte sikkerhetstiltak.

Revisor finner at IKT Indre Namdal IKS i liten grad har dokumentert risikovurdering. Revisors inntrykk er at det gjøres løpende risikovurderinger i selskapet, at selskapet har erkjent risiko og at selskapet blant annet gjennom avtaler med Atea og NTE har gjort sikkerhetstiltak. Revisor oppfatter at det er gode risikovurderinger som gjøres og at selskapet har en saklig tilnærming til risikovurderingene. Selskapet har også hatt ønsker om andre sikkerhetstiltak som det ikke har blitt bevilget midler til.

Revisors vurdering er at IKT Indre Namdal IKS ikke har dokumentert risikovurderinger, men at selskapet har gjort sikkerhetstiltak.

4.4.3 Internkontrollsystem

Revisjonskriteriet er at databehandler skal ha et internkontrollsystem som bygger på risikovurderinger.

Revisor finner at selskapet ikke har noe internkontrollsystem, men at det er planer om å anskaffe.

Revisor vurderer at IKT Indre Namdal IKS ikke har noe internkontrollsystem.

4.4.4 Databehandleravtaler

Revisjonskriteriet er at det skal finnes databehandleravtaler med det innholdet personvern-forordningen krever.

Revisor finner at IKT Indre Namdal IKS har databehandleravtaler med leverandører av systemer. Hvis det hadde vært en databehandleravtale mellom selskapet og kommunene som behandlingsansvarlig, hadde denne kunne åpnet muligheten for at selskapet kunne hatt databehandleravtaler på vegne av kommunene. Punkt to i artikkel 28 i forordningen åpner for at en databehandler kan engasjere en annen databehandler hvis det finnes en særlig eller generell skriftlig tillatelse fra den behandlingsansvarlige (kommunen). Revisor har ikke gått nærmere inn på innholdet i databehandleravtalene ettersom flere av disse er standardiserte avtaler utarbeidet av leverandørene.

Revisor vurderer at IKT Indre Namdal IKS har databehandleravtaler med sine leverandører. Det mangler databehandleravtale mellom selskapet og kommunene som påpekt i kapittel 3.

4.4.5 Behandlingsaktiviteter

Revisjonskriteriet er at databehandler skal føre protokoll over alle kategorier av behandlings-aktiviteter som er utført på vegne av behandlingsansvarlig.

Revisor finner at IKT Indre Namdal IKS har en protokoll over behandlingsaktiviteter som er en bruttoprotokoll over selskapets og kommunenes behandlingsaktiviteter. En databehandleravtale mellom selskapet og kommunene vil klargjøre ansvaret for behandlingsaktiviteter.

Revisor vurderer at IKT Indre Namdal IKS har en protokoll over behandlingsaktiviteter, men den har flere mangler.

4.4.6 Tekniske og organisatoriske tiltak

Revisjonskriteriet sier at databehandler skal ha gjennomført egnede tekniske og organisatoriske tiltak.

Revisor finner at selskapet er opptatt av organisatoriske tiltak, men at det er lite dokumentasjon ut over saker til styret. Selskapet framstår som veldig operativt og handlingsorientert, men mangler mye dokumentasjon som setter både tekniske og organisatoriske tiltak i system. Det er en erkjennelse at selskapet er lite og at det er fornuftig å samarbeide med andre om ulike løsninger og tiltak, blant annet for å ha god ressursutnyttelse og et større fagmiljø å støtte seg til. Det er revisors oppfatning at selskapet jobber innenfor et krevende fagområde som stiller store krav til faglig oppdatering og rask støtte til kommunene når det trengs. Med knappe ressurser blir den operative virksomheten og akutte hendelser prioritert i hverdagen, og ikke utviklingsarbeidet.

Revisor finner at selskapet har iverksatt ulike tekniske tiltak selv eller i samarbeid med andre. Etter revisors oppfatning er det uklart om de tekniske tiltakene har sitt utspring i risikovurderinger og internkontrollsystemet, fordi slik dokumentasjon mangler. Revisor opplever det er en god vurdering av hva selskapet klarer selv og det er betryggende at selskapet samarbeider og kjøper tjenester fra NTE og Atea. Det kan forventes at de har mer spisskompetanse og er mer oppdatert på sikkerhetsutfordringer som finnes. Samtidig er det selskapet selv som best kjenner til forhold som påvirker eget risikobilde og delvis kommunene sitt. Arbeidet med informasjonssikkerhet er omfattende og krevende, ikke minst fordi det hele tiden skjer en internasjonal utvikling på området. Derfor er det fornuftig å ha en hierarkisk oppbygging av informasjonssikkerhetsarbeidet gjennom avtaler med eksterne.

Ved et par anledninger kommer det fram at daglig leder ønsker å investere i flere tekniske sikkerhetstiltak, men at det er knapt med ressurser og alt blir ikke prioritert av styret eller eiere.

Revisor vurderer at selskapet gjennomfører egnede tekniske og organisatoriske tiltak innenfor de økonomiske rammene selskapet har, men at det mangler dokumentasjon på systemer.

4.4.7 Personvernombud

Databehandler skal ha personvernombud

Revisor vurderer at en av konsulentene i selskapet har rollen som personvernombud.

5 HØRING

En foreløpig rapport ble sendt på høring til selskapet, samt til eierrepresentantene og kommunedirektørene i kommunene 21.12.2021. Det blir opplyst om at høringssvaret legges ved endelig rapport og at revisor vil korrigere eventuelle faktafeil i tråd med tilbakemeldingene.

