Møteinnkalling - Kontrollutvalget i Namsos kommune

Arkivsak:	22/146
Møtedato/tid:	30.08.2022 kl. 09:00
Møtested:	Møterom Saga - Namdalshagen

Møtet avvikles for åpne dører, i tråd med kommuneloven § 11-5.

Eventuelle forfall, eller spørsmål om habilitet, meldes til Konsek Trøndelag IKS
v/ Einar Sandlund på telefon 938 97 555, eller e-post: einar.sandlund@konsek.no

Sakliste

Saksnr.	**Sakstittel**
22/22	Forvaltningsrevisjonsrapport - Informasjonssikkerhet
23/22	Oppfølging av Forvaltningsrevisjonsrapport - Personal nærvær
24/22	Tilbakemelding - statsforvalterens tilsyn landbruksforvaltning
25/22	Bestilling av forvaltningsrevjson -
26/22	Budsjett 2023 og økonomiplan 2023-26 for kontrollarbeidet
27/22	Referatsaker august 22
28/22	Godkjenning av protokoll

Varamedlemmer møter etter nærmere innkalling.

Steinkjer, 23.08.2022

Bjørn Dag Derås (sign.)
Leder av kontrollutvalget

Einar Sandlund/s/
Seniorrådgiver
Konsek Trøndelag IKS

Kopi: Varamedlemmer, ordfører, kommunedirektør og Revisjon Midt-Norge SA

Forvaltningsrevisjonsrapport - Informasjonssikkerhet

Behandles i utvalg	Møtedato	Saknr
Kontrollutvalget i Namsos kommune	30.08.2022	22/22

Saksbehandler Einar Sandlund
Arkivkode FE-217, TI-&58
Arkivsaknr 21/234 - 7

Forslag til vedtak:

1. Kontrollutvalget slutter seg til forvaltningsrevisjonsrapporten Informasjonssikkerhet.
2. Saken oversendes kommunestyret med slik innstilling til vedtak:

1) *Kommunestyret tar forvaltningsrevisjonsrapporten Informasjonssikkerhet til orientering.*
2) Kommunestyret ber kommunedirektøren følge opp rapportens anbefalinger:

- *Inkludere informasjonssikkerhet i helhetlig ROS.*
- *Utarbeide målsettinger og strategi for informasjonssikkerhet separat eller i forbindelse med andre plandokumenter.*
- *Om organisering og ansvar for informasjonssikkerhet er tydelig og hensiktsmessig.*
- *Få på plass et internkontrollsystem.*
- *Iverksette gjennomganger for å avvikle tilganger til personer som har sluttet.*
- *Sikre at behandlingsoversikter kommer på plass i henhold til personopplysningsloven.*
- *Løfte fokuset på informasjonssikkerhet som et ledd i å bygge en sikkerhetskultur.*

3) Kommunestyret ber kommunedirektøren innen 01.03.22 om skriftlig rapport til kontrollutvalget på hvordan anbefalingene er fulgt opp.

Vedlegg
Forvaltningsrevisjonsrapport informasjonssikkerhet

Saksopplysninger
Kommunelovens § 23-3 sier at det skal gjennomføres forvaltningsrevisjon i kommunen. Kommunestyret behandlet den 29.10.20 i sak 155/20 plan forvaltningsrevisjon 2020-2024.

Ut fra prioriteringen i planen gjorde kontrollutvalget i sak 21/21 slikt bestillingsvedtak:
1. Kontrollutvalget bestiller forvaltningsrevisjon området IKT, datasikkerhet, GDPR.
2. Kontrollutvalget gir følgende innspill på følgende problemstillinger/spørsmål:
· Sikkerhet , drifting og dublering av system,
· Samordning mellom enhetene på bruk av digitale plattformer, effektivisering.
· Fremtidig lagring og tilgang. Kompatibilitet av system, rettsdokumentasjon,
3. Revisor bes å utarbeide prosjektplan i henhold til neste møte, 23.11.21.

Kontrollutvalget behandlet prosjektplanen i sak 27/21 og fattet slikt vedtak:
1. Prosjektplan datert 04.11.21 godkjennes.
2. Rapporten forventes levert 01.06.22 og innenfor den angitte ressursbruk på 400 timer.
3. Kontrollutvalget bes å bli orientert underveis for å kunne ta stilling til evt. behov for endringer i prosjektplanen.

Følgende problemstillinger er besvart i rapporten, jfr. vedtatt prosjektplan :
1. Hvordan ivaretar Namsos kommune informasjonssikkerhet?
2. Hvordan har kommunen sikret integritet, konfidensialitet og tilgjengelighet for informasjon fra de gamle kommunene?

Endelig rapport ble oversendt 07.07.22. Kommunedirektøren har rapporten til høring og avgitt høringssvar 27.05.22, jfr. vedlegg 2 i rapporten. Etter oppstartsmøtet ble det klart at den andre problemstillingen om sikring av integritet, konfidensialitet og tilgjengelighet for informasjon fra de gamle kommunene, burde tones ned. Dette skyldes at de sammenslåtte kommunene, Overhalla kommune og Flatanger kommune har hatt et samarbeid innenfor IT siden 2002. Revisor har derfor valgt å lage et beskrivende svar på denne problemstillingen, uten revisjonskriterier.

Metodene brukt for å samle data i denne forvaltningsrevisjonen, nærmere beskrevet i kap. 1.3., er gjennomført med intervjuer og dokumentgjennomgang. Til intervjuene ble det laget tilpassede intervjuguider. Det er skrevet referat fra alle intervjuene, som er verifiserte. Noen av de som er intervjuet har fått tilleggsspørsmål på e-post i etterkant. I dokumentgjennomgangen er sentrale politiske dokumenter slik som samfunnsplan og beredskapsplan, dokumenter og referater fra informasjonssikkerhetsutvalgets arbeid og rutiner fra kvalitetssystemet m.v. Det er revisors oppfatning at de data som er samlet inn gir et tilstrekkelig grunnlag for å belyse arbeidet med informasjonssikkerhet i Namsos kommune

Hvordan ivaretar Namsos kommune informasjonssikkerhet?
Konklusjon er at Namsos kommune mangler en forankring for arbeidet med informasjonssikkerhet i kommunens mer overordnede risikovurderinger og planer. Videre mangler kommunen blant annet internkontroll og kontroll med brukertilganger. Kommunen har en del forebyggende og oppdagende sikkerhetstiltak. Korrigerende tiltak er i stor grad på plass for IT-enheten, men ikke andre deler av kommunen. Det mangler en overordnet risikovurdering for informasjonssikkerhet i Namsos kommune, som kan legge premissene for informasjonssikkerhetsarbeidet, men det er gjort enkelte risikovurderinger innenfor området.

Videre er det uklart om det finnes et mål for informasjonssikkerhet, det mangler en sikkerhetsstrategi og kommunen har ikke en sikkerhetsorganisasjon hvor ansvar og roller for informasjonssikkerhet framgår. Internkontroll er ikke på plass og det arbeides med å få på plass et kvalitetssystem som grunnlag for internkontroll. Flere rutinebeskrivelser er på plass.

Kommunen har et system på opprettelse av brukere, men har ikke kontroll på å avvikle brukere som ikke skal ha tilgang til datasystemet lengre. Kommunen har en behandlingsoversikt i henhold til personopplysningsloven som ligger i dagens kvalitetssystem, men det er ikke oppdatert. Det gis opplæring i informasjonssikkerhet til nyansatte og skal gjennomføre årlige opplæringstiltak, men slik revisor ser det er det et forbedringspotensial i å bygge en sikkerhetsstruktur.

Det vurderer ikke IKT-risiko ved alle anskaffelser av datasystemer. Kommunen har systemer for for å overvåke datasikkerhet, sårbarheter, trafikkanalyse og det er gjennomført inntrengingstest i 2022. Likedan vurderer revisor det slik at kommunen har planer for gjenoppretting, hendelseshåndtering og enkelte hendelser, f.eks. ransomwareangrep.

Informasjonssikkerhet i overgangen til ny kommune
Overgangen til ny kommune medførte ikke store endringer siden samarbeidet på IT allerede var på plass og det var lite problemer knyttet til IT ved sammenslåingen av kommunene. Revisor har valgt å lage en beskrivende besvarelse på denne problemstillingen, fordi det er historie og lite aktuelt for revisjon. Kommunen leverer i dag mange IT-tjenester til Flatanger og Overhalla kommuner.

Revisors oppfatning er at integritet, konfidensialitet og tilgjengelighet for informasjon ble ivaretatt ved kommunesammenslåingen. Kommunene som ble sammenslått, hadde allerede et samarbeid og datasystemene var allerede koblet sammen, slik at jobben med overgangen handlet om å integrere like systemer. Historiske data fra sak- og arkivsystemet ble tatt vare på og tilgjengelig fra historiske databaser.

Imidlertid kommer det frem behov for at det utarbeides en ny IKT-strategi i forbindelse med etableringen av Nye Namsos og som kan være felles for alle kommunene, som fortsatt skal ha samdrift om IKT-infrastruktur. Revisor har ikke funnet at det er laget noen IKT-strategi etter kommunesammenslåinga.

Vurdering
Sekretariatet viser til den framlagte rapport og er av den oppfatning at den svarer ut de gitte problemstillinger i prosjektplanen.

Sekretariatet viser til at rapporten viser at kommunen har flere mangler vedrørende informasjonssikkerhet. Det gjelder forankringen av arbeidet med risikovurderinger, internkontrollsystem, og kontrollen med brukertilganger m.v. Målsettinger og strategi for informasjonssikkerheten bør utarbeides separat eller i forbindelse med andre planer. Videre kommer det frem at å sikre behandlingsoversikter iht. personopplysningsloven kommer på plass. Fokuset på informasjonssikkerhet for å bygge en sikkerhetskultur må økes.
En god del forebyggende og oppdagende sikkerhetstiltak er imidlertid på plass og innenfor IT-enheten er mange korrigerende tiltak på plass, men ikke i andre deler av kommunen.

Sekretariatet viser forøvrig til at kommunen leverer mange IT-tjenester til Flatanger og Overhalla kommuner.

Kontrollutvalget anbefales å slutte seg til rapporten. Saken anbefales videre lagt frem for kommunestyret med innstilling på å ta forvaltningsrevisjonsrapporten Informasjonssikkerhet til orientering og videre be kommunedirektøren følge opp anbefalingene i innstillingens pkt. 2. Kommunestyret anbefales til slutt å be kommunedirektøren innen 01.03.22 .22 gi skriftlig rapport til kontrollutvalget på hvordan anbefalingene er fulgt opp.

FORVALTNINGSREVISJON

Informasjonssikkerhet

RAPPORT

Namsos kommune

Juli 2022

FR1195

FORORD

Revisjon Midt-Norge SA har gjennomført denne forvaltningsrevisjonen på oppdrag fra Namsos kommunes kontrollutvalg i perioden januar 2022 til mai 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 Thomas Furunes, og kvalitetssikrere Merete Montero og Unni Romstad. Revisor har vurdert egen uavhengighet overfor Namsos kommune, jf. kommuneloven § 24-4 og forskrift om kontrollutvalg og revisjon kapittel 3.

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

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, 07.07.2022

Margrete Haugum

Oppdragsansvarlig revisor

[1] Kommuneloven § 23-3, 1.ledd

[2] www.nkrf.no

SAMMENDRAG

Denne forvaltningsrevisjonen ser i hovedsak på hvordan Namsos kommune ivaretar informasjonssikkerhet. I tillegg er det en beskrivelse av hvordan kommunen sikret integritet, konfidensialitet og tilgjengelighet i forbindelse med kommunesammenslåingen.

Forvaltningsrevisjonen er basert på data samlet inn gjennom kommunale dokumenter og intervjuer med ansatte i kommunen.

Konklusjon er at Namsos kommune mangler en forankring for arbeidet med informasjons-sikkerhet i kommunens mer overordnede risikovurderinger og planer. Videre mangler kommunen blant annet internkontroll og kontroll med brukertilganger. Kommunen har en del forebyggende og oppdagende sikkerhetstiltak. Korrigerende tiltak er i stor grad på plass for IT-enheten, men ikke andre deler av kommunen.

Det er uklart om det finnes et mål for informasjonssikkerhet, og det mangler en sikkerhets-strategi. Sikkerhetsorganisasjonen har en uklar plass i kommuneorganisasjonen.

Flere rutinebeskrivelser er på plass, men det mangler et kvalitetssystem som legger grunnlaget for internkontroll. Kommunen har ikke kontroll på å avvikle brukere av systemene som ikke er ansatt i kommunen lengre og heller ikke kontroll på kommunens datautstyr når noen slutter. Ansatte får opplæring i IT-sikkerhet.

IT kommer sent inn i anskaffelse av programvare, noe som kan gjøre det vanskelig å ivareta sikkerheten og lage et effektivt driftsmiljø.

Noen av de ansatte har god oversikt over enheter og strukturen på IKT-systemet, men det finnes ikke noe konfigurasjonskart. Kommunen har en behandlingsoversikt i henhold til personopplysningsloven, som ligger i dagens kvalitetssystem, men det er ikke oppdatert. Kommunen har praksis for sikkerhetsoppdateringer og sikkerhetskopier, men de er ikke skriftliggjort. Namsos kommune har system for å overvåke, oppdage og fjerne sårbarheter. Kommunen har gjennomført en sikkerhetstest.

IT-avdelingen har en plan for håndtering av sikkerhetshendelser og gjenoppretting. Det finnes en beredskapsplan på IT, men det er uklart om beredskapsplanen har en rolle i andre deler av organisasjonen.

Revisors oppfatning er at integritet, konfidensialitet og tilgjengelighet for informasjon ble ivaretatt ved kommunesammenslåingen.

Kommunene som ble sammenslått, hadde allerede et samarbeid og datasystemene var allerede koblet sammen, slik at jobben med overgangen handlet om å integrere like systemer. Historiske data fra sak- og arkivsystemet er tatt var på og tilgjengelig fra historiske databaser.

Revisor anbefaler kommunedirektøren å vurdere følgende anbefalinger:

- Inkludere informasjonssikkerhet i helhetlig ROS.
- Utarbeide målsettinger og strategi for informasjonssikkerhet separat eller i forbindelse med andre plandokumenter.
- Om organisering og ansvar for informasjonssikkerhet er tydelig og hensiktsmessig.
- Få på plass et internkontrollsystem.
- Iverksette gjennomganger for å avvikle tilganger til personer som har sluttet.
- Sikre at behandlingsoversikter kommer på plass i henhold til personopplysningsloven.
- Løfte fokuset på informasjonssikkerhet som et ledd i å bygge en sikkerhetskultur.

INNHOLDSFORTEGNELSE

Tabell

Figurer

1 INNLEDNING

I dette kapittelet redegjøres det for bestillingen, problemstillinger, metode og bakgrunn for prosjektet.

1.1 Bestilling

Kontrollutvalget i Namsos kommune bestilte med bakgrunn i plan for forvaltningsrevisjon, en forvaltningsrevisjon med temaet informasjonssikkerhet, i kontrollutvalgets møte 21.09.2021, sak 21/21. Kontrollutvalget vedtok 23.11.2021, sak 27/21 prosjektplanen.

1.2 Problemstillinger

Problemstillingene i forvaltningsrevisjonen er:

1. Hvordan ivaretar Namsos kommune informasjonssikkerhet?
2. Hvordan har kommunen sikret integritet, konfidensialitet og tilgjengelighet for informasjon fra de gamle kommunene?

Etter oppstartsmøtet ble det klart at den andre problemstillingen om sikring av integritet, konfidensialitet og tilgjengelighet for informasjon fra de gamle kommunene, burde tones ned. Dette skyldes at de sammenslåtte kommunene, Overhalla kommune og Flatanger kommune har hatt et samarbeid innenfor IT siden 2002. Revisor har derfor valgt å lage et beskrivende svar på denne problemstillingen, uten revisjonskriterier.

1.3 Metode

I denne forvaltningsrevisjonen er det lagt til grunn sentrale politiske dokumenter slik som samfunnsplan og beredskapsplan. Dette for å finne ut hvordan arbeidet med informasjons-sikkerhet er forankret i kommunens planverk. I tillegg har revisor fått tilgang til dokumenter og referater fra informasjonssikkerhetsutvalgets arbeid. Informasjonssikkerhetsutvalget er nærmere beskrevet i kapittel tre. Informasjonssikkerhetsutvalget har en overordnet operativ og oppfølgende rolle, og deres arbeid gir informasjon om hvordan kommunens praktiske tilnærming til informasjonssikkerhet følges opp. Dette omfatter blant annet risikovurderinger og kartlegginger. Revisor har fått tilsendt noen rutiner fra kvalitetssystemet. Rutine-beskrivelsene er viktig informasjon i revisjonen fordi de beskriver hvordan det praktiske arbeidet er tenkt lagt opp. Revisor fikk tilgang til kvalitetssystemet, men klarte ikke å komme inn på systemet. Dette ble ikke fulgt opp videre fordi vi hadde fått en papirversjon av de mest interessante rutinene.

Det er gjennomført et oppstartsmøte med følgende deltakere:

- Assisterende kommunedirektør

- Kommunalsjef personal og organisasjon
- IT-leder Overhalla kommune

I oppstartsmøtet ble det innhentet informasjon som grunnlag for en nærmere definering av revisjonen. Det ble laget en intervjuguide og skrevet et referat.

Videre ble det gjennomført intervjuer med ulike personer i Namsos kommune, for å få en nærmere innsikt og forståelse for informasjonen som finnes i dokumentene som er undersøkt. I tillegg vil intervjuene gi ytterligere informasjon om sammenhenger og praksis. Følgende er intervjuet og flere av disse er medlemmer i informasjonssikkerhetsutvalget:

- Personvernombudet
- IT-leder
- Driftssjef-IT
- Konsulent på dokumentsenteret
- Spesialrådgiver-IT
- Konsulent-IT
- Gruppeintervju med assisterende kommunedirektør, kommunalsjef personal og organisasjon samt kommunalsjef strategi og samfunnsutvikling.

Til disse intervjuene ble det laget tilpassede intervjuguider. Det er skrevet referat fra alle intervjuene, som er verifiserte. Noen av de som er intervjuet har fått tilleggsspørsmål på e-post i etterkant.

Revisor har ikke hatt tilgang inn i datasystemene for å undersøke hvilke programmer som finnes. Vurderingene her er basert på informasjon fra intervjuer og demonstrasjon av enkelte systemer. Revisor har eksempelvis ikke undersøkt om kommunen har andre datasystemer, som ikke er registrert i *avtaler* i kvalitetssystemet.