Revisjon Midt-Norge SA mottok svar fra IKT Indre Namdal IKS ved daglig leder og styreleder 09.01.2022. Høringsbrevet er vedlagt rapporten (vedlegg to). Revisor har korrigert faktafeil i tråd med tilbakemeldingene fra selskapet. Høringssvaret har ut over dette ikke medført endringer i rapporten.

Den foreløpige rapport ble også sendt på høring til den enkelte eierkommune 21.12.2021 ved kommunedirektøren og eierrepresentanten. Kommunedirektøren fikk rapporten på høring fordi det er spesielt kapitlet om ansvars- og arbeidsfordeling som berører kommunedirektørens ansvarsområde. Revisjon Midt-Norge SA mottok svar fra eierrepresentanten i Høylandet kommune 20.01.2022. Høringsbrevet er vedlagt rapporten (vedlegg tre). Under er det redegjort for hvordan revisor har svart ut høringsuttalelsen.

5.1 Høringssvar fra selskapet

Selskapet ved daglig leder og styreleder har gitt en høringsuttalelse som er vedlagt i vedlegg to.

Revisjon Midt-Norge SA tolker kommentarene til eierskapskontrollene som supplerende og oppdaterte opplysninger. De oppdaterte opplysningene er tatt inn i rapporten. I høringssvaret er det også vist til hvilke planer som foreligger for å følge opp noen av anbefalingene. Anbefalingen om styrevervregisteret er tatt ut i de kommunene hvor styremedlemmene er registrert.

Selskapets kommentarer til kapitlet ansvars- og arbeidsfordeling gir oppdaterte opplysninger som er tatt inn i rapporten. Revisor har også utdypet vurderingen om databehandleravtale.

Selskapets kommentarer til kapitlet om informasjonssikkerhet i IKT Indre Namdal IKS er oppdatert informasjon, presiseringer og nyanseringer som er tatt inn i rapporten.

Selskapets kommentarer til konklusjon og anbefalinger forstås som en oppdatert informasjon om hvordan selskapet har startet å arbeide med databehandleravtaler og internkontrollsystem, for å følge opp vurderinger og anbefalinger til selskapet. Revisor har ikke endret noe på konklusjon og anbefalinger.

5.2 Høringssvar fra eierrepresentant Høylandet

Eierrepresentanten har gitt en høringsuttalelse om eierskapskontrollen. Revisor har tatt inn supplerende opplysninger og presiseringer. Informasjonen om oppnevning av eier-representant er tatt inn og har ført til endret vurdering og konklusjon.

Eierrepresentanten har også kommentert forhold omkring kommunikasjonsformen mellom eierrepresentant og eier. Deler av dette er tatt inn i teksten og vurderingen er endret og det får også betydning for konklusjonen.

6 KONKLUSJONER OG ANBEFALINGER

6.1 Konklusjon

I dette kapitlet konkluderes det på de to problemstillingene som omhandler forvaltnings-revisjonen i selskapet.

- Er ansvars- og arbeidsfordelingen for informasjonssikkerheten klarlagt mellom IKT Indre Namdal IKS og kommunen?

Revisor konkluderer med at ansvars- og arbeidsfordelingen mellom den enkelte kommune og IKT Indre Namdal IKS ikke er klarlagt. Selskapsavtalen gir noen overordnede føringer for forholdet mellom selskapet og eierkommunen. Det finnes ingen databehandleravtale, noe som lov om personopplysninger stiller krav om. Mye av kommunenes dokumentasjon på GDPR-området er utdatert og mangelfullt. Denne dokumentasjonen fanger ikke opp forholdet til IKT Indre Namdal IKS.

- Følger IKT Indre Namdal IKS kravene til håndtering av informasjonssikkerhet?

Revisor konkluderer med at IKT Indre Namdal IKS har svakheter i oppfølging av kravene til informasjonssikkerhet. Selskapet har mye god praksis, men mangler vesentlig dokumentasjon som personvernforordningen krever. Følgende svakheter er funnet.

- Risikovurderinger er ikke dokumentert
- Selskapet har ikke noe internkontrollsystem
- Selskapet har databehandleravtaler med leverandører, men mangler databehandler-avtaler med kommunene
- Protokollen over behandlingsaktiviteter er mangelfull og ikke oppdatert
- Det er gjort tekniske og organisatoriske tiltak innenfor de økonomiske rammene selskapet får, men det mangler dokumentasjon på flere av tiltakene

6.2 Anbefalinger

Revisor anbefaler IKT Indre Namdal IKS å:

- sørge for at kravet om databehandleravtale i tråd med personopplysningsloven følges opp. Herunder at arbeids- og ansvarsfordelingen mellom selskapet og eierkommunene blir klarlagt og dokumentert.
- sørge for at kravene i personopplysningsloven oppfylles.

KILDER

eForvaltningsforskriften. FOR-2004-06-25-988. Forskrift om elektronisk kommunikasjon med og i forvaltningen. Kommunal- og moderniseringsdepartementet.

Forvaltningsloven. LOV-1967-02-10. Lov om behandlingsmåten i forvaltningssaker. Justis- og beredskapsdepartementet.

IKS-loven. LOV-1999-01-29-06. Lov om interkommunale selskap. Kommunal- og moderniseringsdepartementet.

Kommuneloven. LOV-2018-06-22-83. Lov om kommuner og fylkeskommuner. Kommunal- og moderniseringsdepartementet.

KS (2020). Anbefalinger om eierskap, selskapsledelse og kontroll. KS Folkevalgtprogram 2019-2023. KS

Personopplysningsloven. LOV-2018-06-15-38. Lov om behandling av personopplysninger. Justis- og beredskapsdepartementet.