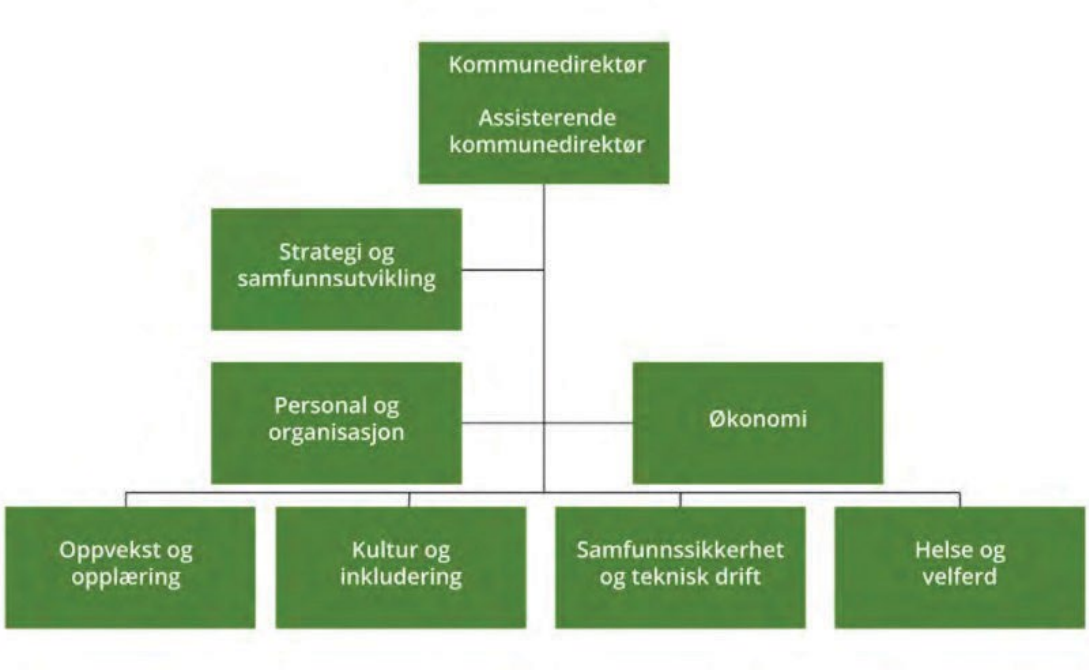
På et tidspunkt vurderte revisor å sammenligne brukertilganger til datasystemet med de som får utbetalt lønn fra kommunen, for å undersøke om tilganger ble fjernet når ansatte sluttet. Flere av de revisor har intervjuet har fortalt at kommunen ikke klarer å følge opp fjerning av tilganger og derfor har revisor ikke undersøkt det selv.

På noen områder viser revisor til å ha sett kommunens dokumentasjon uten å presentere den nærmere. Dette er gjort av sikkerhetshensyn. Eksempelvis vil en presentasjon av et konfigurasjonskart være av stor nytte for noen som planlegger angrep på et datasystem. I tillegg har revisor fått tilbud om å se resultatene fra penetrasjonstesten, men har takket nei til å se denne rapporten. Det viktigste er at kommunen har fått gjennomført en test og følger den opp.

Det er revisors oppfatning at de data som er samlet inn gir et tilstrekkelig grunnlag for å belyse arbeidet med informasjonssikkerhet i Namsos kommune. Underveis har vi opplevd at intervjuobjektene har vært ganske samstemt om hvordan situasjonen er. IT-området er preget av mange ukjente begreper, forkortelser og teknisk språk. Dette kan lett føre til misforståelser spesielt i intervjusituasjonen. Derfor er verifisering av intervjuene viktig for å luke ut misforståelser. Kommunen har også fått rapporten uten vurderinger og konklusjon til faktasjekk for å luke ut eventuelle uklarheter og misforståelser. Revisor har ikke mottatt svar fra datasjekken tidsnok til at det er hensyntatt i høringsutkastet.

1.4 Bakgrunn

Namsos kommune består av tidligere Namsos, Fosnes og Namdalseid kommuner, etter kommunesammenslåingen i 2020. Namsos kommune er organisert med tre avdelinger i stab og fire avdelinger i linje slik som vist i figur 1.



Kilde: www.namsos.kommune.no 21.02.2021

Figur 1. Organisasjonskart Namsos kommune

Informasjonsteknologi er en del av kommunalsjef for personal og organisasjon sitt område, under interne tjenester sammen med personal og dokumentsenteret. Det er ti til tolv personer som jobber med IT.

Namsos kommune er vertskommune for samarbeidet med Overhalla kommune og Flatanger kommune. Det finnes samarbeidsavtaler med kommunene og databehandleravtaler.

1.5 Begreper

IT-området og personopplysningsloven inneholder en del begreper som det kan være nyttig å ha oversikt over. Under er noen av IT-begrepene og begrepsdefinisjonene fra personvern-forordningen[3] gjengitt.

1.5.1 IT begreper

Informasjonssikkerhet - Denne rapporten tar utgangspunkt i informasjonssikkerhet, og omhandler da både digital og analog informasjon. Hovedvekten er lagt på digital informasjon, men ikke avgrenset bort fra analog informasjon.

IT og IKT – forkortelsen IT – informasjonsteknologi og IKT – informasjons- og kommunikasjonsteknologi er forkortelser som brukes litt om hverandre. Begrepene brukes i dagligtale noe unøyaktig om hverandre.

Tofaktorautentisering - betyr at det benyttes to ulike trinn for å bekrefte identitet.

Switch - nettverkskomponent som styrer datatrafikk mellom ulike noder i et nettverk, slik som PC, server[4], skriver og Internett-forbindelse. (Wikipedia, 07.05.2022.)

Ransomware – er på norsk omtalt som løsepengevirus, utpressingsprogramvare eller gisselvare. Det er skadelig programvare (datavirus) som krypterer hele eller deler av innholdet i en infisert datamaskin slik at den blir utilgjengelig for brukeren, for så å be om løsepenger.

1.5.2 Begreper fra personvernforordningen

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. Identifiseringen kan særlig skje ved hjelp av en identifikator, for eksempel et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere

[3] Personvernforordningen er tatt inn i personopplysningsloven

[4] En server er en tjener, datamaskin eller programvaresom leverer tjenester til enheter i et nettverk. (Store norske leksikon, lastet ned 06.07.2022.)

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

Dette innledende kapitlet presenterer bestillingen, problemstillingene i revisjonen, metode og bakgrunn.

Kapittel to og tre handler henholdsvis om informasjonssikkerhet generelt og i Namsos kommune. Disse to kapitlene er bakgrunnskunnskap for de påfølgende kapitlene.

Kapittel fire handler om informasjonssikkerhet i Namsos kommune og er delt i fem hoveddeler, kapittel 4.3 til 4.7. Hver del inneholder en presentasjon av data med en påfølgende vurdering fra revisor.

Problemstillingen om integritet, konfidensialitet og tilgjengelighet etter kommunesammenslåingen er beskrevet i kapittel fem.

I kapittel seks omtales høringen av den foreløpige rapporten.

Kapittel sju er konklusjon og anbefalinger.

2 INFORMASJONSSIKKERHET I EN STØRRE SAMMENHENG

2.1 Sikkerhet på nasjonalt nivå

Nasjonal sikkerhetsmyndighet (NSM) er Norges direktorat for forebyggende nasjonal sikkerhet. Direktoratet gir råd om og gjennomfører tilsyn og kontrollaktiviteter på sivil og militær side knyttet til sikring av informasjon, systemer, objekter og infrastruktur av nasjonal betydning. NSM har et nasjonalt ansvar for å avdekke, varsle og koordinere håndtering av alvorlige IKT-angrep. NSM har gitt ut rapporten *Risiko 2022* (NSM 2022) og *Nasjonal digitalt risikobilde for 2021* (NSM 2021). Begge rapportene beskriver forhold omkring informasjonssikkerhet i samfunnet og informasjonen i dette kapitlet er hentet fra disse to rapportene.

Samfunnet har blitt mer digitalisert. Ny teknologi endrer måten vi jobber på og hvordan vi behandler data. Det oppstår flere og større avhengigheter mellom ulike digitale systemer og dette skaper sårbarheter. Det er bekymringsverdig at stadig flere samfunnsverdier flyttes over i det digitale domenet, uten at det først er gjennomført tilstrekkelig verdi- og risikovurderinger. Når en risikovurdering foreligger med risikoer identifisert og evaluert, må beslutningstaker håndtere risikoen på en god måte. (NSM 2021)

I dag understøttes samfunnet av en rekke digitale kritiske funksjoner som må fungere til enhver tid. En uønsket hendelse mot en eller flere av disse kan få store konsekvenser og føre til synlige og negative samfunnseffekter. Vi ser at det gjøres mye godt sikkerhetsarbeid i mange virksomheter, og stadig flere får opp bevisstheten rundt og fokuset på digital sikkerhet. Men arbeidet må forsterkes betydelig. Det kreves et taktskifte i forebyggende arbeid og beredskap. (NSM 2021)

Flere og flere virksomheter erkjenner at cyberoperasjoner kan ramme alle og Nasjonalt cybersikkerhetssenter[5] erfarer at stadig flere prioriterer det digitale sikkerhetsarbeidet. Vi ser likevel at mange norske virksomheter ikke har et forsvarlig sikkerhetsnivå for å beskytte viktige verdier. Økt bevissthet om digital risiko har ofte ikke blitt omsatt i handling. Dette bør være et tema i alle styrerom og ledergrupper. (NSM 2021)

Risikovurderingen bygger på forholdet mellom verdi, trussel og sårbarhet. Virksomheten og ledelsen har alltid ansvaret for sikring av egne verdier. Risikovurdering og risikohåndtering er helt nødvendig for å oppnå et forsvarlig sikkerhetsnivå i egen virksomhet. (NSM 2021) Mange

[5] Nasjonalt cybersikkerhetssenter (NCSC) er en del av nasjonal sikkerhetsmyndighet og samtidig et partnerskap mellom NSM og ulike offentlige og private virksomheter. Sentret skal bidra til å beskytte grunnleggende nasjonale funksjoner, offentlig forvaltning og næringsliv mot cyberoperasjoner.

virksomheter sikrer seg mot driftsforstyrrende hendelser som innbrudd eller nedetid på systemene. Men disse sikringstiltakene beskytter ikke nødvendigvis mot målrettede trussel-aktører. Et tilstrekkelig sikkerhetsnivå avhenger av at virksomheter oppdaterer sin kunnskap, blir mer sikkerhetsbevisste og tilpasser sikringstiltak etter endringer i trusselbildet. (NSM 2022)

I *Risiko 2022* (NSM 2022), beskrives det at trussel-aktørene viser stor kapasitet til å gjennomføre cyberangrep. Siden 2019 har NSM sett en tredobling i antall cyberhendelser som får alvorlige konsekvenser for virksomheter i Norge. Det siste året har kartleggingsaktivitet, phishing[6], digital utpressing og sabotasje, og utnyttelse av digitale sårbarheter hos et stort antall virksomheter preget cyberbildet. Kartleggingsaktivitet kan innebære kartlegging av tekniske sårbarheter, hvilken informasjon som ligger på åpne nettsider og kartlegging av personer eller organisasjoner. Vi må være oppmerksomme på at dette kan være forberedelser til neste fase i et cyberangrep.

Phishingforsøkene er ofte svært godt tilpasset til hvert enkelt mål. Vi er kjent med at trussel-aktører bruker offentlig tilgjengelig informasjon for å skreddersy e-poster som sendes virksomheter. Virksomheter bør derfor vurdere hvor mye informasjon om ansatte som skal ligge tilgjengelig på internett. (NSM 2021)

Utnyttelse av tekniske programvaresårbarheter er den vanligste veien inn for få uautorisert tilgang til en virksomhets digitale systemer. Utnyttelse av nulldagssårbarheter har preget det internasjonale risikobildet det siste året. En nulldagssårbarhet er en sårbarhet som ikke er kjent for leverandøren av programvaren, og som kan utnyttes av en trussel-aktør. (NSM 2021) Det betyr at trussel-aktøren oppdager sårbarheten først.

Norske virksomheter blir jevnlig rammet av krypteringsvirus med krav om løsepenger, såkalt løsepengevirus. Løsepengevirus har blant annet som formål å hindre virksomheten i å bruke sitt eget IT-system, slik at virksomheten presses til å betale angriperen for å kunne opprettholde ordinær drift. Bruken av løsepengevirus fortsetter å øke både i omfang og antall, og har i flere tilfeller ført til store systemlammelser med utilgjengeliggjøring av funksjoner, varer og tjenester, samt sensitiv informasjon på avveie. Internasjonalt rapporteres det om en dramatisk økning i summen av løsepengekrav. (NSM 2021)

Programvare- og tjenesteleverandører kan også utnyttes av trussel-aktører for å få innpass i systemene til selskapets kunder i såkalte leverandørkjedeangrep. Trussel-aktører kan skjule skadevare i programvare som leverandøren selger videre til sine kunder. På denne måten kan

[6] Phishing er en form for sosial manipulering hvor en angriper forsøker å lure noen til å gjøre en handling, eksempelvis trykke på en lenke. (Phishing - hvordan beskytte virksomheten | Datatilsynet, lastet ned 0707.2022)

en trussel-aktør enkelt etablere brohoder hos mange nye virksomheter. Skadevaren kommer inn i nye virksomheters systemer i form av en ordinær anskaffelse eller oppgradering, og slike sårbarheter kan være vanskelig å oppdage. Kartlegging av egne digitale avhengigheter og verdikjeder, samt å stille krav til tjenesteleverandørenes IT-sikkerhet er helt essensielt for en virksomhet for å redusere konsekvensene av en cyberoperasjon mot tjenesteleverandøren. (NSM 2021)

Gjenoppretting er både tid- og ressurskrevende og komplisert. Full stans i virksomheten og tap av sensitiv informasjon kan vise seg å bli vesentlig mer kostbart enn å investere i forebyggende sikkerhetsarbeid. Det bør derfor stå høyt på agendaen hos alle å sikre seg mot dette. (NSM 2021)

Den 09.03.2022 sendte KS ut et brev til alle landets kommuner om sikkerhetstiltak i norske kommuner i forbindelse med Russlands invasjon i Ukraina. Her opplyses det at norske sikkerhetsmyndigheter forventer økt aktivitet med svindel, phishing og sosial manipulering, og at kommune derfor må prioritere å innarbeide en god sikkerhetskultur. Brevet viser til Nasjonal sikkerhetsmyndighet (NSM) sine råd til virksomheter om å forebygge og avverge cyberangrep. KS anbefaler kommunene å iverksette undersøkelser og vurdere iverksetting av tiltak på følgende områder:

- Sikkerhetsovervåkning
- Sikring av kritiske funksjoner og tjenester
- Beskytte tjenester som er tilgjengelige på internett
- Årvåkenhet og teknologi

2.2 Erfaringer fra dataangrepet i Østre Toten kommune i 2021

Østre Toten kommune ble 9. juni 2021 utsatt for et løsepengevirusangrep som rammet store deler av kommunens tjenesteproduksjon. Kommunedirektøren bestilte en rapport fra KPMG for å bidra til å belyse forholdet rundt årsak og konsekvens for berørte parter. Formålet med rapporten var å legge til rette for læring og komme med innspill til arbeidet med digital sikkerhet i framtiden. (KPMG, 2021)

I rapporten gis det anbefalinger til Østre Toten kommune som også er relevant for andre kommuner. Anbefalingene innledes med (KPMG 2021, s. 26)[7]:

[7] offentlig-versjon.pdf (ototen.no)

Et forsvarlig sikkerhetsnivå for informasjon og IKT-systemer oppnås ved å redusere risiko for uønskede hendelser til at akseptabelt nivå. For å lykkes er det nødvendig at kommunen har velfungerende og helhetlig sikkerhetsstyring som er en integrert del av virksomhetsstyringen og samtidig må det gjøres kontinuerlig vurdering av risiko knyttet til egne verdier og håndtering av tilhørende risiko. Risikovurderingene må omfatte vurdering av verdier, identifisering av trusler og avdekking av sårbarheter. Risikovurderingene vil definere hva som er forsvarlig sikkerhetsnivå for kommunen og danner grunnlag for videre risikohåndteringsarbeid.

Noen av anbefalingene som ble gitt til Østre Toten kommune er gyldig for mange kommuner (forkortet versjon):

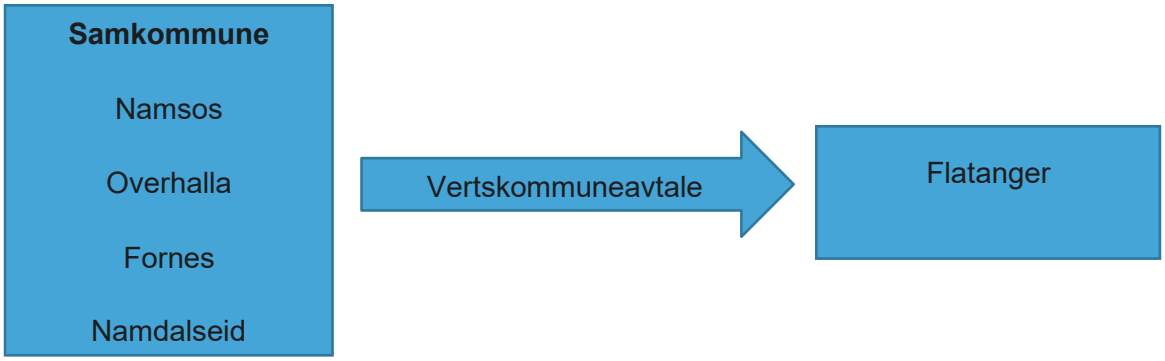
- Oppdatere kommunedirektørens internkontroll på IKT-sikkerhet i samsvar med anerkjente standarder.
- Gjennomføre jevnlige risikovurderinger, både overordnet, på IKT-avdelingen og tjenesteområdene.
- Innføre og styre etter NSMs grunnprinsipper.

Etter dataangrepet mot Østre Toten kommune sendte KS brev til kommunedirektørene og kommunens IT-ansvarlig/IT-sikkerhetsansvarlig i februar 2021. I brevene ga KS råd og anbefalinger som kommunen burde vurdere og at det er nødvendig at kommunene vurderer egen sikkerhets- og sårbarhetssituasjon. I brevet pekes det på følgende alvorlige konsekvenser av et dagangrep.

- Kommunen blir totalt lammet over lengre tid
- Kostnaden for å komme tilbake til normal drift vil kunne beløpe seg til 10-talls millioner
- Sensitive data på avveie kan innebære nasjonal risiko og eller brudd på personvern og rettssikkerhet til den enkelte borger, og som kan utløse erstatningskrav
- Andres IT-systemer kan bli rammet
- Tapt tillit til data og systemer

3 INFORMASJONSSIKKERHET I NAMSOS KOMMUNE

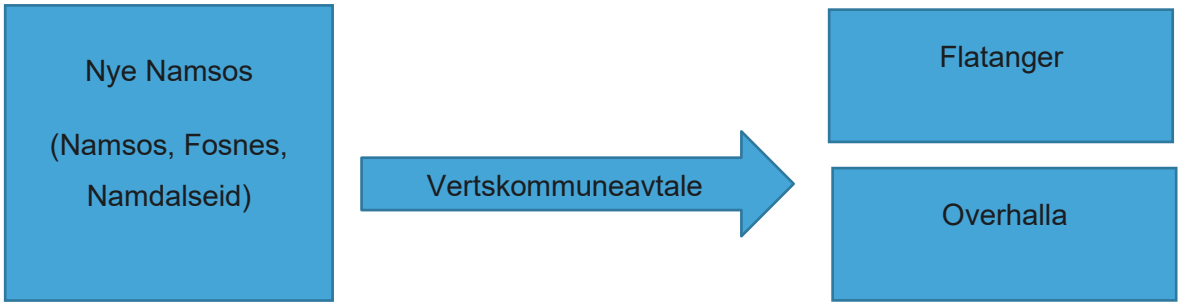
I 2009 ble Midtre Namdal Samkommune etablert som organisasjonsmodell for interkommunale tjenester for Fosnes, Namdalseid, Namsos og Overhalla. Midtre Namdal samkommune hadde en vertskommuneavtale med Flatanger kommune IKT, hvor Flatanger var fullt integrert i datasystemet, jf. figur 2.