Utviklingsstrategi for driftsplattformen 2020-2024 for IKT Indre Namdal IKS. Vedtatt av representantskapet for IKTIN 27.04.2020, sak 07/20.

VEDLEGG 1 – UTLEDNING AV REVISJONSKRITERIER

Ifølge forskrift om kontrollutvalg og revisjon (§ 15) skal det etableres revisjonskriterier for gjennomføring av forvaltningsrevisjon. Revisjonskriterier er de krav og forventninger som forvaltningsrevisjonsobjektet skal revideres/vurderes i forhold til. Disse kriteriene skal være begrunnet i, eller utledet av, autoritative kilder innenfor det reviderte området. Slike autoritative kilder kan være lov, forskrift, forarbeider, rettspraksis, politiske vedtak (mål og føringer), administrative retningslinjer, samt statlige føringer og praksis. I eierskapskontrollen benyttes vurderingskriterier i tråd med RSK 002, som er standarden for eierskapskontroll.

A. Eierskapskontroll

Styringsdokumenter

IKT Indre Namdal IKS er et interkommunalt selskap og styrt av IKS-loven (Lov 29.01.1999 nr.6). Lovens § 3 slår fast at hver deltaker hefter ubegrenset for en prosentandel av selskapets forpliktelser, og tilsvarer eierandelen i selskapet hvis annet ikke framgår av selskapsavtalen.

IKS-loven stiller i § 4 krav til at det skal være en selskapsavtale og angir at selskapsavtalen minst skal inneholde følgende:

1. selskapets foretaksnavn
2. angivelse av deltakerne
3. selskapets formål
4. den kommune der selskapet har sitt hovedkontor
5. antall styremedlemmer
6. deltakernes innskuddsplikt og plikt til å foreta andre ytelser overfor selskapet
7. den enkelte deltakers eierandel i selskapet og den enkelte deltakers ansvarsandel i selskapet dersom denne avviker fra eierandelen
8. antall medlemmer av representantskapet og hvor mange medlemmer den enkelte deltaker oppnevner
9. annet som etter lov skal fastsettes i selskapsavtalen

Kommunelovens stiller i § 26-1 krav til at kommunestyret en gang i valgperioden skal behandle eierskapsmelding som skal inneholde:

- Kommunens prinsipper for eierstyring,
- Oversikt over virksomheter kommunen har eierinteresser i,
- Formål med eierinteresser

KS sin anbefaling nummer fire bygger opp under denne bestemmelsen og sier at det skal utarbeides en årlig eierskapsmelding eller rapport om selskapene for kommunestyret eller fylkestinget. I anbefalingen er følgende krav til innhold i eierskapsmeldingen tatt inn.

- Årlig revidering av eierskapsmeldingen knyttet til (økonomi, eller andre spesielle forhold i selskapene, nye styremedlemmer etc.)
- Selskapenes samfunnsansvar, miljø, likestilling, etikk mv.
- Organisere en administrativ støttefunksjon - sikre betryggende saksbehandling jf. KL § 13-1. Et (eierskapssekretariat) som forbereder saker til politisk behandling og er uavhengig selskapene

Operasjonaliserte vurderingskriterier styringsdokumenter

- Det skal foreligge en selskapsavtale som minst angir informasjon som IKS-loven krever
- Kommuner skal minst en gang i valgperioden utarbeide en eierskapsmelding som skal vedtas av kommunestyret. Den skal inneholde: Prinsipper for eierstyring, oversikt over eierskap, formål med eierskapet.
- Selskapsinformasjonen i eierskapsmeldingen bør revideres årlig med oppdatert selskapsinformasjon.

Eierrepresentasjon

IKS-loven § 6 slår fast at selskapet skal ha et representantskap hvor samtlige deltakere (kommunene) er representert med minst én representant. Videre går det fram at det enkelte kommunestyre oppnevner selv sine representanter og det skal oppnevnes minst like mange varamedlemmer som faste medlemmer. Hvis ikke annet er fastsatt i selskapsavtalen, velger representantskapet selv sin leder og nestleder. Representantskapets medlemmer velges for fire år om ikke annet er fastsatt i selskapsavtalen. Den enkelte deltaker kan foreta nyvalg av sine representantskapsmedlemmer i valgperioden. Nyvalg skjer for den gjenværende del av valgperioden.

KS sine anbefalinger berører også eierrepresentasjon. KS anbefaling 7 sier at som hovedregel bør sentrale folkevalgte oppnevnes som representanter i eierorganet. Dette utdypes blant annet med at det bør etableres forutsigbare kommunikasjonsformer mellom eier og eierrepresentant. Anbefalingen sier at dersom formålet med selskapet er rene driftsoppgaver er det ingen ting i veien for at ansatte i kommunens eller fylkeskommunens administrasjon sitter i eierorganet.

KS anbefaling 3 sier at det må sørges for god kunnskap til folkevalgte om eierskap. Dette kan for eksempel gjøres ved å arrangere et eierskapsseminar for folkevalgte tidlig i valgperioden.

Det er viktig at de folkevalgte får innsikt i de ulike rollene de har som folkevalgte, som styremedlemmer eller som medlemmer av selskapets eierorgan. Rollen som folkevalgt i kommunestyret eller fylkestinget er ulik den rollen man har i et selskapsorgan. Det er viktig å være bevisst roller, styringslinjer og ansvarsfordeling.

Operasjonaliserte vurderingskriterier

- Kommunestyret skal oppnevne sentrale folkevalgte til representanter og vara-representanter til representantskapet for fire år
- Kommunen bør gjennomføre opplæring om eierskap for kommunestyrerepresentantene i løpet av de seks første månedene av valgperioden.
- Det bør etableres forutsigbare kommunikasjonsformer mellom eier (kommunestyret) og eierrepresentant som forankres i eierskapsmeldingen.