Figur 2. IT samarbeid før kommunesammenslåingen

Med bakgrunn i den nye kommuneloven ble samkommunen avviklet 31.12.2019 og fra samme tidspunkt ble Namsos, Fosnes og Namdalseid kommune slått sammen til Namsos kommune. Etter den tid har det interkommunale samarbeidet mellom Nye Namsos og Overhalla fortsatt på flere områder, blant annet innenfor IKT.

I forbindelse med avvikling av samkommunen ble det inngått en vertskommuneavtale for IKT mellom Namsos kommune og de samarbeidskommunene som ikke be med inn i Nye Namsos kommune jf. figur 3. I 2019 ble det derfor inngått vertskommuneavtaler med Overhalla kommune og Flatanger kommune, med Nye Namsos kommune som vertskommune. (Midtre Namdal samkommune 2020). Avtalen er signert av prosjektleder for Nye Namsos som også var rådmann i den allerede sammenslåtte nye kommunen.



Figur 3. IT samarbeid etter kommunesammenslåingen

Årsmeldingen fra Midtre Namdal samkommune for 2019 peker på informasjonssikkerhet som en av utfordringene framover, sammen med opplæring og kompetanseheving, anskaffelser, brukerstyring og porteføljestyring.

Vertskommuneavtalen med Overhalla kommune ble inngått i mai 2019. Vertskommunen har ifølge avtalen ansvar for organisering av felles infrastruktur, IKT-oppgaver og programvare tilsvarende det som i dag er innenfor Midtre Namdal samkommune for samarbeidskommunen beskrevet i leveringsavtalen, som er vedlegg til vertskommuneavtalen. Leveringsavtalen er datert 27.03.2019.

I Namsos kommune ble det videreført et informasjonssikkerhetsutvalg fra Namsos kommune i forbindelse med kommunesammenslåingen. Utvalgets arbeid har blitt intensivert etter kommunesammenslåingen og arbeider med å sikre infrastruktur og personvern, samt innarbeide en god sikkerhetskultur. Informasjonssikkerhetsutvalget består av:

- Assisterende kommunedirektør
- Kommunalsjef personal og organisasjon
- Kommunalsjef strategi og samfunnsutvikling
- Driftssjef-IT og sikkerhetsansvarlig
- Personvernombud
- IKT-ansvarlig Overhalla
- IKT-ansvarlig Flatanger
- Spesialrådgiver-IT

4 INFORMASJONSSIKKERHET

Dette kapitlet er en forvaltningsrevisjon av informasjonssikkerhet i Namsos kommune. Følgende problemstilling belyses:

- Hvordan ivaretar Namsos kommune informasjonssikkerhet?

Forvaltningsrevisjonen er inndelt i fem områder med hver sine revisjonskriterier. Revisjonskriteriene er gjengitt først i hvert delkapittel. Utledningen av revisjonskriteriene finnes i vedlegg en.

4.1 Informasjonssikkerhet på strategisk nivå

4.1.1 Revisjonskriterier

- Kommunen skal regelmessig gjennomføre og dokumentere overordnede risikovurderinger som grunnlag for informasjonssikkerhetstiltak
- Kommunen skal ha sikkerhetsmål og sikkerhetsstrategi
- Kommunen skal ha en sikkerhetsorganisasjon hvor ansvar og roller for informasjonssikkerhet framgår

4.1.2 Overordnet system

Driftssjef-IT forteller at han bruker NIST CSF-standarden[8] i sitt arbeid på strategisk nivå. En stor del av dette rammeverket er risikovurderinger. Verktøyet er et gratis rammeverk som er utviklet for amerikanske myndigheter. Et referat fra informasjonssikkerhetsutvalget viser at NIST CSF-standarden er presentert og at den skal legges fram i juni 2022. Namsos kommune har tidligere vært sertifisert etter ISO 14001 (miljøledelse), men er ikke det lengre. Personvernombudet mener at kommunen burde vært sertifisert på kvalitet og personvernsikkerhet.

4.1.3 Overordnede risikovurderinger

Nasjonal sikkerhetsmyndighet har utarbeidet en veileder i sikkerhetsstyring. For å ivareta sikkerhetsarbeidet må virksomheten blant annet identifisere hvilke verdier virksomheten råder over, analysere risikoen for at verdiene kan gå tapt og iverksette og opprettholde nødvendig tiltak slik at verdiene er tilstrekkelig beskyttet[9].

[8] NIST CSR – National Institute of Standards and Technology Cybersecurity framework (US). Et sett med retningslinjer og anbefalinger for å redusere organisatoriske cybersikkerhetsrisikoer.

[9] Introduksjon - Nasjonal sikkerhetsmyndighet (nsm.no)

Namsos kommune utarbeidet sammen med Namdalseid og Fosnes kommuner en helhetlig risiko- og sårbarhetsanalyse (ROS) like før sammenslåingen. Den ble vedtatt av kommunestyret i Namsos 14.11.2019. I kommunens planstrategi er helhetlig ROS planlagt gjennomført i 2023. ROS fra 2019 er avgrenset til hendelser og forhold, som har et større omfang enn hva som løses i den ordinære linjeorganisasjonen. Forhold som ikke berøres i den helhetlige ROS vil være tema i ROS på ulike fagområder. ROS analysen fra 2019 omhandler 14 uønskede hendelser, hvor bortfall av elektronisk kommunikasjon kan relateres direkte til informasjonssikkerhet. Det er ett eksisterende tiltak på området elektronisk kommunikasjon og ingen nye i planer. Tiltaket er å sikre tilgang til kommunens informasjonssystemer, IT-verktøy og data uten elektronisk kommunikasjon (lastet ned lokalt). Den helhetlige ROS er basert på veilederen fra Direktoratet fra sikkerhet og beredskap fra 2014. Den inneholder lite om informasjonssikkerhet.

4.1.4 Sikkerhetsmål og sikkerhetsstrategi

I Namsos kommune sin samfunnsplan 2020-2032 (vedtatt 13.02.2020) er digitalisering et av innsatsområdene og det skal oppnås blant annet gjennom å bruke trygge og sikre digitale løsninger. Dette skal følges opp gjennom en digitaliseringsstrategi og en sikkerhetsplan/-tiltak. Kommunalsjef for strategi og samfunn forteller at kommunen jobber med digitaliseringsstrategien som en del av en FoUI[10]-strategi som skal legges fram i 2022. Videre informerer kommunalsjefen at informasjonssikkerhet er et vesentlig moment for å kunne benytte de stadig større mulighetene digitalisering gir, og det er viktig med et kontinuerlig fokus på informasjonssikkerhet.

Det vil også være et samarbeid med andre kommuner i Trøndelag om felles digitale løsninger, jf. samhandlingsstrategien for digital utvikling[11]. Et av delmålene under innsatsområdet samfunnssikkerhet og beredskap er at kommunen skal jobbe helhetlig og systematisk for å redusere risiko og forebygge uønskede hendelser. Dette skal følges opp med blant annet en oppdatert ROS og en oppdatert og øvd beredskapsplan.

Namsos kommune har en *strategi for internkontroll informasjonssikkerhet og personvern*, sist oppdatert 23.03.2022. Denne sikkerhetsstrategien er en del av Namsos kommune sitt styringssystem for informasjonssikkerhet og personvern. Dokumentet viser hvilke dokumenter som inngår i sikkerhetsstrategien, hvem som er ansvarlig og status.

I sikkerhetsstrategien skilles det mellom hovedpunktene:

- Organisering - sikkerhetsorganisasjon (her opplyses det at status kommer)

[10] FoUI - forskning, utvikling og innovasjon

[11] Avtale knyttet til samarbeid vedrørende digitalisering. Signert av Namsos kommune 09.11.2020.

- Instruks - fire instrukser som alle er tatt i bruk i 2020
    - Instruks for informasjonssikkerhet
    - Sikkerhetsinstruks medarbeider
    - Sikkerhetsinstruks leder
    - Taushetserklæring.
- Rutiner - 19 rutiner hvor noen er tatt i bruk i 2021, 2022 og noen som kommer
- ROS - tre områder som alle er i arbeid i 2022
- DPIA - nytt sak og arkivsystem i arbeid i 2022
- Systemoversikt - i arbeid i 2022
- Avvik - Melding til Datatilsynet, i bruk i 2021 og generell rutine i bruk i 2019
- Ledelsens gjennomgang - rutiner som kommer

I informasjonssikkerhetsinstruksen står det at kommunens sikkerhetsmål er:

> *Den fysiske sikkerheten ved Namsos kommune skal hindre uautoriserte å få adgang til lokaler der beskyttelsesverdig informasjon og sensitive personopplysninger lagres og behandles.*

I oppstartmøtet fortelles det at IT-sikkerhet er tatt inn i kommunens samfunnsplan og henvist til i økonomiplanen, men kun på overordnet nivå. Noe ligger i kommunens kvalitetssystem. Kommunen skal gå over til et nytt kvalitetssystem og i den forbindelse har det skjedd en opprydding i og fornyelse av dokumenter. Kommunen har ingen uttalt sikkerhetsstrategi, men mange aktiviteter og prosedyrer som naturlig hører hjemme der. Kommunens planstrategi inneholder ikke en sikkerhetsstrategi.

Personvernombudet informerer om at det finnes noen målsettinger og strategier fra 2010, som skal revideres før de legges ut i nytt kvalitetssystem. De har ikke vært tilgjengelig for ansatte etter kommunesammenslåingen.

Kommunen har ingen nedskrevne mål og strategier knyttet til informasjonssikkerhet. Det er et stadig mer fokus på at kommunene bør ha en informasjonssikkerhetsstrategi. IT-lederen mener at det er mulig at dette bør være en del av digitaliseringsstrategien.

4.1.5 Sikkerhetsorganisasjon

I strategi for internkontroll informasjonssikkerhet og personvern, går det fram at sikkerhets-organisasjon har status som *kommer.*

Kommunen har et informasjonssikkerhetsutvalg. Informasjonssikkerhetsutvalget har utarb-eidet to offentlige rapporter fra arbeidet sitt, som er behandlet i arbeidsmiljøutvalget i kommunen. Referatene fra informasjonssikkerhetsutvalget er ikke offentlig ettersom de kan

inneholde sensitiv informasjon. Revisor har fått tilgang til informasjonssikkerhetsutvalgets referater og dokumenter.

Driftssjef på IT har ansvar for oppsett og drift av servere og har rollen som sikkerhetsansvarlig. Det finnes ingen stillingsbeskrivelse for jobben som sikkerhetsansvarlig, opplyser driftssjefen.

Driftssjef-IT er usikker på om kommunen har en sikkerhetsorganisasjon, og tenker at informasjonssikkerhetsutvalget kan være en slik organisasjon. Driftssjef-IT vil gjerne ha på plass en CISO (Chief Information Security Officer), som er tett på kommunedirektøren og som har innflytelse på forhold som påvirker informasjonssikkerheten. I dagens situasjon blir ikke alltid sikkerhetsbaserte ting gjennomført fordi det ikke passer resten av organisasjonen, noe som er en risiko. I faktaverifiseringen peker kommunalsjef personal og organisasjon på at det er gjort investeringer på it-sikkerhet etter råd fra IT, og at ledelsen ikke kjenner seg igjen i at det er en risiko at sikkerhetsbaserte ting ikke blir gjennomført fordi det ikke passer resten av organisasjonen. Driftssjef opplever å bli motarbeidet fra andre områder, dersom sikkerhets-anordninger medfører merarbeid eller andre måter å gjøre ting på, og viser til motstand da tofaktorautentisering[12] ble innført. I Norge og norske kommuner er det ikke så vanlig å ha en person som kan ta avgjørelser når det gjelder sikkerhetsorienterte forhold, og som kan iverksette strakstiltak ved behov. Driftssjef-IT kan gjøre dette hvis han må, men mangler egentlig myndighet.

I det daglige er det driftssjef-IT og en seniorkonsulent som arbeider med det overordnede sikkerhetsbildet. Dokumentasjon som lages på dette ligger på en egen Teams-gruppe.

Flere av personene på IT opplever at IT er litt feil plassert og langt ned i organisasjonshierarkiet etter kommunesammenslåingen. IT-leder forteller at arbeidslogikken for IT er veldig annerledes enn resten av enheten personal og organisasjon.

Det som skjedde i Østre Toten kommune har vært en vekker for resten av kommunen forteller driftssjef-IT. Det har blitt fokus på forhold som driftssjefen har mast på lenge. Driftssjefen skulle ønske at IT hadde en mer sentral rolle i kommunen og kunne satt dagsorden mer. Det er vanskelig å jobbe forebyggende slik situasjonen er nå. Driftssjef og sikkerhetsansvarlig er egentlig to stillinger og vanlig drift har mye tid som skulle vært brukt på sikkerhetsarbeid. Sikkerhetsarbeid kommer ofte i andre rekke fordi et driftsproblem har oppstått og må løses. Spesialkonsulenten er også en enorm ressurs og pådriver i sikkerhetsarbeidet, men også

[12] Tofaktorautentisering - betyr at det benyttes to ulike trinn for å bekrefte identitet

vedkommende har driftsansvar som gjør at sikkerhetsarbeidet ofte kommer i andre rekke. Informasjonssikkerhetsutvalget bidrar godt til kartlegging av det forebyggende arbeidet.

4.1.6 Vurdering

Kommunen har ikke regelmessig gjennomført og dokumentert en overordnet risikovurderinger som omfatter informasjonssikkerhet og gir grunnlag for informasjonssikkerhetstiltak.

Kommunen har en helhetlig og overordnet risiko- og sårbarhetsvurdering fra 2019 hvor elektronisk kommunikasjon inngår. Revisor finner at kommunen har gjort risikovurderinger på fire områder innenfor informasjonssikkerhet. Revisor savner en helhetlig tilnærming for informasjonssikkerhet som er overordnet for de mer spesifikke risikovurderingene som gjøres. Dette gjør at det kan bli litt tilfeldig hvordan risikovurderingen bygges opp og hvilke områder som risikovurderes. Etter revisors oppfatning må det vurdere om informasjonssikkerhet bør få en større plass i overordnet risiko og sårbarhetsvurdering, ettersom eksempelvis et dataangrep kan få store konsekvenser for hele kommuneorganisasjonen.

Namsos kommune har ikke sikkerhetsmål, og en sikkerhetsstrategi knyttet til informasjonssikkerhet.

Kommunens sikkerhetsmål er formulert i informasjonssikkerhetsinstruksen og omhandler fysisk sikkerhet for beskyttelse av informasjon og sensitive personopplysninger. Revisor har ikke funnet sikkerhetsmål som omhandler informasjonssikkerhet og heller ingen sikkerhetsstrategi. Det innebærer at det mangler overordnede føringer for informasjonssikkerhetsarbeidet, som er basert på vurderinger av risiko og hvilke informasjonsverdier kommunen har, som det er viktig å beskytte. Målsettinger og strategier danner igjen grunnlaget for de sikkerhetstiltakene som iverksettes.

Kommunen har ikke en sikkerhetsorganisasjon hvor ansvar og roller for informasjonssikkerhet framgår.

Namsos kommune har et informasjonssikkerhetsutvalg, som selv omtaler seg som sikkerhetsorganisasjon. Driftssjef-IT har rollen som sikkerhetsansvarlig. Revisor opplever at det er uklart hvordan arbeidet med informasjonssikkerhet er organisert. Informasjonssikkerhetsutvalget er et godt fundament, men det er uklart hvilken plassering og rolle det har i kommuneorganisasjonen. Det er positivt at assisterende kommunedirektør og flere kommunalsjefer er medlemmer, men den formelle rollen er uklar, noe som gir manglende legitimitet og dermed er en risiko i seg selv.

4.2 Ledelsesnivået

4.2.1 Revisjonskriterier

- Det skal gjennomføres og dokumenteres risikovurderinger innenfor informasjonssikkerhet
- Informasjonssikkerhet skal inngå i kommunens internkontrollsystem
- Kommunen må ha rutiner med tilhørende praksis for tildeling og fjerning av tilganger og jevnlig kontrollere identiteter og tilganger
- Kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet
- Kommunen bør vurdere og dokumentere IKT-risiko ved anskaffelser av datasystemer

4.2.2 Ledelsesinformasjonssystem

Jøsang (2021) skriver at ledelse av informasjonssikkerhet bør være basert på et ledelsesinformasjonssystem bygd opp av et sett med prosesser og aktiviteter definert av et utvalg av standarder, rammeverk og egendefinerte retningslinjer og policyer, eksempelvis ISO 27001. Driftssjef-IT har et regneark som viser hvordan kommunen ligger an i forhold til NIST CSF-standarden. Revisor har sett dette regnearket. Rammeverket er delt inn i fire hovedgrupper, identifisere, beskytte, oppdage, gjenopprette og respondere. Driftssjef-IT har gjort vurderinger av hvordan kommunen ligger an i forhold til et mål på fire. Svært få av de forholdene som er vurdert har status fire. Hovedvekten ligger på status to.

4.2.3 Risikovurderinger innenfor informasjonssikkerhet

Dokumentet *strategi for internkontroll informasjonssikkerhet og personvern i Namsos kommune*, viser at det er gjort tre risikovurderinger, datakriminalitet, pålogging og sak- og arkivsystemet Elements. Revisor har fått tilgang til fire risikovurderinger på informasjonssikkerhet. Det er risikovurdering knyttet til:

- Elektronisk pasientjournal
- Pålogging
- Datakriminalitet
- Elements

Risikovurderingen av pålogging og datakriminalitet har vært behandlet i informasjonssikkerhetsutvalget. Det refereres til at risikovurderingene er utarbeidet på grunnlag av en sjekkliste med påstander som Arbeidstilsynet har utarbeidet. I begge dokumentene er en uønsket hendelse vurdert.

Risikovurderingen i forhold til datakriminalitet er datert 20.01.2020 og det opplyses at den er gjennomført i forbindelse med ROS på helse/IT. Det er bare løsepengevirus som er vurdert og det vil gi konsekvenser som at systemer går ned og mange berøres. Tiltakene er skybaserte systemer, økte ressurser på sikkerhet, beredskap og ansattes oppmerksomhet.

Risikovurderingen om pålogging er datert 19.01.2020 og er utført av personvernombudet og driftssjef-IT. Risikovurderingen er knyttet til at påloggingsadresse og brukernavn for Office 365 er det samme som epostadressen. Det skisseres flere tiltak med frist for gjennomføring 30.04.2022.

I risikovurdering av nytt sak og arkivsystem, Elements, er 14 forhold vurdert. Noe er merket som *ikke ferdig*. I årsmeldingen fra personvernombudet i Namsos kommune går det fram at kommunene i Midtre og Indre Namdal har etablert et samarbeid for å utarbeide og dele rutiner og retningslinjer for forsvarlig behandling av personopplysninger samt utarbeide ROS og DPIA (data protection impact assessment), som er en vurdering av personvernkonsekvenser for Elements.