Representantskapet

Representantskapet er selskapets øverste myndighet og skal behandle selskapets regnskap, budsjett og fireårig økonomiplan og andre saker som etter loven eller selskapsavtalen skal behandles av representantskapet. (IKS-loven § 7 første ledd andre setning)

IKS-loven § 10 om styret og styrets sammensetning sier i andre ledd at styremedlemmene velges av representantskapet og tredje ledd sier at representantskapet velger styrets leder og nestleder med mindre selskapsavtalen sier at styret selv skal gjøre det. Aksjelovens regler (§ 20-6) om representasjon av begge kjønn i styret gjelder for IKS. Styremedlemmene velges for to år med mindre annet er avtalt.

KS har flere anbefalinger som omfatter representantskapets valg av styret og forhold omkring det. KS anbefaling ni sier at det bør sørges for god sammensetning og kompetanse i styret, som samlet sett er tilpasset det enkelte selskaps formål og virksomhet. Dette handler blant annet om komplementær kompetanse og erfaring.

KS anbefaling 10 anbefaler å vedtektsfeste bruk av valgkomite ved styreutnevnelser og at det lages retningslinjer som regulerer valgkomiteens arbeid.

KS anbefaling 15 anbefaler at styrene etablerer rutiner for vurdering og håndtering av habilitet. I anbefalingen heter det at ingen kommunalt ansatte eller folkevalgte skal håndtere saker i kommunen eller fylkeskommunen som gjelder et selskap der de selv er styremedlem. Dette gjelder uansett om selskapet er privat eid eller helt eller delvis offentlig eid. Det anbefales at styrene etablerer faste rutiner for å håndtere mulige habilitetskonflikter. Ordfører og kommunedirektør bør ikke sitte i styrer i selskaper. IKS-lovens § 15 sier at inhabilitet for

selskapets ansatte og medlemmer av selskapets styrende organer gjelder kommuneloven § 13-3 og § 11-10 tilsvarende.

Kommunelovens § 11-10 handler om *folkevalgtes inhabilitet*. Kommunelovens § 13-3 omhandler inhabilitet for ansatte med henvisning til forvaltningsloven.

Forvaltningslovens § 6 omhandler situasjoner når en *offentlig tjenestemann* er inhabil til å tilrettelegge grunnlaget for en avgjørelse eller til å treffe avgjørelse i en forvaltningssak. Første ledd punkt e 2. omhandler tilfeller hvor offentlig tjenestemann er medlem av styret og selskapet er part i saken. Videre i punktet står det at dette likevel ikke gjelder for person som utfører tjeneste eller arbeid for et selskap som er fullt ut offentlig eid og dette selskapet, alene eller sammen med andre tilsvarende selskaper eller det offentlig full ut eier selskapet som er part i saken.

KS anbefaling 17 anbefaler at styrets medlemmer er registret i KS styrevervregister, for å bidra til åpenhet omkrig ulike roller.

Operasjonaliserte kriterier i undersøkelsen

- Representantskapet skal behandle selskapets regnskap, budsjett og økonomiplan.
- Representantskapet bør vedtektsfeste bruk av valgkomite og vedta retningslinjer for valgkomiteens arbeid.
- Representantskapet skal velge et styre og bør sikre at styrets kompetanse er tilpasset det enkelte selskaps formål og virksomhet.
- Eier bør ha et system for å unngå inhabilitet og unngå at sentrale folkevalgte og administrative ledere velges som styremedlemmer der kommunen har eierinteresser.
- Eier bør sikre at styrets medlemmer er registrert i styrevervregister.

B. Ansvars- og arbeidsfordeling

Personopplysningsloven 200018-12-20-116 består av nasjonale regler med norske tilpasninger (kapittel 1-9) og EUs personvernforordning[7] som består av to deler. Del en er en fortale som er en tolkingshjelp som kan utfylle eller forklare artiklene og selve artiklene (kapittel

[7] Europaparlamentets- og Rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning)

I-XI). Det er bare artiklene som er juridisk bindende[8]. Artikkel 4 definerer sentrale begrep og noen av dem er gjengitt i kapittel 1.5 i denne rapporten.

To av de sentrale begrepene er *behandlingsansvarlig* og *databehandler*. Slik det framgår i fortsettelsen vil den enkelte kommune være behandlingsansvarlig, mens IKT Indre Namdal IKS er en av flere databehandlere som kommunene har. Kommunene er behandlingsansvarlig fordi det er de som bestemmer formålet med behandlingen av personopplysninger. Artikkel 26 åpner for at to eller flere behandlingsansvarlige kan være felles behandlingsansvarlige.

Forordningens artikkel 1 sier at den fastsetter regler om vern av fysiske personer i forbindelse med behandling av personopplysninger samt regler om fri utveksling av personopplysninger. Artikkel 2 sier at forordningen gjelder for helt eller delvis automatiserte behandling av personopplysninger og på ikke-automatisert behandling av personopplysninger som inngår i eller skal inngå i et register.

Artikkel 5 er prinsipper for behandling av personopplysninger og det er den behandlings-ansvarlige (den som bestemmer formålet med behandlingen) som er ansvarlig for å overholde prinsippene, altså i denne sammenhengen kommunene. Personopplysninger skal:

a. **Lovlighet, rettferdighet og åpenhet.** Behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte
b. **Formålsbegrensning**. Samles inn for spesifikke, uttrykkelige angitte og berettigede formål og ikke videre behandles på en måte som er uforenlig med disse. (arkiv er forenlig)
c. **Dataminimering.** Være adekvat, relevant og begrenset til det som er nødvendig for formålet de behandles for (dataminimering)
d. **Riktighet**. Være korrekte og om nødvendig oppdaterte.
e. **Lagringsbegrensning.** Lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for (unntak arkivformål for allmennhetens interesse)
f. **Integritet og konfidensialitet.** Behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak.