Risikovurderingen for elektronisk pasientjournal følger en annen mal enn de tre andre risikovurderingene. I den er 17 forhold vurdert.

I oppstartsmøtet fortelles det at det er informasjonssikkerhetsutvalget som har gjort ROS analysene. Informasjonssikkerhetsutvalget jobber med å kartlegge og håndtere risiko.

Personvernombudet samarbeider med IT om risikoanalyser. De har ikke kommet langt i arbeidet, men de har blitt enig om hvordan de skal gjøre det, forteller personvernombudet. Resultatet fra risikoanalysene skal overføres til en DPIA og risikoanalysen fra Elements er grunnlaget for en DPIA som er påbegynt. Informasjonssikkerhetsutvalget er informert om risikoanalysene knyttet til informasjonssikkerhet og personvern, forteller personvernombudet.

Driftssjef-IT forteller at det er litt problematisk at samarbeidskommunene kan ha forskjellige fagsystemer som utfører de samme oppgavene. Dette gir merarbeid for IT ettersom det må settes opp flere integrasjoner mellom systemer. Det er også en sikkerhetsrisiko ettersom mange eksterne konsulenter fra ulike leverandører er inne og gjør ting i systemene, forteller driftssjef-IT. Kompetansen på IT-sikkerhet er veldig varierende hos de eksterne konsulentene. I tillegg innebærer selve samarbeidet en risiko, blant annet fordi et dataangrep kan spre seg fra en kommune til en annen. Driftssjef-IT forteller at det hender at andre i kommunen tar snarveier uten at dette er klarert med IT. Et eksempel var en server som skulle styre låsene i de kommunale dørene, som ble plassert i det åpne nettet. Ut fra et sikkerhetsperspektiv burde denne vært mer avsperret og IT ble oppmerksom på dette ved en tilfeldighet, forteller driftssjef-IT.

IT-konsulentene forteller at det gjøres bestandig en risikoanalyse ved overgangen til nye systemer. Dette for å sikre at informasjon ikke kommer på avveie.

4.2.4 Internkontroll

I dokumentet *strategi for internkontroll, informasjonssikkerhet og personvern*, ligger et rammeverk for internkontroll. Statusen for de ulike delene viser at noe er på plass, noe er i arbeid og noe kommer. Ledelsens gjennomgang av internkontrollen har status som *kommer*.

I Handlingsprogram med økonomiplan 2022-2025[13] går det fram at det mangler en helhetlig struktur på internkontrollen i kommunen. I oppstartsmøtet fortelles det at kommunen har et internkontrollsystem og at informasjonssikkerhet inngår her.

Personvernombudet er involvert i informasjonssikkerhet i arbeidet med nytt kvalitetssystem og forteller at det er viktig å få på plass et nytt kvalitetssystem slik at kommunen har tilfredsstillende internkontroll. Personvernombudet er prosessdriver for nytt kvalitetssystem og holder på å bygge det opp og de fleste enhetene i kommunen har ikke dette på plass. IT-avdelingen har god oversikt over hva som finnes og mangler i kvalitetssystemet på eget område, men ferdigstillelse tar tid fordi de må prioritere drift, forteller personvernombudet.

Kvalitetssystemet er utgangspunktet for internkontrollen, forteller personvernombudet. Det er forskjellige rutiner på forskjellige enheter, selv om de jobber med samme område. Rutinene mangler også henvisninger til lovverket. Tidligere kunne alle lage rutiner i systemet, men dette er nå begrenset til kommunalsjefer og virksomhetsledere. Det ligger dokumentmaler for rutiner i det valgte systemet. Styring og avvik ligger i systemet og alt må knyttes sammen i forhold til drifta. Det tar tid å få på plass kvalitetssystemet, sier personvernombudet.

Personvernombudet forteller at det er utarbeidet fire rutiner for håndtering av personopplysninger. Det er:

- Innsyn i egne personopplysninger
- Innhenting av personopplysninger
- Den registrertes rettigheter
- Retting og sletting av personopplysninger

Alle lederne har tilgang til rutinene og det forventes at lederne distribuerer disse til sine ansatte.

[13] Framsikt

Personvernombudet får en del henvendelser fra ansatte og det registreres en del avvik knyttet til håndtering av personopplysninger. Ofte er det spørsmål om noe er et avvik og om hvordan det skal håndteres. Det har ikke vært mange henvendelser i det siste.

Når det gjelder personopplysningsloven, er noe på plass, men det er mer som mangler enn det som er plass, forteller personvernombudet. Bruken av kvalitetssystemet har vært vanskelig å få til, særlig det at lederne skal lære opp sine ansatte. Det er utfordrende å få de ansatte til å se helheten i det de gjør. Kommunen har fått på plass et informasjonssikkerhetsutvalg og ansatte på IT har også kommet mer på banen, selv om de har et sterkt fokusert på drift.

4.2.5 Rutiner og kontroll med tilganger

Revisor har fått tilgang til dokumenter i kvalitetssystemet som omhandler regulering av tilganger til kommunens IT-system og fagsystemer. Følgende dokumenter omtales i fortsettelsen:

- Taushetserklæring (med signering)
- Informasjonssikkerhet - instruks (med signering)
- Sikkerhetsinstruks for medarbeidere
- Sikkerhetsinstruks for ledere

I instruksen for informasjonssikkerhet beskrives brukeradministrasjon. Her går det blant annet fram at:

- IKT-enheten tildeler brukernavn og førstegangs passord for pålogging til Namsos kommune sitt domene. Passord for tilgang til fagsystemer opprettes om nødvendig av systemansvarlig for de respektive fagsystemene.
- Det er ikke tillatt å opprette felles bruker eller å dele passord.
- Instruksen beskriver retningslinjer for opprettelse av passord, som ikke trenger fornyelse.
- Datamaskinene skal låses ved fravær i kortere perioder. Automatisk passordbeskyttet skjermsparer aktiveres etter 15 minutter.
- Det skal alltid logges ut når datamaskinen overlates til andre.

I *instruksen for informasjonssikkerhet* går det fram at tofaktorautentisering brukes for å sikre autorisert tilgang til kommunes programvare og filer, utenfor kommunes lokaler. I rapporten fra informasjonssikkerhetsutvalget står det at multifaktorautentisering er tatt i bruk.

Hvis en medarbeider har behov for annen programvare kan IKT-enheten gi midlertidig administrasjonsrettigheter.

I *sikkerhetsinstruksen for medarbeidere* går det fram at når ansatte slutter eller ved lengre permisjoner skal nøkler/nøkkelkort leveres inn og det samme gjelder for datautstyr om ikke annet er avtalt med arbeidsgiver. Utrangert og kassert datautstyr leveres IKT-avdelingen for destruksjon.

Sikkerhetsinstruksen for ledere regulerer at kommunalsjefer, virksomhetsledere og avdelingsledere skal bestille relevante tilganger til informasjonssystemer, både opprettelse, endring og avslutning. Tilgang til databruker bestilles hos IKT-avdelingen, tilgang til fagsystemer bestilles hos systemansvarlige og tilgang til å bruke hjemmekontor må bestilles hos IKT-avdelingen (egen rutine). Lederne skal også bidra til en periodisk gjennomgang av medarbeidernes tilganger en gang i året.

Det kommer fram i oppstartsmøtet at kommunen er god på å opprette brukere, men ikke på å slette. Kommunen har en gjennomgang av bruker- og adgangsstyringen. IT-lederen forteller at i forbindelse med kommunesammenslåingen, ble det gjort en opprydning i antallet brukere og adganger. Kommunen er ikke i mål med dette arbeidet og IT-avdelingen har sett etter programvare som kan bidra til å holde orden på brukerne, men ikke funnet noen løsning som virker god.

I oppstartsmøtet fortelles det at tilgangsstyring er en sårbarhet i systemene og at det derfor er nødvendig å ha en oversikt over hvem som gir tilganger i de forskjellige systemene, samt at det er viktig å følge opp at personer mister tilgang når de ikke skal ha den lengre.

Driftssjef-IT forteller at IT har kontroll på tilgangen til kommunens datasystem gjennom opprettelsen av Office/Windows-brukere, som alle må ha. Tilgangen til de ulike fagsystemene både bestemmes og gis ut på de ulike avdelingene. Kommunen har et egenutviklet system BOSS, hvor ledere kan legge inn bestillinger for at ansatte skal få tilgang til fagsystemer. Kommunalsjef personal og organisasjon informerer om at i BOSS registreres nyansatte i systemet og de tildeles epostadresse og passord, og at det må opprettes tilganger i de ulike fagsystemene i tillegg.

IT-avdelingen ser at antall ansatte i lønnssystemet, personalsystemet og systemet for tilgangsstyring ikke stemmer overens, forteller IT-lederen. Videre må IT-avdelingen kjøpe nye lisenser hele tiden, til tross for at antallet ansatte ikke øker. Utfordringen er å fjerne brukere når noen slutter. IT-leder forteller at etter overgangen til skybaserte tjenester, må kommunen betale for kontoen for at en brukers personlige innhold skal beholdes. Avvikles lisensen forsvinner epost etter 30 dager og brukerinnholdet etter 90 dager.

IT-konsulenten forteller at det er en svakhet i arbeidet med å frata brukere tilganger, fordi det ikke gis beskjed om at brukere slutter eller bytter jobb. Her burde kommunen hatt et bedre system, siden dagens system ikke sørger for at alle tilganger slettes når de ikke lenger trengs. Kommunalsjef personal og organisasjon forteller at kommunen arbeider med dette i dag i forbindelse med mulighetsstudie på interne tjenester.

Kommunen bruker ikke to-faktorautentisering på fagsystemer internt, forteller driftssjef-IT. Fagsystemer som er plassert i skyløsninger har aktivert multifaktor autentisering, tror driftssjef-IT. Dette kan enten være igjennom kommunenes Office365-løsning eller andre løsninger som for eksempel ID-Porten. Det er ingen multifaktor autentisering på lokale systemer.

4.2.6 Opplæring og sikkerhetskultur

Informasjonssikkerhetsinstruksen inneholder regler for ansattes bruk av datasystemer og spesielt håndtering av personopplysninger. Informasjonssikkerhetsinstruksen er utformet som en egenerklæring, som ansatte må signere på. Informasjonssikkerhetsutvalget har diskutert at sikkerhet kan inngå i medarbeidersamtalen. Rutinebeskrivelsen for medarbeidersamtale er endret slik at sjekklisten nå har et punkt om informasjonssikkerhet og personvern.

Det går fram av informasjonssikkerhetsinstruksen at arkivdokumenter og utskrifter som inneholder personsensitive eller annen taushetsbelagt informasjon ikke skal ligge framme på kontorer eller andre steder slik at uvedkommende får tilgang. Personsensitiv informasjon skal ikke lagres på minnepinne eller annen mobil lagringsenhet. Alle skal logge seg ut av dataprogrammer ved dagens slutt. Utlån av dokumenter med sensitiv informasjon skal skje via den som er ansvarlig for oppbevaringen og registreres. Fortrolige utskrifter skal skrives ut med sikret utskrift.

Informasjonssikkerhetsinstruksen sier at det er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte opplysninger uten at det er begrunnet i hjemmel i lov eller forskrift. Det tillates heller ikke snoking i dokumenter, som ikke er relatert til eget arbeid.

Sikkerhetsinstruksen for ledere pålegger kommunalsjefer, virksomhetsledere og avdelingsledere å sørge for at det gis nødvendig opplæring i informasjonssystemer. Om opplæring står det at før en medarbeider får tilgang til aktuelle IKT-systemer skal vedkommende i samarbeid med nærmeste leder bidra til at en får tilstrekkelig opplæring i rutiner og regelverk, i bruk av IKT-systemer og i informasjonssikkerhet. Sikkerhetsinstruksen for ledere sier at lederne skal sørge for at personvern og informasjonssikkerhet hvert år settes på dagsorden ved enheten for å bevisstgjøre egne medarbeidere.

Konsulenten ved dokumentsenteret forteller de har opplæring knyttet til saksbehandlingssystemet omtrent daglig via Teams. I opplæringen legges det vekt på at skjerming er viktig, men det er ingen bevisst opplæring knyttet til personopplysninger i denne forbindelse.

Den største sikkerhetsrisikoen hviler den enkelte ansatte, forteller driftssjef-IT. Ansatte må selv gjøre vurderinger og handlinger ved mottak av epost (phishing), SMS og telefonoppringninger. Ansatte fungerer dermed som en *menneskelig brannmur* og IT må stole på at ansatte gjør de riktige valgene, eller rapporterer dersom de tror de har blitt lurt.

Seniorkonsulent-IT sier at det er mye som kan unngås ved å ha forsiktige og sikkerhetsbevisste brukere. Det er ingen systematisk opplæring av ansatte når det gjelder informasjonssikkerhet. Kommunen sender ut informasjon via Teams ved behov. Bevisstheten knyttet til informasjonssikkerhet er blitt bedre de siste årene.

Mye kan gjøres via opplæring og driftssjef-IT har brukt en phishing-simulator for å gjøre falske angrep rettet mot kommunens ansatte og får tilbakemeldinger basert på dette. Driftssjef-IT forteller at hvis det kommer konkrete trusler så legges det ut informasjon om dette på Teams slik at ansatte kan være ekstra påpasselig. IT-avdelingen prøver å informere ansatte om mulige angrep, men det er farlig å sende for mye informasjon, forteller IT-konsulenten. Hvis det kommer for mye informasjon tar ikke brukerne dette inn over seg.

IT-konsulenten har ansvaret for oppfølging av sak og arkivsystemet, og forteller at ansatte er flinke til å melde feil i ePhorte. Det er stort sett brukerfeil som ligger til grunn for henvendelsene.

De fleste ansatte tenker nok at IT-sikkerhet er IT-avdelingen sitt ansvar, forteller IT-lederen. Det er ingen oppfatning av at dette er et felles ansvar, heller ikke blant ledelsen i kommunen. IT-avdelingen har sjelden kontakt med resten av organisasjonen. IT-leder mener at den operasjonelle driften går på bekostning av det strategiske arbeidet. I faktaverifiseringen skriver kommunalsjef personal og organisasjon at ledelsen ikke kjenner seg igjen i at IT-avdelingen har sjelden kontakt med resten av organisasjonen.

4.2.7 Anskaffelser

Driftssjef-IT gir føringer for hvilke løsninger kommunen skal velge basert på vurderinger av sikkerhet. Driftssjef-IT forteller at det hender at andre i kommunen tar snarveier uten at dette er klarert med IT, jfr. anskaffelse av låser omtalt i kapittel 4.2.3

Når IT-avdelingen anskaffer ny programvare, gjennomføres det risikovurderinger. Driftssjef-IT, seniorkonsulten og IT-konsulenten opplever at de noen ganger blir lite involvert og kommer for sent inn i prosessen når det gjelder anskaffelse av ny programvare. Ofte blir det innført programmer med alt for mye rettigheter, forteller driftssjef-IT. IT blir ofte ikke involvert før i

etterkant av anskaffelsen. Driftssjef-IT savner en strukturert måte å anskaffe programvarene på. Mye er skybasert, noe som gjør kommunen mindre utsatt for angrep. IT-konsulenten forteller at når de kommer for sent inn i prosessene kan det gi utfordringer nettverkstilgang og brannmurer.

IT-lederen forteller at det i samkommunen var det mer samarbeid mellom kommunene. Etter overgangen til vertskommune er det flere tilfeller hvor kommunene på egen hånd kjøper inn systemer, noe som medfører problem og merarbeid knyttet til integrering. For eksempel er det kjøpt inn forskjellige systemer for forvaltning av eiendommer. Kommunene har også valgt ulike kvalitetssystemer og IT-leder mener at kommunen ikke klarte å ta med seg de gode relasjonene fra samkommunen inn i den nye samarbeidsformen.

IT-leder opplever at det kjøpes inn systemer og utstyr som skal implementeres og driftes av IT, uten at det er noen dialog med IT før innkjøp skjer.

Driftssjef-IT forteller at IT kan få henvendelser om programvare som ønskes brukt, som ikke er avklart med IT tidligere. Dette kan være en utfordring, fordi programvaren faktisk kan anses som en sikkerhetstrussel. Et eksempel på dette er en henvendelser om å installere Python (script-språk). Enkelte lærere har vært på kurs og noen (ukjent og ikke klarert med IT) har bestemt at dette skal brukes i undervisningen for å lære elever programmering. Driftssjef-IT anser dette som en stor trussel for IT-sikkerheten og at det ikke er ønskelig å installere programmet på PCer i administrasjonsnettet. Saken løses gjennom en større operasjon med å flytte lærerne ut av administrasjonsnettet, for å gi dem mulighet til å installere og bruke Python. Dette ble plutselig en arbeidsoppgave som involverer mange på IT-avdelingen.

4.2.8 Vurdering

Namsos kommune har enkelte risikovurderinger innenfor informasjonssikkerhet.

Av de fire risikovurderingene revisor har sett, framstår risikovurderingen knyttet til Elements og elektronisk pasientjournal som mest gjennomarbeidet. Revisor savner en mer helhetlig tilnærming til hvilke risikovurderinger som burde vært gjort og som hadde vært forankret i en overordnet risikovurdering innenfor IT, jf. kapittel 4.1.6. Det ser ut til å være litt tilfeldig hvem som har ansvaret for å bestemme hvilke risikovurderinger som skal gjøres og hvem som gjør dem. Noen av risikovurderingene vurderes som mangelfulle eller veldig begrenset.

Namsos kommune har ikke et internkontrollsystem hvor informasjonssikkerhet inngår.

Revisor finner at Namsos kommune ikke har på plass et oppdatert kvalitetssystem, men skal ta i bruk et nytt kvalitetssystem som grunnlag for internkontroll. Det foregår en opprydding i rutiner fra det gamle kvalitetssystemet og en oppgradering til det nye.

Namsos kommune har rutiner med tilhørende praksis for tildeling av brukere, mens fjerning av brukere skjer mer tilfeldig.

I Namsos kommune gir IT brukertilgang til kommunens IT-system, mens tilgangen til fag-system er delegert til lederne og skjer i et eget program BOSS. Det er ingen rutine eller praksis for fjerning av tilganger når ansatte slutter. Når oversikter fra personalsystemet, lønnssystemet og tilgangssystemet ikke stemmer overens er det tydelig at det ikke er kontroll på bruker-tilgangene. Kontroll med brukertilganger er et viktig sikkerhetstiltak og spesielt avvikling av brukertilganger har ikke kommunen kontroll på. Brukertilganger har også en kostnadsside som gjør at det vil være interessant å avvikle brukere som har sluttet. Det ser også ut til å være dårlig oppfølging av innsamling av datautstyr når noen slutter, slik at kommunens datautstyr med eventuelle tilganger brukes etter at arbeidsforholdet er avsluttet.

Namsos kommunen gir opplæring i informasjonssikkerhet til nyansatte og skal gjennomføre årlige opplæringstiltak.

Det er en rutine for at ansatte får opplæring i informasjonssikkerhet ved ansettelse og at det skal gjennomføres årlige opplæringstiltak. I tillegg informerer IT-avdelingen om trusler og forhold som ansatte bør være oppmerksomme på. Opplæringstiltakene er viktig for å bygge en sikkerhetskultur. Det er revisors oppfatning at kommunen har et forbedringspotensial i å bygge en sikkerhetskultur. Til det trengs en mer solid forankring i kommuneledelsen og en mer utbredt forståelse for sikkerhetstrusler og behovet for sikkerhetstiltak.