[8] www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/om-personopplysningsloven-og-nar-den-gjelder/. Lastet ned 19.08.2021

Punkt 2 i artikkel 5 sier at den behandlingsansvarlige er ansvarlig for og skal kunne påvise at det første punktet overholdes. Det betyr at det må finnes en dokumentasjon på at behandlingsansvarlig overholder prinsippene for behandling av personopplysninger og herunder at det er gjort vurderinger i forhold til lovlighet, formål, dataminimering, lagringsbegrensninger og tiltak for å ivareta integritet og konfidensialitet.

Artikkel 6 utdyper behandlingens lovlighet og angir mulige vilkår som må være oppfylt. Lovligheten kan oppfylles med samtykke fra den registrerte eller at den er nødvendig for å oppfylle avtale med den registrerte, oppfylle rettslig forpliktelse, beskytte den registrertes vitale interesser, utøve offentlig myndighet eller utføre oppgaver i allmennhetens interesse eller legitime interesser som overstiger den registrertes rett til personvern. Artikkel 9 omhandler sensitive personopplysninger.

Artikkel 24 omhandler behandlingsansvarliges ansvar. Her går det fram at den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordningen. Artikkel 26 åpner for at to eller flere behandlingsansvarlige i fellesskap fastsetter formålene med og midlene for behandling. De skal på en åpen måte fastsette sitt respektive ansvar for å overholde forpliktelsene i denne forordningen.

eForvaltningsforskriftens formål er å legge til rette for en sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen. I § 15 første ledd krever at det skal være beskrevet mål og strategi for informasjonssikkerhet (sikkerhetsmål og sikkerhetsstrategi). Dette skal danne grunnlaget for internkontrollen. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks. Her vil kravene i personvernforordningen være aktuelle å innarbeide i en slik sikkerhetsstrategi.

I § 15 andre ledd står det at internkontrollen skal basere seg på anerkjente standarder for styringssystem og være en integrert del av virksomhetens helhetlige styringssystem. § 15 tredje ledd sier at omfang og innretning på internkontrollen skal være tilpasset risiko. Revisor legger til grunn at det skal være gjennomført en risikovurdering som grunnlag for internkontrollsystemet. Forordningens krav i artikkel 24 om tekniske og organisatoriske krav bør da inngå i sikkerhetsstrategien og internkontrollen, som skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.

Revisjonskriterier

- Det skal foreligge en databehandleravtale mellom kommunen som behandlingsansvarlig og IKT Indre Namdal IKS som databehandler

C. Informasjonssikkerhet

Problemstillingen om informasjonssikkerhet er knyttet til IKT Indre Namdal IKS og da i rollen som databehandler. § 15 i eForvaltningsforskriften omhandler internkontroll på informasjons-sikkerhetsområdet for forvaltningsorgan. Dette er da bestemmelser som gjelder kommunens internkontroll for informasjonssikkerhet og som bør følges opp av et interkommunalt selskap som håndterer IKT på vegne av kommunene. § 15 første ledd krever at det skal være beskrevet mål og strategi for informasjonssikkerhet (sikkerhetsmål og sikkerhetsstrategi). Dette skal danne grunnlaget for internkontrollen. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks. Her vil kravene i personvernforordningen være aktuelle å innarbeide i en slik sikkerhetsstrategi.

I § 15 andre ledd står det at internkontrollen skal basere seg på anerkjente standarder for styringssystem og være en integrert del av virksomhetens helhetlige styringssystem. § 15 tredje ledd sier at omfang og innretning på internkontrollen skal være tilpasset risiko. Revisor legger til grunn at det skal være gjennomført en risikovurdering som grunnlag for internkontrollsystemet. Sikkerhetslovens § 4-1 pålegger virksomhetens leder ansvaret for det forebyggende sikkerhetsarbeidet og at dette skal være en del av virksomhetens styrings-system. Sikkerhetstilstanden i virksomheten skal regelmessig kontrolleres. § 4-1 andre ledd sier at virksomheten skal sørge for at ansatte, leverandører og oppdragstakere har tilstrekkelig risiko- og sikkerhetsforståelse. § 4-2 handler om vurdering av risiko og sier at en virksomhet skal regelmessig gjennomføre vurdering av risiko og at vurderingen skal danne grunnlag for iverksetting av forebyggende sikkerhetstiltak. § 4-2 andre ledd sier at virksomheten som en del av vurderingen skal det kartlegges hvilke virksomheter den er avhengig av for å fungere som den skal. I § 4-4 står det at virksomheten skal dokumentere vurderingen av risiko og de gjennomførte og planlagte sikkerhetstiltakene.

I § 15 fjerde ledd bokstavene a til h gis det eksempler på hvilke forhold sikkerhetsstrategien og internkontrollen bør adressere, herunder prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon.

Artikkel 28 i personvernforordningen omhandler databehandleren. Det første punktet sier at behandlingsansvarlig skal bruke databehandlere som i tilstrekkelig grad gir garantier for at de vil gjennomføre egnede *tekniske og organisatoriske tiltak* for å sikre at behandlingen oppfyller kravene i denne forordningen og vern av den registrertes rettigheter. Revisor legger til grunn at tekniske og organisatoriske tiltak inngår i internkontrollsystemet slik eForvaltningsforskriften omtaler i § 15.

Punkt to i artikkel 28 sier at databehandleren ikke skal engasjere annen databehandler uten at det på forhånd er innhentet særlig eller generell skriftlig tillatelse fra den behandlingsansvarlige. Artikkel 28 punkt 3 omhandler databehandleravtale som skal være en skriftlig avtale som er bindende for databehandleren med hensyn til den behandlingsansvarlige, og der gjenstanden for og varigheten av behandlingen, behandlingens art og formål, typen personopplysninger og kategorier av registrerte samt den behandlingsansvarliges rettigheter og plikter er fastsatt. I bokstav a til h er det oppgitt hva databehandleravtalen særlig skal inneholde.

Artikkel 29 sier at databehandleren og enhver person som handler for den behandlingsansvarlige eller databehandleren, og som har tilgang til personopplysninger, skal behandle nevnte opplysninger bare etter instruks fra den behandlingsansvarlige.

Artikkel 30 stiller krav til at behandlingsansvarlig og databehandler skal føre protokoll over behandlingsaktiviteter som de utfører. Artikkelens krav er mer omfattende for behandlingsansvarlig enn databehandler. Punkt 2 sier at hver databehandler og databehandlers representant skal føre protokoll over alle kategorier av behandlingsaktiviteter som er utført på vegne av behandlingsansvarlig, og skal inneholde:

a) navnet på og kontaktopplysningene til databehandleren eller databehandlerne og til hver behandlingsansvarlig som databehandleren opptrer på vegne av, samt, dersom det er relevant, den behandlingsansvarliges eller databehandlerens representant og personvernombudet
b) kategoriene av behandling utført på vegne av hver behandlingsansvarlig
c) dersom det er relevant, overføringer av personopplysninger til en tredjestat eller en internasjonal organisasjon, herunder identifikasjon av nevnte tredjestat eller internasjonale organisasjon og, ved overføringer nevnt i artikkel 49 nr. 1 annet ledd, dokumentasjon på nødvendige garantier
d) dersom det er mulig, en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene nevnt i artikkel 32 nr. 1

Artikkel 32 sier at behandlingsansvarlig og databehandler skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risiko. Dette kan omhandle:

- Pseudonymisering og kryptering av personopplysninger.
- Evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene.

- Evne til å gjenopprette tilgjengelighet og tilgangen til personopplysninger i rett tid dersom det oppstår fysisk eller teknisk hendelse.
- En prosess for regelmessig testing, analysering og vurdering av hvor effektiv behandlingens tekniske og organisatoriske sikkerhetstiltak er.

Artikkel 33 sier at ved brudd på personopplysningssikkerheten skal behandlingsansvarlig meldes tilsynsmyndigheten (jf. artikkel 55) uten ugrunnet opphold og senest 72 timer etter å ha fått kjennskap til det. Databehandler skal uten ugrunnet opphold underrette behandlingsansvarlig. Det stilles også krav til dokumentasjon.

Artikkel 37 sier at den behandlingsansvarlig og databehandleren skal utpeke et personvern-ombud når behandlingen utføres av en offentlig myndighet eller et offentlig organ. Personvern-ombudet skal utpekes på grunnlag av faglige kvalifikasjoner og særlig på grunnlag av dybdekunnskap om personvernlovgivning og praksis på området samt evne til å utføre oppgavene nevnt i artikkel 39.

- Databehandler skal ha sikkerhetsmål og sikkerhetsstrategi
- Databehandler skal dokumentere vurderingen av risiko og gjennomførte og planlagte sikkerhetstiltak
- Databehandler skal ha et internkontrollsystem som bygger på risikovurderinger
- Det skal finnes databehandleravtaler med det innholdet personvernforordningen krever
- Databehandler skal føre protokoll over alle kategorier av behandlingsaktiviteter som er utført på vegne av behandlingsansvarlig
- Databehandler skal ha gjennomført egnede tekniske tiltak og organisatoriske tiltak
- Databehandler skal ha personvernombud

VEDLEGG 2 – HØRINGSSVAR IKT INDRE NAMDAL IKS

IKTIN
IKT Indre Namdal IKS
7898 Limingen

Revisjon Midt-Norge SA

Deres ref: Margrete Haugum	Vår ref: SVA	Dato:09.01.22

Svar på høringsrapport forvaltningsrevisjon IKTIN

Viser til mottatt høringsrapport for eierskapskontroll og forvaltningsrevisjon IKT Indre Namdal IKS den 21.12.2021.

Undertegnede og styreleder (Karl Audun Fagerli) hadde 05.01.22 et møte hvor høringsrapport er gjennomgått.
Vi ønsker å komme med følgende innspill/korrigeringer/spørsmål.

«Eierskapskontroll i xxxxx kommune»

- 2.3.3 Representantskapet – regnskap, budsjett og økonomiplan (Gjelder alle 4 kommuner)
  - I femte avsnitt står følgende: «I behandling av denne saken i 2021 bestiller representantskapet et strategimøte med ordfører, rådmenn/kommunedirektører og administrasjon i selskapet, hvor målsettingen er å utvikle samarbeidet mellom kommunene og selskapet videre».
    - Styret har valgt å gjennomføre dette med et møte hver enkelt kommune. Pr. 05.01.2022 har 2 av 5 kommuner takket ja til et slikt møte. Mål om at møtene skal være gjennomført i forkant av representantskapsmøte i 2022.
- 2.6 Anbefaling (Gjelder alle 4 kommuner)
  - «Sørge for at representantskapet behandler økonomiplan»
    - Tas opp som egen sak på styremøte i januar. Mål om å utarbeide økonomiplan som behandles av representantskapet i 2022.
  - «Sørge for at det utarbeides retningslinjer for valgkomiteens arbeid»
    - Tas opp som egen sak på styremøte i januar. Styret vil utarbeide utkast til retningslinjer.
  - «Følge opp bruken av styrevervregister»
    - Vi merker oss at alle 4 kommuner har fått anbefaling om å følge opp bruken av styrevervregister, men at representanter fra 3 av 4 kommuner allerede er registrert.