Namsos kommune vurderer ikke IKT-risiko ved anskaffelse av alle datasystemer.

Revisor vurderer at IKT risiko ikke alltid vurderes ved anskaffelse av alle systemer som skal knyttes til nettverket. IT-avdelingen kommer ofte for sent inn i prosessene og revisor vurderer at dette kan innebære en sikkerhetsrisiko i tillegg til at løsninger ikke trenger å bli optimal driftsmessig. Ettersom IT involveres sent, har de ikke muligheten til å gjøre risikovurderinger forut for anskaffelsen.

4.3 Forebyggende tiltak

IT-konsulenten forteller at truslene som er rettet mot kommunen utvikler seg hele tiden. Det er anskaffet forskjellige sikkerhetsverktøy som kan oppdage ting. IT-avdelingen får innspill angående trusler fra kollegaer i andre kommuner og leverandører. Kommunen har så langt klart å stoppe det meste. På grunn av manglende budsjett er kommunen nødt til å prioritere hvilke tiltak som settes inn. IT-avdelingen har et eget budsjett, men for større investeringer må dette tas oppover i systemet.

IT-avdelingen gjør tiltak basert på egne sikkerhetsvurderinger, men er mer usikker på om de har den formelle myndigheten, forteller seniorkonsulent-IT. Det må tas mange store og små avgjørelser rundt sikkerhet, men dette skal helst ikke påvirke brukerne unødvendig.

4.3.1 Revisjonskriterier

- Kommunen må ha en oversikt over enheter i IT-systemet
- Kommunen bør etablere en sikker IT-arkitektur
- Kommunen må ha en oversikt over programvare som er i bruk, som tilfredsstiller kravene til en behandlingsoversikt
- Kommunen skal beskytte virksomhetens data
- Kommunen bør ha sentral styring med sikkerhetsoppdateringer
- Kommunen må sikkerhetskopier

4.3.2 Oversikt over enheter IKT-systemet

I informasjonssikkerhetsinstruksen går det fram at PCer, smarttelefoner, nettbrett og lagringsmedium og annet portabelt utstyr skal konfigureres av IKT-enheten. All maskinvare og lagringsmedium/harddisk skal være registrert hos IKT-enheten. Lagringsenheter skal leveres IKT-enheten for destruksjon.

Driftssjef-IT forteller at kommunen har en skyløsning hvor alle PCer meldes inn og administreres, *Microsoft Insight*. Det er installert en agent på hver enkelt PC som rapporterer dens tilstedeværelse og eventuelle alarmer til den skybaserte SIEM[14] løsningen Rapid7 Insight, og antivirusprogrammet Windows Defender Cloud. SIEM gir sanntidsanalyse av sikkerhetsvarsler som er generert av applikasjoner og nettverksmaskinvare (Wikipedia 02.05.2022).

[14] SIEM - Security Information and Event Management

Alle nye mobiler og nettbrett legges også automatisk inn i Insight for administrasjon og styring. Dette gjelder ikke Android-enheter. Disse må registreres i Insight manuelt og noen av enhetene har dermed IT ikke kontroll over.

IT-avdelingen har startet implementering av et system for tilgangsstyring på portnivå, NAC (Network Access Control). Denne vil sørge for at bare godkjente og ellers kjente enheter får kontakt med nettverket når de plugges inn i en switch. Ukjent utstyr vil ikke få tilgang til nettverket.

Kommunen har per april 2022 ikke kontroll på teknisk utstyr som plugges inn rundt omkring på alle kommunens lokasjoner inkludert samarbeidskommunene, forteller driftssjef-IT og seniorkonsulent-IT. Eksempelvis ble det ved en tilfeldighet avdekket at fysioterapeuter brukte private PCer, som de koblet til kommunens nettverk. Seniorkonsulent-IT forteller at det er gjort risikovurdering på dette. Det forekommer også at noen tar med seg gamle PCer etter at de er erstattet med nye, noe som ikke skal skje. Kommunen prøver å samle inn gamle PCer ved utskifting. Seniorkonsulenten forteller at kommunen ikke har noen policy på utskifting av PCer. Utskifting skjer når en PCen ikke kan levere kurant ytelse og kjøre siste utgave av Microsoft sine systemer. IT-leder forteller at IT har en egen plan for utskifting av utstyr med rullering hvert femte år. Det ble gjennomført en større utskiftning i 2020 og når det skal skje en rullering i 2025 vil sky-baserte løsninger i større grad være tatt i bruk slik at behovet for lokale lagringsløsninger vil være mindre.

Kommunen har en del teknisk utstyr som står ute i det tekniske nettet, hvor kommunen har mindre kontroll. Disse står i en egen sone innenfor brannmuren, forteller seniorkonsulent-IT.

Det er ingen kontroll eller styring på andre enheter koblet til nettverket enn kommunenes PCer, forteller driftssjef-IT. Dette kan være alarmer, dørlåser, ovner, kamera, sensorer og lignende. IT-avdelingen har startet utprøving av en løsning for sårbarhetsskanning, som aktivt vil søke på alle kommunens nettverk etter utstyr, rapportere funn og kjøre sårbarhetsskanning av disse. Seniorkonsulent-IT er involvert i konfigurasjonen av enheter. Det er IT-enheten som konfigurerer det meste, med unntak av utstyr som står i teknisk sone. Utstyr i teknisk sone er det ofte leverandører som konfigurerer.

Kommunen har god kontroll på skrivere, forteller driftssjef-IT. Skriverne har ikke kontakt via internett, men er kun på et eget skjermet nettverk. Det er noen printere utenfor det interne nettverket, for eksempel på oppvekst slik at elever skal ha muligheten til å skrive ut.

Det er veldig få PCer uten fast bruker, da dette ikke er i tråd med sikkerhetspolicyen, forteller driftssjef-IT. 110-sentralen har en egen PC uten fast bruker. Det skal legges opp til at de ansatte logger på med sin egen bruker.

Seniorkonsulent-IT føler ikke at kommunen er spesielt dårlig på avinstallering av programvare, som de ikke lenger bruker. Kommunen har god kontroll med hvilken programvare ansatte får lov til å kjøre.

4.3.3 Sikker IKT-arkitektur

Av informasjonssikkerhetsinstruksen går det fram at soner brukes som et grunnleggende prinsipp i sikkerhetsarkitekturen. På sikker sone finnes sensitive personopplysninger. Den enkelte sikre sone er teknisk adskilt fra resten av internt og eksternt nettverk samt eventuelt andre sikre soner. Ikke-sensitive personopplysninger behandles i åpen sone.

Informasjonssikkerhetsinstruksen sier at alle installasjoner, endringer og lignende knyttet til IKT-systemer skal dokumenteres og det skal føres en endringslogg. Installasjoner skal evalueres i forhold til enhver tid gjeldende sikkerhetsbestemmelser.

I oppstartsmøtet fortelles det at kommunen ikke har laget et komplett konfigurasjonskart, men at det er laget en delvis beskrivelse. Et konfigurasjonskart står på listen over hva som skal utarbeides og det skal inngå i kvalitetssystemet.

Driftssjef-IT forteller at det ikke er utarbeidet et sikkerhetskart (konfigurasjonskart) på overordnet nivå, men det finnes muligens innenfor enkelte områder. Driftssjefen har en oversikt over nettverket i hodet. Dette er noe som etterspørres i NIST CSF, slik at dette vil komme på plass.

Det er ikke utarbeidet en total konfigurasjonskart, men kommunen har noen deler her og der, forteller seniorkonsulent-IT. Et totalt konfigurasjonskart bør bli laget, noe som kommer til å resultere i et stort og komplekst kart. Det er flere ansatte på IT-avdelingen, som må være med på å tegne dette kartet. Seniorkonsulenten har ganske god kjennskap til hvordan ting henger sammen.

IT-konsulenten forteller at ytterligere segmentering av datasystemet er en av anbefalingen i den gjennomførte penetrasjonstesten, jfr. kapittel 4.4.3.

4.3.4 Behandlingsoversikt

Lov om personopplysninger krever at kommunen som behandlingsansvarlig for person-opplysninger har en oppdatert behandlingsprotokoll eller behandlingsoversikt for person-opplysninger. Det er ingen formkrav til behandlingsoversikten.

I oppstartsmøtet fortelles det at kommunen har en oversikt over behandling av person-opplysninger samt databehandleravtaler. Det er mange systemer og arbeidet med å få oversikt startet før kommunesammenslåingen. Namsos kommune sitt eksisterende kvalitetssystem

inneholder en oversikt over hvilke dataprogram og applikasjoner kommunen har, med tilhørende opplysninger. Revisor har fått en systemoversikt for Namsos kommune med 80 systemer. Det er uklart for revisor om det er samsvar mellom denne oversikten og det som ligger i dataprogrammet. Revisor har ikke kontrollert om det finnes andre programmer som ikke er registrert.

Driftssjef-IT forteller at IT ikke har en fullstendig oversikt over programvaren som brukes i kommunen, men de har god kontroll på programvaren som er i bruk. Det er innført en sikkerhetsfunksjon kalt AppLocker fra Microsoft, slik at all programvare må godkjennes før den kan kjøre. Kommunen har valgt å stole på all programvare fra Microsoft og det lages regler for programvare IT kjenner til. Programvare som ikke er godkjent eller ukjent for IT, vil dermed ikke kunne kjøre. I kvalitetssystemet er det laget en oversikt over fagprogrammer og programeiere.

I årsmeldingen fra personvernombudet i Namsos kommune står det at personvernombudet kan ha oppgaven med å samle inn informasjon for å identifisere behandlingsaktiviteter og analysere og sjekke at de er i tråd med regelverket. Personvernombudet informerer i en epost at vedkommende vil bli involvert i dette arbeidet når oppdateringer starter opp, men at oversikten ikke er oppdatert per april 2022.

Personvernombudet forteller at det brukes en modul i kvalitetssystemet som heter *avtaler*, for å ha oversikt over antall systemer og hvem som har ansvaret for systemene, databehandler-avtaler, ansvar etter GDPR og lignende informasjon. Hjemmel for behandling av person-opplysninger er lagt inn for noen programmer. Personvernombudet oppdaterer informasjonen, men har ikke tilstrekkelig tid til å gjøre dette. Dette ansvaret burde vært fordelt. Ved overgangen til nytt kvalitetssystem vil denne modulen i det gamle kvalitetssystemet bli beholdt. Personvernombudet mener at kommunen klarer å ivareta behandlingsansvaret.

På kommunens hjemmeside (under personvern og informasjonskapsler) går det fram at kommunen har en rutine som skal gi nødvendig sikkerhet for at alle personopplysninger er tilstrekkelig sikret. Videre står det at kommunedirektøren er behandlingsansvarlig for personopplysningene og har delegert behandlingsansvaret til assisterende kommunedirektør som har delegert det videre til kommunalsjefene. I kommunens delegasjonsreglement på hjemmesiden (sist endre 09.11.2021) går ikke denne delegasjonen fram. Her er det videredelegert til kommunalsjef for oppvekst og opplæring, videre til leder barnehage og leder grunnskole, og videre derfra ut til barnehagestyrer og rektor.

4.3.5 Beskyttelse av data

På dokumentsenteret kontrolleres alle saker og journalposter hver dag, forteller konsulenten. Det passes på at unntatt offentlighet er markert og at skjerming av navn er riktig. I tillegg kontrolleres tilgang. Konsulenten mener at kulturen knyttet til skjerming er god. Det skjermes mer enn det egentlig er behov for. Særlig gjelder det personalsaker.

Konsulenten forteller videre at dokumentsenteret mottar, men behandler ikke innsynskrav. Det er den enkelte saksbehandler som må behandle innsynskravet. Det er bare postlisten som legges ut automatisk, mens konkrete dokumenter må etterspørres.

Ved dokumentsenteret har de ikke jobbet spesielt med sikkerhetstiltak, forteller konsulenten. Noen ganger melder konsulenten avvik når saksbehandlere ikke gjør ting riktig. Dokumentsenteret har fått beskjed om å være ekstra påpasselig som følge av krigen i Ukraina. Dokumentsenteret får alle inngående eposter og er oppmerksom på om det er noe skummelt. Hvis de er usikre så kontakter de IT, forteller konsulenten.

Driftssjef-IT forteller at det brukes et system som gjør at skriverjobbene ikke blir liggende i bunker ute på skriverne. Brukerne må gå til skriveren og dra et nøkkelkort for at utskriftsjobben skal komme ut.

ePhorte

Konsulenten ved dokumentsenteret forteller at ved overgang til nytt saksbehandlingssystem blir det en gjennomgang av tilgangene i saksbehandlingssystemet.

Konsulenten ved dokumentsenteret forteller at når det opprettes en sak, kan det legges til en fast tilgangsgruppe der alle som er medlemmer i gruppen har tilgang til saken. Det er også mulig å legge på en ad-hoc tilgangsgruppe, hvor det defineres konkret hvilke personer som skal ha tilgang til saken. Konsulenten er usikker på om tilgangsgrupper skal videreføres i det nye saksbehandlingssystemet. Konsulenten oppfatter at en del ansatte får unødvendige tilganger når det brukes tilgangsgrupper. Tilgangsstyringen er veldig streng for personsensitive saker og barnevernssaker, og her er det egne retningslinjer, men disse er ikke dokumentert. Praksisen er slik at hvis noen etterspør tilgang til personsensitive saker så henvises de til kommunalsjefen på området. Konsulenten kjenner ikke til om det er egne retningslinjer for tilganger ut over dette.

Dokumentsenteret må få beskjed når ansatte slutter, slik at det kan legges inn sluttdato for den enkelte bruker. Dette skjer ikke alltid. Konsulenten forteller at de aldri har fått beskjed om at ansatte skal ut av noen tilgangsgrupper. Hvis noen i en tilgangsgruppe slutter mister de tilgangen til gruppen når de mister tilgangen til saksbehandlingssystemet.

4.3.6 Rutiner for sikkerhetsoppdateringer

Godt nok-prinsippet legger opp til at små endringer innføres kontinuerlig i tråd med brukerens og virksomhetens ønsker, når nye systemer utvikles. Dette medfører at systemet ikke nødvendigvis blir *100 prosent* sikkert (men sikkert nok), og samtidig gir nødvendig fleksibilitet for å kunne drive virksomheten fremover i tråd med forventninger og samfunnsendringer. (Finstad og Mushtaq, 2021)

Driftssjef-IT forteller at kommunen har tatt i bruk et program, som brukes til oppdatering og installering av programvare og operativsystem på PCer, kalt Heimdal. Programmet gjør det også mulig å sjekke hva som kjøres på hver enkelt maskin og i noen tilfeller fjerne programvare. Det er ikke klare rutiner for å avinstallere programvare som ikke er i bruk, forteller driftssjef-IT.

Informasjonssikkerhetsutvalget har hatt en sak om at vedlikeholdet av saksbehandlingssystemet ePhorte avsluttes, noe som gjør det betydelig enklere for skadevare å finne inngangsveier til systemet. Nytt saksbehandlingssystem skal tas i bruk i kommunen i 2022.

Seniorkonsulent-IT forteller at kommunen har kjøpt inn et par gode overvåkningssystemer de siste årene. De satser på klare å oppdage ting tidlig. Kommunen får råd og informasjon om konkrete trusler og sårbarheter fra Atea og HelseCERT. Ved kritiske svakheter oppdateres programmer så raskt som mulig, innenfor de nødvendige hensyn til brukernes behov. Seniorkonsulent-IT forteller at utstyret som blir brukt daglig blir oppdatert.

4.3.7 Sikkerhetskopier

Informasjonssikkerhetsinstruksen gir regler for sikkerhetskopiering for de ansatte. Det omfatter at jobbrelatert informasjon lagres på servere i kommunens nett slik at det blir tatt sikkerhetskopier. Ved arbeid utenfor kontoret må det regelmessig gjøres oppdateringer mot servere i nettet, spesielt hvis andre er avhengig av informasjonen. IKT-enheten kan kontaktes ved behov for gjenoppretting av sikkerhetskopiert informasjon. Gjenoppretting omtales nærmere i kapittel 4.5.3.

IT-konsulenten forteller at kommunen har systemer for sikkerhetskopiering internt og til skylagring. Alt blir sikkerhetskopiert og det blir oppbevart sikkerhetskopier for flere generasjoner tilbake. Flere generasjoner lagres fordi det kan være latent skadevare i noen av sikkerhetskopiene. Kommunen har gått over til å bruke skysystemer til backup. Kommunen undersøker nye løsninger for sikkerhetskopiering nå. Det er gjennomført tester med å hente inn dokumenter fra backup-løsningene, samt at IT må bistå i å hente fram backup når brukere mister dokumenter.

Kommunen har sikkerhetskopiering via skytjenester, forteller driftssjef-IT. De viktigste systemene har også en ekstra backup, som ligger i Stockholm. Dette er systemer som bruker *imutable storage*, noe som vil si at informasjonen ikke kan endres eller slettes før det har gått en viss tid (30 dager er valgt). All data blir kryptert både i transitt og hvilende. Krypteringsnøklene lagres i et eget internt system med tofaktorautentisering. Seniorkonsulenten forteller at risikoen spres ved å ha forskjellige løsninger for sikkerhetskopiering. Det kan ligge latent skadevare i backup og derfor er det viktig å ha en serie med backup fra ulike tidspunkter.

4.3.8 Vurdering

Namsos kommunen har en god oversikt over enheter som er i bruk, men det er uklart om den er komplett.

Kommunen har god oversikt over det aller meste av enheter som er koblet på kommunens IT-system, men kan ikke utelukke at det kobles på enheter som de ikke har kontroll på. Kommunen bruker Microsoft Insight for å administrere PCer. Kommunen har startet utprøving av sårbarhetsskanning som kan identifisere ukjente enheter. Kommunen har også en utfordring med at det alltid ikke følges opp at datautstyr blir innlevert når noen slutter. Etter revisors vurdering vil denne løsningen bedre kontrollen med enheter som bruker datasystemet.

Revisor vurderer at Namsos kommunen har etablert en sikker IKT-arkitektur, men at det er knyttet noen svakheter til den.

Namsos kommune har bygd opp en IKT-arkitektur hvor ulike sikkerhetstiltak er innebygd. IKT-arkitekturen har etter revisors vurdering noen svakheter med at den er delt med flere kommuner, noe som gjør at et angrep i en kommune kan spre seg til andre kommune. Det er også en svakhet at det ikke finnes noen skisse over IKT-arkitekturen slik at alle som jobber med IT-systemene har et felles visuelt bilde av sammenhengene. Nettverket er beskyttet gjennom ulike sikkerhetstiltak. Data er også beskyttet gjennom sikkerhetstiltak i nettverket og gjennom styring av blant annet tilganger.

Namsos kommunen har ikke en oppdatert behandlingsoversikt.

Namsos kommune har en oversikt over programvare som brukes i kommunen med mange av de opplysningene en behandlingsoversikt krever. Revisor oppfatter at oversikten ikke er oppdatert og det er usikkert om den inneholder alle behandlinger av personopplysninger. Det er personopplysningsloven som stiller krav om å ha en oversikt over alle behandlinger av personopplysninger. Det finnes ingen mal for hvordan denne oversikten skal se ut. En

alternativ tilnærming til å lage oversikten er at hvert virksomhetsområde gjennomgår de områdene hvor de behandler personopplysninger, i stedet for å se hvilke dataprogram som behandler personopplysninger. Det kan da være enklere å knytte behandlingen til hjemmelen for behandling av personopplysninger og kommunen kan fange opp personopplysninger som ikke behandles i digitale arkiver.

Namsos kommune beskytter virksomhetens data gjennom ulike forebyggende tiltak, men manglende oversikt over tilganger og bruk av tilgangsgrupper gjør at flere enn de som trenger det kan få tilgang til personopplysninger.

Revisor har også undersøkt tilgangen til sak- og arkivsystemet. Her gis det tilganger til grupper. Etter revisors oppfatning kan slike gruppetilganger føre til at flere enn de som trenger det får tilgang til personopplysninger. Spesielt ettersom det ikke gjøres noen vurderinger av hvem som til enhver tid er i den enkelte gruppe. I tillegg er det mange grupper, noe som antas å være krevende å holde oversikt over og holde oppdatert. Revisor har ikke undersøkt den fysiske sikringen.

Namsos kommunen har en praksis med sentral styring med sikkerhetsoppdateringer

IT-avdelingen gjennomfører sikkerhetsoppdateringer og basert på alvorlighetsgrad kan de iverksettes umiddelbart eller senere når bruken av systemene er minimal. Kommunen har et nettverk av leverandører og andre som gjør at de raskt får informasjon om behovet for oppdateringer. Revisor har ikke sett skriftlig rutine på sikkerhetsoppdateringer.

Namsos kommunen har praksis for sikkerhetskopiering.

Revisor vurderer at Namsos kommune har ulike systemer for sikkerhetskopiering slik at risikoen er spredt. Det finnes også flere generasjoner sikkerhetskopier og det gjøres jevnlig gjenopprettinger for ansatte og egne gjenopprettinger for å teste sikkerhetskopiene. Revisor har ikke sett skriftlig rutine på sikkerhetskopiering.

4.4 Oppdagende

4.4.1 Revisjonskriterier

- Kommunen bør ha et system for å overvåke sikkerheten og analysere data fra overvåkningen
- Kommunen bør ha et system for å oppdage og fjerne kjente sårbarheter (automatisert og sentralisert verktøy eks antivirus, loggføring og sikkerhetsovervåkning)
- Kommunen bør gjennomføre sikkerhetstester

4.4.2 System for overvåkning

Sikkerhetsinstruksen for medarbeidere skal sikre at ledere med personalansvar ivaretar personvern og informasjonssikkerhet ved enheten. I sikkerhetsinstruksen for medarbeidere går det fram at arbeidsgiver har rett til innsyn i arbeidstakers e-postkasse og personlige filområder ved begrunnet mistanke om grovt pliktbrudd eller når det er påkrevet av hensyn til drift av systemet. Arbeidsgiver har anledning til å logge informasjon om internett og e-posttrafikk for å sikre alminnelig drift, samt for sporing ved sikkerhetsbrudd.

I utkast til årsmelding for 2021 for Namsos kommune går det fram at kommunen har anskaffet datasikkerhetsprogrammet SIEM (Security Information and Event Management), som samler logger fra servere, nettverk, påloggingsinformasjon, brannmur og programvare. Programmet analyserer loggene for å avdekke avvik og hendelser knyttet til IT-sikkerhet. Alle systemer som involverer overvåkning medfører en del ekstraarbeid ettersom det generes mange meldinger som må gjennomgås, inkludert såkalte falske positive. Systemene må finjusteres for å kunne fungere optimalt, blant annet i forhold til nye trusler og for å hindre at IT får mange unødvendige meldinger.

Overvåkningssystemene håndteres av IT og er sentralisert, forteller driftssjef-IT. Overvåkningen er delvis automatisert. Det betyr at det er laget arbeidsflyter eksempelvis på antivirus. Det er to agenter som følger med – Windows defender (antivirus) og SIEM – Insight. I Insight blir varsel i kategorien høy satt direkte i karantene, mens varsel i kategori middels går til IT for vurdering. Defender lager sammendrag og ved nærmere undersøkelse må noen gå manuelt inn i loggene. Det leses ikke logger uten at det er indikasjoner på noe.

Utprøving av sårbarhetsskanning, som aktivt søker på alle kommunens nettverk etter utstyr, rapportere funn og kjøre sårbarhetsskanning av disse, er en del av overvåkningen forteller driftssjef-IT.

4.4.3 System for å oppdage og fjerne sårbarheter

Informasjonssikkerhetsinstruksen sier at alle feil eller mistanker om feil i informasjonssystemer skal rapporteres til IKT-enheten snarest mulig.

Kommunen har også systemer for å se etter annen unormal trafikk, forteller driftssjef-IT. Nivået på alarmer er satt opp av leverandøren av systemet. Det aktiveres automatiske sikkerhets-varsel når terskler brytes. IT-avdelingen har også satt opp programmatiske arbeidsflyter, som for eksempel automatisk vil isolere en PC fra de andre maskinene i nettverket, dersom en alvorlig sikkerhetstrussel oppdages. Disse systemene fungerer bra.

Kommunen har tatt i bruk et system for å sjekke om passord som brukes er blitt hacket, sier driftssjef-IT. Det stilles ikke krav om jevnlig bytte av passord, men kommunen har retningslinjer for passordbruk.

Alle på IT er mer fokusert på sikkerhet enn tidligere, forteller driftssjef-IT. Driftssjefen har kjørt et kurs i hacking av systemer for de andre på IT. I den forbindelse er det laget et eget nettverksmiljø utenfor kommunens nettverk. På dette nettverket er det egne virtuelle maskiner til hver enkelt medarbeider og utplassert servere med forskjellige sårbarheter. Formålet er at de ansatte på IT skal kunne teste gjennomførelse av angrep og prøve ut programvare og metodikk som finnes til dette formålet uten å være redd for å infisere eller angripe de kommunale nettverkene. Dette vil gjøre det enklere å gjenkjenne slike angrep når ansatte senere ser dem i logger eller i aktivitet på PCer eller servere.

4.4.4 Sikkerhetstester

I oppstartsmøtet fortelles det at kommunen har bestilt en penetrasjonstest og det henvises til at nasjonal sikkerhetsmyndighet har anbefalt at dette gjøres en til to ganger i året. Kommunen har leid inn et selskap til å utføre penetrasjonstester i kommunen og foreløpige anbefalinger er ytterligere segmentering av datasystemet.

Sikkerhetstesten er gjennomført av et eksternt selskap våren 2022. Resultatene fra testen er presentert i informasjonssikkerhetsutvalget.

Driftssjef-IT forteller at kommunen fikk skryt for mange bra tiltak, eksempelvis AppLocker som gjorde det vanskelig å komme videre. I testen ble en maskin satt i nettet og tester opplevde å få et godt overblikk over nettet. Det jobbes nå med å stoppe denne muligheten, som skyldes at nettverket er ikke segmentert godt nok.

4.4.5 Vurdering

Namsos kommune har et system, SIEM (Security Information and Event Management), for å overvåke sikkerheten og analysere data fra overvåkningen.

Revisor finner at kommunen har et overvåkningssystem som henter data fra antivirusprogram, nettverk, brannmur og lignende. I overvåkningen er det innebygd analyser av arbeidsflyten og det er mulig å sette terskelverdier for når verdiene overskrider akseptabelt nivå.

Namsos kommune har et system for å oppdage og fjerne kjente sårbarheter

Kommunens overvåkningssystem er koblet sammen med systemer som oppdager og som stopper eksempelvis nettverkstrafikk hvis data fra overvåkningen overskrider terskelverdier. I tillegg leses det logger ved mistanke om trusler eller feil. Sårbarheter i programvare varsles vanligvis av leverandører og det kommer da sikkerhetsoppdateringer, jfr. kapittel 4.3.6.

Namsos kommune har gjennomført inntrengningstest våren 2022.

Revisor finner at Namsos kommune har gjennomført en penetrasjonstest våren 2022. Ansatte på IT har også et eget miljø hvor de kan prøve og feile for å lære om sikkerhet.

4.5 Korrigerende tiltak

4.5.1 Revisjonskriterier

- Kommunen bør ha en plan for hendelseshåndtering (ansvar, tiltak, kommunikasjon, gjenopprettingsplan og loggføring)
- Kommunen må ha en plan for gjenoppretting
- Kommunen må ha en beredskapsplan som omfatter IKT-hendelser

4.5.2 Plan for hendelseshåndtering

I informasjonssikkerhetsinstruksen går det fram at det er bare kommunedirektøren eller den som får oppgaven delegert som har myndighet til å uttale seg offentlig i forbindelse med saker som gjelder IT-sikkerhet, sikkerhetsbrudd eller større hendelser.

Informasjonssikkerhetsinstruksen inneholder informasjon om avvik og sikkerhetsbrudd. Avviksbehandlingen skjer i kvalitetssystemet. Alle avvik som skyldes brudd på datasikkerhet, skal meldes til Datatilsynet. Kommunedirektøren har ansvaret og kan melde avvik. I tillegg har

kommunalsjefer og personvernombudet tilgang til å melde avvik til Datatilsynet. Avvik til Datatilsynet har en egen rutinebeskrivelse, nærmere beskrevet som brudd på person-opplysningssikkerheten. Her går det fram at avvik skal meldes når det er brudd på person-opplysningssikkerheten og at det er sannsynlig at bruddet vil medføre en risiko for den registrerte sine rettigheter og friheter

Driftssjef-IT varsler de ansatte via Teams dersom noe skjer, og har også mulighet til å sende SMS ved behov. Det er laget en rutine som skal brukes ved ransomware-angrep[15]. Ved et eventuelt angrep, skal kommunens systemer fysisk fjernes fra nettet, ved at visse switcher skal skrues av eller kobles fra. Ansatte på IT-tjenesten vet hva som skal gjøres i slike tilfeller og det er etablert en vaktliste i forhold til dette, forteller driftssjef-IT.

Så lenge det er mulig å kontakte systemene via hjemmekontor, noe det vanligvis er, vil vakta kunne stenge tilgang til internett, men dette krever kompetanse på utstyret. Det samme gjelder ikke når det kan løses med å dra ut en kabel.

Det er laget en plan for hva IT skal gjøre hvis det skjer et angrep, forteller driftssjef-IT. En foliert kopi av denne ligger på pauserommet og et eksemplar ligger på kontoret til driftssjefen. Det viktigste er å få på plass nye systemer. Det vil kanskje også være behov for hjelp til å legge tilbake informasjon fra back-up systemene. Seniorkonsulent-IT trekker også fram denne planen som blant annet har en oppskrift på hvilke systemer og hvilket utstyr som skal skrus av.

Driftssjef-IT forteller at han har startet på en gjenopprettingsplan, men er ikke i mål med denne og ønsker innspill fra andre avdelinger. De andre avdelingene er informert om at de må kunne fungere uten tilgang til data, blant annet ved å ha nødvendig informasjon skrevet ut.

Konsulenten ved dokumentsenteret forteller at hvis det skjer er angrep må de føre manuell journal. Konsulenten har ingen spesiell beredskapsrolle. All informasjonen ligger nå i det digitale arkivet som kommunen kanskje ikke får tilgang til.

4.5.3 Plan for gjenoppretting

Driftssjef-IT har startet på en gjenopprettingsplan, og vil gjerne ha innspill fra andre avdelinger. De andre avdelingene er informert om at de må kunne fungere uten tilgang til data, blant annet ved å ha nødvendig informasjon skrevet ut.

[15] Ransomware – er på norsk omtalt som løsepengevirus, utpressingsprogramvare eller gisselvare. Det er skadelig programvare (datavirus) som krypterer hele eller deler av innholdet i en infisert datamaskin slik at den blir utilgjengelig for brukeren, for så å be om løsepenger.

Driftssjef-IT har gjort en test i forbindelse med gjenoppretting, når det gjelder den lokale lagringen av systemer. Ved store angrep vil IT måtte gjenopprette hele systemet og tilbakeføre data. Maskinvaren vil ikke bli rammet i et slik angrep.

Driftssjef-IT forteller at det i handlingsplan for ransomware-angrep, som skiller mellom ulike angrepsnivå, fra at en PC blir angrepet til at mange servere og PCer er angrepet. Estimert forløp for gjenoppbygging etter et totalangrep er seks uker, ifølge handlingsplanen. Kommunen har gjort en kartlegging av verdier som rammes ved et ransomware-angrep. Kartleggingen er knyttet til de enkelte fagsystemer og hva som blir rammet ved et eventuelt angrep. I handlingsplanen går det fram at det finnes tiltaksplaner og om de er på plass. En del av tiltaksplanen er å ha papirbaserte utskrifter av verdifull informasjon.

Planen for gjenoppretting er mindre konkret enn planen for hendelseshåndtering, forteller seniorkonsulent-IT. I slike tilfelles må kommunen gjenopprette ting fra backup, så lenge denne er sikker.

Konsulenten ved dokumentsenteret forteller at det ikke er diskutert om det er visse ting som dokumentsenteret burde ha skrevet ut på papir og konsulenten har ikke tenkt over om de har noen dokumenter som burde vært på papir, i tilfellet de mister tilgangen til datasystemet.

4.5.4 Beredskapsplan for IKT-hendelser

Namsos kommune har en beredskapsplan som ble vedtatt 14.11.2019 gjeldende for den nye kommunen, hvor informasjonssikkerhet er tema. I oppstartsmøtet fortelles det at det ble gjort en risiko- og sårbarhetsanalyse i den forbindelse. I beredskapsplanen beskrives alternative kommunikasjonsmidler ved hendelse som utfall av elektronisk kommunikasjon. Det er også laget et tiltakskort for denne typen hendelser. I oppstartsmøtet fortelles det at kommunen har en beredskapsplan for hva som må gjøres hvis kommunen utsettes for et dataangrep, handlingsplan for ransomware-angrep. Kommunen har gjort noen grep for å redusere risikoen ved å lagre data i ulike skyløsninger. Videre er det laget en prioritering over hvilke tjenester det er viktig å gjenopprette først.

I 2022 er det innført en beredskapsordning for å sikre bemanning som kan håndtere virksomhetskritiske avvik etter normal arbeidstid. Det går fram at høyere fokus på sikkerhet har ført til økt arbeidsmengde på IKT-området og digitalisering innen helse. IT-konsulenten forteller at det er definert hva som er kritisk, slik at brukere ikke kan kontakte beredskapsvakten om hva som helst. Noen av de ansatte på IT bemanner denne beredskapsvakten. Driftssjef-IT forteller at det er opp til den enkelte å vurdere om henvendelsen er kritisk nok til å løses av beredskapsvakta. Eksempelvis vil det være kritisk hvis mange blir berørt. Det er ikke satt krav til utrykningstid i denne vaktordningen, men så lenge vaktordningen er basert på sovende vakt

kan det by på utfordringer. Kommunalsjef personal og organisasjon informerer om at det i interne retningslinjer for beredskap er satt krav til utrykningstid serverrom.

4.5.5 Vurdering

Revisor vurderer at Namsos kommune har en plan for hendelseshåndtering.

Det finnes en plan for hvordan kommunens datasystem skal stenges ned ved et eventuelt angrep. Videre er det en rutine for å melde avvik til Datatilsynet.

Revisor vurderer at Namsos kommune har en plan for gjenoppretting.

Kommunen har en plan for gjenoppretting etter ransomeware-angrep. Revisor er usikker på hvor dekkende denne planen er for ulike typer hendelse som kan oppstå.

Revisor vurderer at Namsos kommune har en beredskapsplan for ransomware-angrep og en aksjonsplan for IT hvis det skjer et angrep, men mangler en mer helhetlig beredskapsplan for kommunen.

Kommunens handlingsplan for ransomware-angrep omhandler en type angrep og kan bli for spesifikk knyttet til en type hendelse. Handlingsplanen er en plan for IT sitt arbeid med gjenoppretting og sier lite om utfordringer i andre deler av kommuneorganisasjonen. Risikovurderinger som omtalt i kapittel 4.1.3 bør ligger til grunn for en beredskapsplan for hele kommuneorganisasjonen som tar innover seg at tilgangene til datasystemene kan bli borte for en lengre periode.

5 INFORMASJONSSIKKERHET I OVERGANGEN TIL NY KOMMUNE

5.1 Problemstilling

Det er utarbeidet følgende problemstilling om overgangen til ny kommune:

- Hvordan har kommunen sikret integritet, konfidensialitet og tilgjengelighet for informasjon fra de gamle kommunene?

I oppstartsmøtet med kommunen kommer det fram at overgangen til ny kommune ikke medførte store endringer siden samarbeidet på IT allerede var på plass. Det var lite problemer knyttet til IT ved sammenslåingen av kommunene. Revisor valgt da å lage en beskrivende besvarelse på denne problemstillingen, fordi det er historie og lite aktuelt for revisjon.

5.2 IT-samarbeid

5.2.1 Oppstart og samkommune

Namsos kommune har siden 2004 samarbeidet med nabokommunene om IT. Da samkommunen, med Namsos, Overhalla og Namdalseid ble etablert, ble IT en del av samkommunen. Fosnes, Flatanger og Høylandet kommune hadde et samarbeid med IT i samkommunen. Samkommunen ble avviklet i 2019 og avløst av kommunesammenslåingen mellom Namsos, Namdalseid og Fosnes ble iverksatt fra 2020.

I *Handlingsprogram med økonomiplan 2019 og årsbudsjett 2019*, sak 72/2018 i Namsos kommunestyre (13.12.2018) går det fram at IT-avdelingen har betydelige utfordringer i forhold til den pågående prosessen med avvikling av Midtre Namdal samkommune og etablering av Nye Namsos kommune. Det går videre fram at gjeldende IKT-strategi skulle vært rullert i 2016. Det er behov for at det utarbeides en ny IKT-strategi i forbindelse med etableringen av Nye Namsos og som kan være felles for alle kommunene, som fortsatt skal ha samdrift om IKT-infrastruktur. Revisor har ikke funnet at det er laget noen IKT-strategi etter kommune-sammenslåinga.

5.2.2 Sammenslåingsprosessen

I *Handlingsprogram med økonomiplan 2020-2022 for Nye Namsos*, beskrives arbeidet med avvikling av IT-samarbeidet i Midtre Namdal samkommune og utvikling av nytt vertskommune-samarbeid fra 2020, som en av de sentrale utfordringene for personal og organisasjons-området.

I *Handlingsprogram og budsjett 2019 for Midtre Namdal samkommune* (MNS), går det fram at det er etablert egne prosjektgrupper for avvikling av MNS og etablering av Nye Namsos. Ansatte i IT i MNS deltar i begge gruppene i tillegg til flere prosjektgrupper. IT MNS har i samarbeid med leverandør av kvalitetssystemet etablert et avtaleregister som skal gi oversikt over alle systemer og programmer som brukes av organisasjonen og avhengigheten mellom disse. Dette registeret vil danne utgangspunkt for kommunenes oversikt over registreringer av personopplysninger som er nødvendig for å ivareta den nye personvernforordningen. (omtalt i kapittel 4.3.3) Arbeidet med å fylle inn informasjon om det enkelte program/register er startet og det er en utfordring å få gjennomført dette arbeidet og gjennomføre risikoanalyser for hvert register. Rådmannsgruppen i MNS kommunene har besluttet at alle ansatte skal være på skybasert løsning med Office365.