«Ansvars- og arbeidsfordeling»

- 6.3 Ansvars- og arbeidsfordeling mellom kommunene og selskapet
  - I tredje siste avsnitt står det «IKT Indre Namdal IKS har en utviklingsstrategi for perioden 2020-2024, som er vedtatt i representantskapet 27.04.2020.....».
    - Denne ble også ble behandlet av representantskapet i 2021.
- 6.4.1 Vurdering – Databehandleravtale
  - «Revisor vurderer at det ikke finnes noen databehandleravtale mellom selskapet og kommunene».
    - Selskapet har tatt tak i dette. Det er engasjert ekstern konsulent til å bistå i dette arbeidet. Oppstartsmøte ble gjennomført 15.12.2021, og prosessen er i gang pr 05.01.2022.

IKT Indre Namdal IKS
7898 Limingen
tlf 911 90 943
mail:stein.vidar.aspnes@iktin.no
org.nr. 985 904 332
bank: 4448.50.12564

Informasjonssikkerhet i IKT Indre Namdal IKS

- 7.3.3 Internkontrollsystem
  - I siste avsnitt refereres det til at undertegnede informerte i ettkant av intervju om styrevedtak for anskaffelse av internkontrollsystem. Pr 05.01.2022 er status at det i desember 2021 ble gjort ytterligere vurderinger av løsningen, og avtale vil bli inngått januar 2022.
- 7.3.5 Behandlingsaktiviteter
  - I første avsnitt står det beskrevet at i selskapets behandlingsoversikt står ESA8 oppført som sak og arkivsystem, men kommunene opplyser om at Elements ble tatt i bruk i juni 2021.
    - Det er korrekt som kommunene opplyser og selskapets behandlingsoversikt må oppdateres. Det er her verdt å nevne at selskapet ikke benytter hverken ESA8 eller Elements, og har således ingen behandlinger i dette systemet. Årsaken til at det likevel kommer med i selskapets liste er at behandlingsoversikten ble i 2018 etablert sammen med kommunene, og selskapet har i ettertid markert alle behandlinger som kun eksisterer i kommunene. Resterende behandlinger er de som er gjeldende for selskapet, og ESA8 er ikke en av dem.
- 7.3.6 Tekniske og organisatoriske tiltak – Backup
  - Her står følgende: «Selskapet har ikke oversikt over hvordan backup foregår i fagsystemene, men det står beskrevet i avtalen med de ulike leverandørene. Selskapet kjenner ikke de tekniske detaljene, og må forholde seg til avtalene».
    - Presiserer her at det ikke gjelder alle fagsystemer. Fagsystem installert og driftet i vår infrastruktur blir også håndtert i vår backup løsning. Fagsystemer lever som en tjeneste (sky/saas) er de vi ikke har detaljerte beskrivelse av hvordan backup fungerer. Der inngås det en avtale med leverandør av tjenesten, som da også påtår seg ansvar for sikkerhet og backup.
- 7.3.6 Tekniske og organisatoriske tiltak – Ressurs og samarbeid
  - De 3 siste setningen, fra «Selskapet kan ikke iverksette prosjekter ……» må omformuleres da det kan misforstås. Foreslår derfor følgende formulering:
    «Selskapet er avhengig av nøkkelpersoner i kommunene for å gjennomføre prosjekter. Nøkkelpersoner har ofte flere roller i egen kommune, og det kan derfor by på utfordringer i form av knapphet på ressurser. Selskapet må derfor til tider sette frister for å sikre nødvendig framdrift for fellesskapet.
    En annen utfordring selskapet opplever er kommunenes ressurser til å følge med utviklingen innenfor de enkelte fag. Med dagens utviklingstakt kommer det stadig nye løsninger og muligheter på markedet. Dette medfører at kommunene må følge med på denne utviklingen, da selskapet ikke har ressurser eller kompetanse til å vurdere hva som er relevant og nødvendig innen det enkelte fagfelt. Her opplever selskapet at kommunene kan ha begrensede muligheter til å følge opp denne utviklingen, og kanskje på litt forskjellige områder.

Konklusjoner og anbefalinger

- 9 Konklusjoner og anbefalinger
  - Generell kommentar til konklusjoner og anbefalinger.
    - Selskapet har allerede startet arbeid med å etablere databehandleravtale mellom selskapet og kommunene. Gjennom dette arbeidet vil mangler som

ansvar og arbeidsfordeling mellom selskapet og kommunene bli adressert, samt oppdatering av behandlingsoversikter.
Selskapet vil tidlig i 2022 anskaffe et internkontrollsystem for Informasjonssikkerhet og GDPR. Med et slikt internkontrollsystem vil vi være i stand til å etablere rutiner og dokumentasjon for å etterleve krav ift. informasjonssikkerhet og personvern.
Gjennom disse to grepene vil selskapet kunne adressere mesteparten av de vurdering og anbefalinger som omhandler selskapet i denne rapporten.
Vi tar dermed konklusjoner og anbefalinger i denne rapporten til etterretning, og vil gjennom tiltakene nevnt ovenfor kunne jobbe systematisk og målrettet med dokumentasjon, rutiner mm. slik at dette arbeidet kommer på samme gode nivå som vi selv mener vi har på det praktiske arbeidet.