I sluttrapporten fra kommunesammenslåingen, *Sluttrapport styringsdokument*, går det fram at økonomi og IKT utgjorde en arbeidsgruppe. Følgende handlingspunkter framgår:

- Kartlegging og vurdering av systemer og avtaler
- Gjennomføre forhandlinger
- Gjennomføre anbudskonkurranser
- Digitale konsekvenser av kommunesammenslåingen
- Forberede budsjett og langtidsbudsjett, regnskap og årsberetning
- Strategi for IKT og digitalisering

Flere av ansatte på IT som revisor intervjuet deltok i arbeidsgrupper.

IT-avdelingen var ikke mye involvert i forbindelse med kommunesammenslåingen. Stort sett fikk de bare beskjed om hvilke tiltak som skulle gjennomføres. Driftssjefen kan ikke huske at det ble laget noen plan eller risikovurdering før kommunesammenslåingen.

Seniorkonsulent-IT hadde en sentral rolle i forbindelse med kommunesammenslåingen, og forteller at det var etablert en egen arbeidsgruppe på IT, i tillegg til arbeidsgrupper på andre fagområder. Selve sammenslåingen var en lite omfattende prosess IT-teknisk, siden kommunene hadde et felles driftssenter og felles fagsystemer fra før. Arbeidet gikk mer ut på sammenslåing av forskjellige databaser ettersom de nå ble en felles juridisk enhet. Dette var like mye en jobb for de ulike fagmiljøene som for IT. Det ble gjort noen risikovurderinger, men risikoen var ikke stor IT-teknisk, siden de var så samkjørt fra før. Mest utfordrende var det at ulike fagsystemer skulle slås sammen, eksempelvis helsesystemer, lønn/personal, matrikkel/ kart og saksbehandlingssystem. Dette ansvaret var delt mellom IT og de ulike fagområdene, og en vesentlig del ble utført av systemeier av fagsystemene. Seniorkonsulenten forteller at

det var spenning knyttet til blant annet sammenslåingen av matrikkelen og den første lønnskjøringen. Det var ingen store endringer knyttet til den tekniske infrastrukturen.

5.2.3 IT-samarbeid etter kommunesammenslåingen

Etter kommunesammenslåingen driftes IKT infrastrukturen felles i Namsos, Overhalla og Flatanger, med Namsos som vertskommune og vertskommuneavtaler med Overhalla og Flatanger. Sammen med vertskommuneavtalene ble det laget egne leveranseavtaler, forteller IT-leder. Vertskommuneavtalene er signert våren 2019. Det framgår av leveranseavtalen at vertskommunen har ansvaret for organisering av felles IKT-oppgaver, infrastruktur og programvare som inntil 01.01.2020 var Midtre Namdal samkommune sitt ansvarsområde. Det framgår av samarbeidsavtalen at det er utarbeidet egne databehandleravtaler mellom vertskommunen og den enkelte samarbeidskommune. Sikkerhetsløsninger og sikkerhetstiltak for fysiske installasjoner omfattes av IKT-infrastruktur samt felles programvare.

Seniorkonsulenten forteller at samarbeidet var bedre under samkommunen. Nå er det en tendens til at kommunene kjører sololøp når det gjelder anskaffelser, slik at de ender opp med forskjellige fagsystemer i de forskjellige kommunene. I samkommunen tok de mer hensyn til hverandre, beslutningene ble tatt i fellesskap og de endte opp med ett fagsystem for alle kommunene.

IT-leder deler oppfatningen av at det var mer samarbeid mellom kommunene i samkommunen. Overgangen til vertskommune har medført at samarbeidet har knirket. Nå er det flere tilfeller hvor kommunene på egen hånd kjøper inn systemer, noe som medfører problem og merarbeid knyttet til integrering. For eksempel er det kjøpt inn forskjellige systemer for forvaltning av eiendommer. IT-leder mener at kommunen ikke klarte å ta med seg de gode relasjonene fra samkommunen inn i den nye samarbeidsformen. Leveranseavtalene som ble utarbeidet som en del av vertskommuneavtalene, er ikke fulgt opp på alle områder og de bør revideres. I tillegg har det skjedd mye knyttet til datasikkerhet siden avtalene ble inngått.

5.3 Teknisk overgang

Generelt ble alle rettigheter og plikter overført til ny kommune fra 01.01.2020 med det opprinnelige innhold og omfang, står det i sluttrapporten fra kommunesammenslåingen, *Sluttrapport styringsdokument*. Det må gjøres en ryddejobb i avtalene etter 01.01.2020. Det ble inngått avtaler med en rekke sentrale systemleverandører for å sikre konverteringen av systemene til ny kommune. Det er etablert et digitaliseringsråd som skal samordne og sørge for tverrfaglig drøfting av digitale anskaffelser. Digitaliseringsrådet arbeider med en digitaliseringsstrategi som planlegges ferdigstilt i løpet av våren 2020. Det er etablert et datasikkerhetsutvalg for å ivareta fokus på datasikkerhet, rutiner, vurderinger av risiko,

personvern mm. Revisor forstår det slik at datasikkerhetsutvalget er det som i dag benevnes som informasjonssikkerhetsutvalg. Det er uklart om digitaliseringsrådet eksisterer.

Konsulenten ved dokumentsenteret forteller at alle pågående saker i saksbehandlingssystemet ble avsluttet før kommunesammenslåingen, og den siste uka før sammenslåingen fikk ingen lov å opprette nye saker. For pågående saker ble det opprettet nye saker og deler i arkivet med referanse til den avsluttede basen. Videre forteller konsulenten at dokumenter fra de opprinnelige kommunene ligger i en historisk database. Alle brukerne som hadde tilgang da kan fortsatt gå tilbake for å se på gamle dokumenter, men det er ikke mulig å registrere nye dokumenter i den historiske databasen. Konsulenten ved dokumentsenteret forteller at i forbindelse med sammenslåingen ble alle tilgangene til ePhorte gjennomgått. Dette førte til at noen grupper mistet tilgangene sine.

IT-avdelingen gjorde ikke egne sikkerhetstiltak i forbindelse med overgangen, forteller driftssjef-IT. Kommunene var en samkommune og hadde allerede felles systemer. Stort sett var det drift som vanlig. Det skjedde heller ikke mange fysiske endringer i forbindelse med sammenslåingen. Driftssjef-IT tror ikke ansatte merket overgangen til ny kommune.

Personvernombudet forteller at daværende kommunedirektør ikke ville prioritere kvalitetssystemet i kommunesammenslåingsprosessen. I stedet satset kommunen på å få på plass et nytt kvalitetssystem. Personvernombudet mener at hvis kommunen hadde prioritert oppdatering av det eksisterende systemet parallelt i prosessen ville kommunen fått oversikt på et tidligere tidspunkt. Kommunalsjef personal og organisasjon informerer om at styringsdokumentene for kommunesammenslåingen sier at kvalitetssystemet skulle prioriteres i slutten av 2019. Kommunen prioriterte ikke å oppdatere eksisterende system.

5.4 Sikkerhet

Det går fram av *Handlingsprogram og budsjett 2019 for Midtre Namdal samkommune*, at sikkerhet knyttet til bruk av IKT i kommunale tjenester er en stor utfordring. IT i MNS har laget en strategi for å minske konsekvenser av et angrep, særlig i forhold til krypteringsprogram. Det kreves at kommunene i større grad setter fokus på sikkerhetsarbeidet. IT-avdelingen kan ikke løse alle utfordringene og hver enkelt medarbeider må bidra aktivt til å verne løsningen. I tillegg er det nødvendig å iverksette tiltak. IT MNS er opptatt av at internkontrollen ikke er godt nok ivaretatt. Dette gjenspeiler seg i brukeroversikter, brukerkatalogen, telefonlistene, utlevert utstyr, rettighetsstyring med mer. Det anbefales at det iverksettes tiltak for som sikrer at kommunenes oversikter over ansatte og brukertilganger er i samsvar. Dette har også betydning for de lisenser kommunene betaler for. Dagens situasjon med brukertilgang er beskrevet i kapittel 4.2.5.

Driftssjef-IT forteller at løsningen for sikker sone ble byttet ut i forbindelse med kommunesammenslåingen.

Driftssjef-IT forteller at etter kommunesammenslåingen beholdt Namdalseid og Fosnes ansatte sine brukernavn, slik at de ikke er lik eposten de har i dag. Det jobbes med å endre pålogging for de som tidligere var i Namsos kommunen og dette er en omstendelig prosess som har startet opp. Planen er å bruke pålogging fra samkommunen som brukernavn.

6 HØRING

En foreløpig rapport ble sendt på høring til kommunedirektøren i Namsos kommune 24.05.2022. Høringssvaret er vedlagt rapporten i vedlegg to.

Utkast til rapport uten vurderinger, konklusjon og anbefalinger ble sendt kontaktperson i kommunen for faktaverifisering 09.05.2022. Revisor mottok svar på fakta verifiseringen sammen med høringssvaret fra kommunen den 27. 05.2022.

Revisor har korrigert rapporten i forhold til bemerkninger i faktaverifiseringen. Revisor har ikke gjort noen endringer som følge av høringsuttalelsen.

7 KONKLUSJONER OG ANBEFALINGER

7.1 Konklusjon

Denne forvaltningsrevisjonen har belyst to problemstillinger.

1. Hvordan ivaretar Namsos kommune informasjonssikkerhet?
2. Hvordan har kommunen sikret integritet, konfidensialitet og tilgjengelighet for informasjon fra de gamle kommunene?

Problemstilling to er besvar gjennom en beskrivelse av hvordan kommunen jobbet med IT ved kommunesammenslåingen.

Informasjonssikkerhet i Namsos kommune

Revisors konklusjon er at Namsos kommune mangler en forankring for arbeidet med informasjonssikkerhet i kommunens mer overordnede risikovurderinger og planer. Videre mangler kommunen blant annet internkontroll og kontroll med brukertilganger. Kommunen har en del forebyggende og oppdagende sikkerhetstiltak. Korrigerende tiltak er i stor grad på plass for IT-enheten, men ikke andre deler av kommunen.

Det mangler en overordnet risikovurdering for informasjonssikkerhet i Namsos kommune, som kan legge premissene for informasjonssikkerhetsarbeidet. Videre er det uklart om det finnes et mål for informasjonssikkerhet og det mangler en sikkerhetsstrategi. Driftssjef-IT er sikkerhetsansvarlig og informasjonssikkerhetsutvalget har rollen som sikkerhetsorganisasjon, men rollen i kommuneorganisasjonen er ikke formalisert.

Det finnes enkelte risikovurderinger innenfor informasjonssikkerhet. Internkontroll er ikke på plass og det arbeides med å få på plass et kvalitetssystem som grunnlag for internkontroll. Flere rutinebeskrivelser er på plass. Kommunen har et system på opprettelse av brukere, men har ikke kontroll på å avvikle brukere som ikke skal ha tilgang til datasystemet lengre. Ansatte får opplæring i informasjonssikkerhet. IT kommer sent inn i anskaffelse av programvare, noe som kan gjøre det vanskelig å ivareta sikkerheten og lage et effektivt driftsmiljø.

Når det kommer til tiltak for å forebygge, oppdage dataangrep og gjenopprette data, er dette tekniske tiltak som i stor grad er i stadig utvikling, for å imøtekomme utviklingen hos de som jobber med angrep. Noen ansatte har god oversikt over enheter og strukturen på IKT-systemet, men har ikke noe konfigurasjonskart. Kommunen har en behandlingsoversikt i henhold til personopplysningsloven som ligger i dagens kvalitetssystem, men det er ikke oppdatert.

Kommunen har praksis for sikkerhetsoppdateringer og sikkerhetskopier, men de er ikke skriftliggjort.

Namsos kommune har system for å overvåke, oppdage og fjerne sårbarheter. Kommunen har gjennomført sikkerhetstest.

IT-avdelingen har en plan for håndtering av sikkerhetshendelser og gjenoppretting. Det finnes en beredskapsplan på IT, men det er uklart om beredskapsplanen har en rolle i andre deler av organisasjonen.

Integritet, konfidensialitet og tilgjengelighet for informasjon ved kommunesammenslåingen

Revisors oppfatning er at integritet, konfidensialitet og tilgjengelighet for informasjon ble ivaretatt ved kommunesammenslåingen.

Kommunene som ble sammenslått, hadde allerede et samarbeid og datasystemene var allerede koblet sammen, slik at jobben med overgangen handlet om å integrere like systemer. Historiske data fra sak- og arkivsystemet er tatt var på og tilgjengelig fra historiske databaser.

7.2 Anbefalinger

Revisor anbefaler kommunedirektøren å vurdere følgende anbefalinger:

- Inkludere informasjonssikkerhet i helhetlig ROS.
- Utarbeide målsettinger og strategi for informasjonssikkerhet separat eller i forbindelse med andre plandokumenter.
- Om organisering og ansvar for informasjonssikkerhet er tydelig og hensiktsmessig.
- Få på plass et internkontrollsystem.
- Iverksette gjennomganger for å avvikle tilganger til personer som har sluttet.
- Sikre at behandlingsoversikter kommer på plass i henhold til personopplysningsloven.
- Løfte fokuset på informasjonssikkerhet som et ledd i å bygge en sikkerhetskultur.

KILDER

CISA (2015) CISA Review Manual 26th Edition. CISA

Finstad, A. og Mushtaq, S. (2021) Er en trygg digital hverdag mulig i kommunene? Kommunerevisoren 6/ 2021, s. 10-12.

Jøsang, A. (2021) Informasjonssikkerhet. Teori og praksis. Universitetsforlaget, Oslo

KMPG (2021) IKT-sikkerhet i Østre Toten kommune forut for dataangrepet 9. januar 2021.Kartlegging og ekstern vurdering. KPMG 2021

Nasjonal sikkerhetsmyndighet, udatert, Veileder i sikkerhetsstyring. Versjon 1. Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet (2020) NSMs grunnprinsipper for IKT-sikkerhet, versjon 2.0. 15.04.2020

Nasjonal sikkerhetsmyndighet (2021) Nasjonalt digitalt risikobilde 2021.

Nasjonal sikkerhetsmyndighet (2022) Risiko 2022. Økt risiko kraver økt årvåkenhet.

Namsos kommune (2019) Helhetlig risiko og sårbarhetsanalyse Namsos kommune. Vedtatt i kommunestyret 14.11.2019

Namsos kommune (2019) Overordnet beredskapsplan. Siste revisjon 17.10.2019.

Namsos kommune (2020) Kommuneplanens samfunnsdel 2020-2032 - sammen skaper vi muligheter. Vedtatt i kommunestyret 13.02.2020.

Namsos kommune (2020) Kommunal planstrategi 2020-2023 Namsos kommune. Vedtatt i kommunestyret 18.05.2020.

Namsos kommune (2021) Årsmelding fra personvernombudet 2021

Namsos kommune (2021)

Handlingsprogram med økonomiplan 2022-2025 - kommunestyrets vedtak (framsikt.net)

Namsos kommune (2022) Årsmelding 2021. Utkast 11.04.2022

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 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.

Problemstillingen om informasjonssikkerhet er knyttet til at Namsos kommune samler inn og lagrer informasjon, både elektronisk og på andre medier. Personvernforordningens artikkel 32 b knytter sikkerhet for personers rettigheter og friheter til evnen til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemer og -tjenestene.

- Konfidensialitet - informasjonen blir ikke kjent for uvedkommende
- Integritet - informasjonen ikke blir endret utilsiktet eller av uvedkommende
- Tilgjengelighet - at informasjonen er tilgjengelig for autoriserte ved behov
- Robusthet - summen av konfidensialitet, integritet og tilgjengelighet

Disse prinsippene for personopplysninger er også relevante for annen informasjon som en kommune lagrer, eksempelvis at informasjonen er gjenfinnbar i sin opprinnelige form. Det at informasjonen er tilgjengelig når kommunen trenger den er vesentlig for mye av tjeneste-utøvelsen i en kommune.

I denne forvaltningsrevisjonen legges det opp til tre tilnærminger til informasjonssikkerhet.

1. eForvaltningsforskriften, § 15 om internkontroll på informasjonssikkerhetsområdet for forvaltningsorgan
2. Sikkerhetsloven, kapittel 4 om krav til forebyggende sikkerhetsarbeid
3. Personopplysningsloven, hvor EUs personvernforordning er inntatt i loven og bestemmelsene omtales som artikler.

Informasjonssikkerhet gjenfinnes på flere nivå i en organisasjon, og Jøsang (2021) skiller mellom tre styringsnivå:

- Styring av informasjonssikkerhet
- Ledelse av informasjonssikkerhet
- Administrasjon og drift av informasjonssikkerhet

Strategisk nivå - styring av informasjonssikkerhet

Alle de tre lovbestemmelsene over peker på ledelsens ansvar, som først og fremst er på det strategiske nivået. Sikkerhetsloven stiller krav om at sikkerhetsstyringen skal gjennomføres planlagt og systematisk i et sikkerhetsstyringssystem som samordnes med virksomhetens styringssystem. Nasjonal sikkerhetsmyndighet har utarbeidet en veileder i sikkerhetsstyring[16] basert på kravene i sikkerhetsloven. Styring av informasjonssikkerhet består av å definere strategiske målsettinger av informasjonssikkerhet, sørge for at disse blir oppnådd, styre sikkerhetsrisikoen ved bruk av organisatoriske ressurser og påse at ledelsessystemet for informasjonssikkerhet fungerer hensiktsmessig og at resultater følger forventinger og målsettinger (Jøsang 2021). *Information systems audit and control association* (ISACA har fem hovedmålsettinger for styring av informasjonssikkerhet:

- Strategisk tilpasning av aktiviteter til informasjonssikkerhet - informasjonssikkerhet er ikke et mål i seg selv, men skal bidra til virksomhetens mål.
- Risikostyring
- Effektiv bruk av ressurser - ledelsessystem og -prosesser må standardiseres så langt som mulig for å redusere administrasjons- og opplæringskostnader.
- Verdiskaping – optimal verdiskaping oppstår når strategiske mål for informasjons-sikkerhet oppnås, juridiske krav etterleves og sikkerhetstrusler balanseres med akseptabel risiko, alt til lavest mulig kostand.
- Målbarhet – Måling er viktig for å vurdere om målsettinger oppnås. Metoder for å måle aktiviteter og hendelser relaterte til informasjonssikkerhet på tvers av organisasjonen må utvikles.

Sikkerhetslovens § 4-1 pålegger virksomhetensleder ansvaret for det forebyggende sikker-hetsarbeidet og at dette skal være en del av virksomhetens styringssystem. Sikkerhets-tilstanden i virksomheten skal regelmessig kontrolleres. § 4-1 andre ledd sier at virksomheten skal sørge for at ansatte, leverandører og oppdragstakere har tilstrekkelig risiko- og sikkerhets-forståelse. § 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. I § 4-4 står det at virksomheten skal dokumentere vurderingen av risiko og de gjennomførte og planlagte sikkerhetstiltakene.