IKT Indre Namdal IKS
Daglig leder

Stein Vidar Aspnes

Stein Vidar Aspnes

VEDLEGG 3 – HØRINGSSVAR EIERREPRESENTANT HØYLANDET

Margrete Haugum

Fra: Hege Nordheim-Viken <Hege.Nordheim-Viken@hoylandet.kommune.no>
Sendt: torsdag 20. januar 2022 15:02
Til: Margrete Haugum
Kopi: Merete M. Montero; Marit Grannes; Liv Elden Djokoto
Emne: SV: Høringsrapport IKT Indre Namdal IKS

Til Revisjon Midt-Norge SA v/Margrete Haugum

Viser til epost i dag 20.1.2022, og takker for muligheten til å kommentere utkast Revisjonsrapport for IKT Indre Namdal IKS kapittel 2, Eierskapskontroll Høylandet.

Jeg har følgende merknader til utkastet av rapporten:

Kommentarer til kap. 2.3.1. Eierskapsmelding.

I siste setning på side 15 står det følgende: «*Det er ordfører som har skrevet eierskapsmeldingen*.» Dette er feil. I Høylandet kommune er det administrasjonen som utarbeider eierskapsmeldingen.

Kommentar til kap. 2.3.2. Eierrepresentasjon. Opplæring

I andre avsnitt beskrives det at eierskapspolitikk er kopiert fra andre kommuner. Det presiseres at kommunen har et klart formål med de ulike interkommunale selskapene vi deltar i, som beskrives både i selskapsavtalene for hvert selskap og i sakene der kommunestyret vedtar å tilslutte seg et interkommunalt samarbeid. Det formen på en eierskapsstrategi, og retning for videre utvikling som det kan arbeides videre med ved en revidering av strategien.

Kommentarer til kap. 2.4.2. Eierrepresentasjon. Oppnevning.

I utkast til revisjonsrapport skriver Revisor følgende i kap. 2.4.2. andre avsnitt:
«revisor finner ikke at kommunen har valgt representanter og vararepresentanter til IKT indre Namdal IKS. Selv om ordfører og varaordfører er angitt som kommunenes representanter i selskapsavtalen, må kommunen velge representantene selv.»

Selskapsavtalen for IKT indre Namdal IKS, der det fremgår hvem som er eierrepresentant for kommunen, vedtas av kommunestyret. Selskapsavtalen ble sist vedtatt av sittende kommunestyre den 27.05.2021, i sak 33/21.

I tillegg sier Høylandet kommunestyres delegasjonsreglement kapittel 5.4, vedtatt 22.09.2020, sak 56/20, følgende:

> ***5.4 Representasjon***
> *Ordføreren gis fullmakt til å representere kommunen ved generalforsamlinger, årsmøter hvor kommunen har interesse som eier eller aktør og er kommunens representant på representantskaps-møter. Dette gjelder der kommunestyret ikke har gjort særskilte vedtak eller valg.*

1

Ordføreren kan delegere denne fullmakt til andre politikere, rådmann eller den han bemyndiger.

Jeg mener at kommunestyret har gjort vedtak om eierrepresentant for denne valgperioden både gjennom vedtak om revidert selskapsavtale og gjennom vedtatt delegasjonsreglement.

Kommentarer til kap. 2.4.2. Eierrepresentasjon. Kommunikasjonsformer mellom eier og eierrepresentant, og 2.5. Konklusjon.

I rapportens kap 2.4.2 skriver revisor følgende i 7. avsnitt *: «Vurderingskriteriet er at det bør etableres forutsigbare kommunikasjonsformer mellom eier og eierrepresentant, som er forankret i eierskapsmeldingen.»*

Som eierrepresentant er enig i at kommunikasjonsform bør beskrives bedre i eierstrategi, men er imidlertid uenig i at etablert praksis i dag ikke er forutsigbar:

1. I tillegg til at det er utarbeidet eierskapsmelding som vedtas av kommunestyret, er det også etablert praksis som gir kommunestyret muligheter for å gi innspill til eierrepresentant.
    - Innkallinger med saksliste til representantskap og generalforsamlinger blir sendt til kommunestyremedlemmer pr. epost. Dette mener jeg også ble sagt i intervjuet. Det gjør at eiere enten kan ta kontakt med eierrepresentant i forkant av møtet, eller ta dette opp dersom det er politiske møter fra sakspapirer sendes ut til representantskapsmøte eller generalforsamling finner sted. Dette gjør det mulig å sette opp ekstra møter dersom eiere finner tema som de ønsker mer informasjon om.
    - Referater fra representantskapsmøter og generalforsamlinger blir også gjort kjent for kommunestyret. I tillegg tilstrebes det å orientere formannskap og kommunestyre muntlig om diskusjonen som har gått i møtene.

Jeg mener dette en forutsigbar kommunikasjonsform som er etablert, siden kommunestyret er kjent med denne måten å gjøre det på. Jeg er derfor uenig i konklusjonen som lyder «*det gjenstår å få etablert et forutsigbart system for kommunikasjon mellom eier og eierrepresentant*». Imidlertid er jeg enig i at kommunikasjonsformen mellom eierrepresentant og eier kan beskrives bedre i eierskapsmelding og strategi. Dette vil bli sett på i neste revisjon.

Med hilsen

Hege Nordheim-Viken
Ordfører
Høylandet kommune
Tlf. 915 93 320

Revisjon

Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no