[16] veileder-i-sikkerhetsstyring.pdf (nsm.no)

Ledelse av informasjonssikkerhet

Ledelse av informasjonssikkerhet er å opprette, drifte og vedlikeholde et sett med prosesser og aktiviteter som på en fornuftig måte beskytter organisasjonens informasjonsverdier mot sikkerhetstrusler, og som dermed kan opprettholde sikkerhetsmålene om konfidensialitet, tilgjengelighet og integritet (Jøsang 2021). Videre sier Jøsang (2021) at ledelse av informasjonssikkerhet bør være basert på et ledelsesinformasjonssystem bygd opp av et sett med prosesser og aktiviteter definert av et utvalg av standarder, rammeverk og egendefinerte retningslinjer og policyer, eksempelvis ISO 27001.

Paragraf 15 i eForvaltningsforskriften omhandler internkontroll på informasjonssikkerhetsområdet for forvaltningsorgan. § 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.

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.

Drift av informasjonssikkerhet

Administrasjon og drift av informasjonssikkerhet er en samling ulike aktiviteter, slik som eksempelvis brannmurer, konfigurering, overvåkning, sårbarhetsskanning, forebygge tap og gjenoppretting av data (Jøsang 2021).

På tvers av disse organisatoriske nivåene kan informasjonssikkerhetsarbeidet deles inn i forebyggende, oppdagende og korrigere (CISA 2015). Tilnærmet denne inndelingen finnes også i NSM sine grunnprinsipper for informasjonssikkerhet, jf. tabell 1 under.

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.

Grunnprinsipper for IKT-sikkerhet

Nasjonal sikkerhetsmyndighet har utarbeidet grunnprinsipper for IKT-sikkerhet (NSM 2020), i tillegg til veilederen i sikkerhetsstyring som er omtalt over. Grunnprinsippene for IKT-sikkerhet fokuserer på teknologiske og organisatoriske tiltak. Grunnprinsippene er delt i fire kategorier og er gjengitt i tabellen under.

Tabell 1. Grunnprinsipper for IKT-sikkerhet

1. Identifisere og kartlegge	**2. Beskytte og opprettholde**
Kartlegge styringsstrukturer, leveranser og understøttende system Kartlegge enheter og programvare Kartlegge brukere og behov for tilgang	Ivareta sikkerhet i utviklings- og anskaffelsesprosesser Etablere en sikker IKT-arkitektur Ivareta en sikker konfigurasjon Beskytte virksomhetens nettverk Kontroller dataflyt Ha kontroll på identiteter og tilganger Beskytt data i ro og i transitt Beskytt e-post og nettleser Etablere evne til gjenoppretting av data Integrere sikkerhet i prosess for endringshåndtering
3. Oppdage	**4. Håndtere og gjenopprette**
Oppdage og fjerne kjente sårbarheter og trussel Etablere sikkerhetsovervåkning Analysere data fra sikkerhetsovervåkning Gjennomføre inntrengningstester	Forbered virksomheten på håndtering av hendelser Vurder og klassifiser hendelser Kontroller og håndter hendelser

Kilde: NSM 2020

Hovedinndelingen av grunnprinsippene for IKT-sikkerhet er i stor grad sammenfallende med CISAs inndeling i forebyggende, oppdagende og korrigere tiltak.

I personvernforordningens artikkel 4, nummer 7 defineres behandlingsansvarlig som eksempelvis en offentlig myndighet som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger. Namsos kommune er behandlingsansvarlig for personopplysninger hvor kommunen har et formål med håndtering av personopplysningene. Kommunen skal derfor ha en oversikt over hvilke systemer kommunen har som behandler personopplysninger. Artikkel 30 stiller krav til at behandlingsansvarlig skal føre protokoll over behandlingsaktiviteter som de utfører. Behandlingsoversikten skal være skriftlig og inneholde:

- Navn og kontaktopplysning på behandlingsansvarlig
- Formålet med behandlingen
- Beskrivelse av kategoriene av registrerte og kategoriene av personopplysninger
- Kategori av mottakere av personopplysninger
- Eventuelt planlagte tidsfrister for sletting
- Eventuelt tekniske og organisatoriske sikkerhetstiltak

Kommunen bør ha oversikt over alle enhetene i informasjonssystemet. (NSM 2020) Denne bør være basert på hva kommunen har behov for av enheter og retningslinjer for godkjenning av enheter.

Kommunen skal ha et system for tilgangsstyring, som ivaretar at behandlingen av person-opplysninger begrenses til det som er nødvendig for formålene de behandles for (artikkel 5, 1 punkt, bokstav c). I dette ligger det at bare de som har bruk for informasjonen har tilgang til den. Begrensning av tilganger henger sammen med at eventuelle inntrengeres muligheter blir mindre. En virksomhet må derfor har kontroll på de ulike brukerne, kontoene de disponerer og hvilke rettigheter en gitt konto har (NSM, 2020).

Enheter, programvare og brukere er sentrale elementer i et informasjonssystem som inngår i den overordnede IKT-arkitekturen. Kommunen bør bygge en sikker IKT-arkitektur med sentral styring og automatiserte prosesser hvor det er hensiktsmessig (NSM, 2020). En slik IKT-arkitektur kan visualiseres i et konfigurasjonskart som viser ulike soner for tilganger, brannmurer med mer.

Denne IKT-arkitekturen bør beskyttes med brannmurer, kryptering og antivirus program.

Det er mulig å konfigurere både utstyr og programvare, slik at det legges inn begrensninger i bruken for å ivareta sikkerheten. En viktig del av dette er å sikre at sikkerhetsoppdatering installeres når de foreligger og at dette er sentralt styrt (NSM 2020).

Selv om mange sikkerhetstiltak kan bygges inn i systemer vil det alltid være en risiko for at autoriserte brukere er inngangen for mange som vil bryte seg inn i informasjonssystemer, eksempelvis gjennom å trykke på lenker som kommer på epost. Opplæring av ansatte og informasjon om sikkerhetstiltak som den enkelte kan følge opp er viktig for å bygge en sikkerhetskultur i virksomheten. Samtidig er det viktig at ansatte får beskjed når det dukker opp phishing-kampanjer, slik at ingen aktiverer lenken.

Til tross for at systemer kan beskyttes teknisk vil det alltid være steder som er mer sårbare enn andre. Noe av dette kan også være bevisst for at systemene skal være mer brukervennlig. Det betyr at det må finnes tiltak for å gjenopprette informasjon gjennom for eksempel

sikkerhetskopier. Kommunen må ha system som sikrer tilstrekkelig sikkerhet for personopplysninger, herunder vern mot utilsiktet tap, skade eller ødeleggelse (artikkel 5, punkt 1, bokstav f)

Gjennom skyløsninger for programvare og for eksempel samarbeidsparter vil kommunen kunne utveksle data med andre, såkalte databehandlere. Artikkel 4, punkt 8 definerer databehandler som en fysisk eller juridisk person som behandler personopplysninger på vegne av 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, hvor punkt c henviser til artikkel 32 om sikkerhet ved behandling av personopplysninger. Kommunen bør vurdere sikkerheten i forbindelse med inngåelse av databehandleravtaler.

Moderne skadevare utvikles for å unngå enkelte sikkerhetstiltak, eller for å angripe eller deaktivere tiltakene. Selv de beste produkter har feil og sårbarheter som kan utnyttes av angripere (NSM 2020). Kommunen bør ha et system for sikkerhetsovervåking. Data fra sikkerhetsovervåkningen bør analyseres med tanke på å oppdage uautoriserte handlinger og sikkerhetstruende hendelser. IKT-systemer er under konstant endring og utvikling og utfordres jevnlig av angrepsaktører. Virksomheter bør derfor jevnlig teste egen forsvarsevne for å verifisere etablerte sikkerhetstiltak, identifisere mangler og vurdere egen beredskap. Dette kan gjøres gjennom jevnlige inntrengningstester. (NSM 2020)

Nasjonal sikkerhetsmyndighet (2020) skriver at dataangrep har blitt en del av dagliglivet. Når hendelsen inntreffer er det for sent å utarbeide gode prosedyrer, rapporteringsrutiner, datainnsamling, ledelsesansvar og kommunikasjonsstrategier. Kommunen må derfor ha en plan for hendelseshåndtering som oppdateres minst en gang i året.

Nasjonal sikkerhetsmyndighet sine grunnprinsipper strekker seg på tvers av nivåene i en organisasjon og danner en matrise, slik som vist i tabellen under.

Tabell 2. Nasjonal sikkerhetsmyndighets grunnprinsipper

	Forebygge	**Oppdage**	**Korrigere**
Styringsnivået	Overordnet risikovurdering Sikkerhetsmål og sikkerhetsstrategi Sikkerhetsorganisasjon		Beredskapsplan
Ledelsesnivået	Risikovurderinger Internkontroll (rutiner) Rutiner for tilgangsstyring Opplæring og sikkerhetskultur Anskaffelser	Anskaffelse Lage plan for overvåkning Beslutte sikkerhetstester	Anskaffelse Lage plan for hendelseshåndtering, gjenoppretting og beredskap
Driftsnivået	Kartlegge enheter Konfigurasjonskart Behandlingsoversikt Sikkerhetsoppdateringer Sikkerhetskopier Sikkerhetstester	System for overvåkning Sikkerhetstester	Iverksette plan for hendelseshåndtering Iverksette gjenoppretting Iverksettes beredskapsplan

Kilde: Utviklet av Revisjon Midt-Norge

Tabellen er til hjelp for å strukturere sammenhengene og viser blant annet at ledelsesnivået har en rolle i å legge rammene for driftsnivået, som igjen er forankret i styringsnivået. Derfor ligger det til ledelsesnivået å legge planer, mens driftsnivået er de som iverksetter de konkrete tiltakene og planene. Når det gjelder anskaffelser så er dette en aktivitet som ligger på ledernivået og må ha et fokus på både forebygging, muligheter for å oppdage og korrigere hendelser, som en del av anskaffelsen. Under er revisjonskriteriene utledet med utgangspunkt i aktiviteter på styringsnivået, ledelsesnivået som omfatter både forebygging, oppdage og korrigering. Driftsnivået er delt i tre med forebygging, oppdage og korrigering. Grunnlaget for revisjonskriteriene er utledet foran.

Styringsnivået

- Kommunen skal regelmessig gjennomføre og dokumentere overordnede risikovurderinger som grunnlag for informasjonssikkerhetstiltak
- Kommunen skal ha sikkerhetsmål og sikkerhetsstrategi
- Kommunen skal ha en sikkerhetsorganisasjon hvor ansvar og roller for informasjons-sikkerhet framgår

Ledelsesnivået

- Det skal gjennomføres og dokumenteres risikovurderinger innenfor informasjons-sikkerhet
- Informasjonssikkerhet skal inngå i kommunens internkontrollsystem
- Kommunen må ha rutiner med tilhørende praksis for tildeling og fjerning av tilganger og jevnlig kontrollere identiteter og tilganger

- Kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet
- Kommunen bør vurdere og dokumentere IKT-risiko ved anskaffelser av datasystemer

Forebyggende

- Kommunen må ha en oversikt over enheter i IKT-systemet
- Kommunen bør etablere en sikker IKT-arkitektur
- Kommunen må ha en oversikt over programvare som er i bruk som tilfredsstiller kravene til en behandlingsoversikt
- Kommunen skal beskytte virksomhetens data
- Kommunen bør ha sentral styring med sikkerhetsoppdateringer
- Kommunen må sikkerhetskopiere

Oppdage

- Kommunen bør ha et system for å overvåke sikkerheten og analysere data fra overvåkningen
- Kommunen bør ha et system for å oppdage og fjerne kjente sårbarheter (automatisert og sentralisert verktøy eks antivirus, loggføring og sikkerhetsovervåkning)
- Kommunen bør gjennomføre sikkerhetstester

Korrigere

- Kommunen bør ha en plan for hendelseshåndtering (ansvar, tiltak, kommunikasjon, gjenopprettingsplan og loggføring)
- Kommunen må ha en plan for gjenoppretting
- Kommunen må ha en beredskapsplan som omfatter IKT hendelser

VEDLEGG 2 - HØRINGSSVAR

Namsos kommune
Nåavmesjenjaelmien tjïelte
Personal

Revisjon Midt Norge
Brugata 2
7715 STEINKJER

Uoff i hht: Offl. § 5 1. ledd

Vår referanse	Deres referanse	Saksbehandler	Tlf. saksbehandler	Dato
2021/9312-3		Anne Kristin Melgård	924 15 395	27.05.2022

Tilbakemelding høringsutkast forvaltningsrevisjon

I forordet til foreløpig versjonen av rapporten gis den reviderte part mulighet til å se gjennom og gi sitt syn på innholdet. Viser i tillegg til kommentarer i allerede tilsendt rapport til fakta verifisering. Legger ved denne her også.

Kommunedirektøren vil med denne tilbakemeldingen gi sitt syn på innholdet og vise til at Namsos kommune har et høyt fokus på informasjonssikkerhet. Ved opprettelse av ny kommune ble det prioritert en 50 % ressurs på rollen som Personvernombud. Det ble også prioritert videreutdanning innen området.

Kommunedirektøren vil ta med seg revisors anbefalinger i utkastet til vurdering. Kommunedirektøren ser at de funn og anbefalinger som gir samsvarer med pågående og planlagt arbeid med informasjonssikkerhet.

Det vises til gjeldende planstrategi for perioden 2020-2023 vedtatt av Namsos kommunestyre 18.06.2020, hvor overordnet plan for samfunnssikkerhet og beredskap, samt helhetlig risiko og sårbarhetsanalyse (ROS) skal revideres i 2023. Ny planstrategi er under utarbeidelse og kommunens leveranseavtaler IKT er under revidering.

Arbeid med informasjonssikkerhet er forankret i kommunedirektørens ledergruppe, noe som også kan dokumenteres i referat fra ledermøtene. Kommunens informasjonssikkerhetsutvalg ledes av assisterende kommunedirektør og utvalget møtes en gang pr måned. Når det gjelder arbeid med å bygge en sikkerhetskultur så har kommunen blant annet nylig innarbeidet et eget punkt om informasjonssikkerhet i årlige medarbeidersamtaler og

E-post: postmottak@namsos.kommune.no
Tlf: 74 21 71 00
Internett: namsos.kommune.no

Postadresse:
Stavarvegen 2
7855 Jøa

Besøksadresse:
Namdalshuset, Søren P
Thornæs veg 10, Namsos

Kontonr: 4212.31.87436
Kontonr skatt: 7855.05.37034
Org.nr: 942 875 967

kommunen deltar i KS nettverket Strategisk Nettverk for Informasjonssikkerhet og Personvern – hvor tema er hvordan bygge en sikkerhetskultur.

Oppgi vårt referansenummer når du tar kontakt med oss.

Hilsen
Anne Kristin Melgård
kommunalsjef personal og organisasjon

Dokumentet er elektronisk godkjent og sendes uten signatur.

Revisjon

Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no

Oppfølging av Forvaltningsrevisjonsrapport - Personal nærvær

Behandles i utvalg	Møtedato	Saknr
Kontrollutvalget i Namsos kommune	30.08.2022	23/22

Saksbehandler Einar Sandlund
Arkivkode FE-217, TI-&58
Arkivsaknr 20/422 - 11

Forslag til vedtak:
Kontrollutvalget tar skriftlig rapport fra kommunedirektøren datert 03.03.22 til orientering.

Vedlegg
Rapport -oppfølging av forvaltningsrevisjonsrapport personal nærvær

Saksopplysninger
Kommunestyret fattet 21.10.21 slikt vedtak:
1. Kommunestyret tar forvaltningsrevisjonsrapporten Nærvær - Personal, sykefraværsoppfølging og erstatning av kompetanse ved fravær til orientering.
2. Kommunestyret ber kommunedirektøren følge opp rapportens anbefalinger i kap.6.2.
3. Kommunestyret ber kommunedirektøren innen 30.04.22 om skriftlig rapport til kontrollutvalget, med kopi til kommunestyret, på hvordan anbefalingene er fulgt opp.
Rapporten ga slike anbefalinger:
• *Fortsetter arbeidet med å implementere interne rutiner i avdelingene*
• *Senker avdelingsledernes terskel for å kontakte personalavdelingen*
• *Fortsetter arbeidet med å sikre riktig kompetanse ved sykefravær*

Kommunedirektøren har kommet med skriftlig rapport datert 03.03.22, jfr. vedlegg.

Rapporten ble behandlet av hhv. formannskap og kommunestyret i møter 04.04. og 19.05.22.

Vurdering
Kommunedirektøren har gitt skriftlig tilbakemelding, jfr. vedlegg, på hvordan anbefalingene i rapporten er fulgt opp. Sekretariatet er av den oppfatning at kommunedirektøren følger opp rapportens anbefalinger.
Ut fra den gitte informasjon anbefales kontrollutvalget å ta den den skriftlige orienteringen til orientering.

Namsos kommune
Nåavmesjenjaelmien tjïelte
Personal

Orienteringssak

Arkivreferanse: 2022/1765-1
Saksbehandler: Anne Kristin Melgård
Dato: 03.03.2022

Orientering om oppfølging av Forvaltningsrevisjonens anbefalinger av revisjonsrapport nærvær-personal

Utvalg	Møtedato	Saksnummer
Namsos formannskap	05.04.2022	
Namsos kommunestyre	19.05.2022	

Kommunedirektørens innstilling

Rapportering tas til orientering.

Dokumenter i saken

Type	Dato	Tittel	Adressat
S	03.03.2022	Orientering om oppfølging av Forvaltningsrevisjonens anbefalinger av revisjonsrapport nærvær-personal	

Saksopplysninger

Revisjon Midt-Norge SA gjennomførte en forvaltningsrevisjon første halvår 2021 med tema hvordan kommunen arbeider med sykefraværsoppfølging og erstatning av kompetanse ved sykefravær på fagområdene Helse og velferd og Oppvekst og opplæring.

Revisjonen undersøkte tre problemstillinger

1. Hva mener kommunen er årsakene til sykefraværet i oppvekst og helse/velferd?
2. Hvilke erfaringer har ledere og ansatte med kommunens oppfølging av sykemeldte og er praksis i tråd med gjeldende regelverk?
3. Er kommunen i stand til å ivareta kompetansebehov/-krav ved sykefravær?

Revisjonen oppsummerer sine funn som under:
Namsos kommune fører sykefraværsstatistikk og er tilknyttet bedriftshelsetjeneste. Kommunen har rutiner for både forebygging og oppfølging av sykefravær. Det er uklart hvor mye av dette som følges i praksis ute i avdelingene. Revisors oppfatning er at det kan være en fordel om avdelingslederne tar kontakt med personalavdelingen tidligere i forløpet.

Data tyder på at kommunen ønsker å erstatte syke medarbeidere med arbeidskraft med tilsvarende kompetanse. Ved korttidsfravær gjør de i all hovedsak dette ved å bruke de som allerede er ansatt, enten ved å flytte vakter eller ved å ringe opp noen som ikke er på arbeid den dagen. Stort sett blir sykefraværet erstattet av ansatte med tilsvarende kompetanse. Hvis tilsvarende kompetanse ikke er å få tak i løses dette ved omorganisering av arbeidsoppgaver eller med å ha sykepleier/vernepleier på bakvakt. Barnehagene prioriterer nok bemanning over riktig kompetanse ved korttidsfravær. Ved langtidsfravær er det enklere å rekruttere ansatte med høyere utdanning, enn ved korttidsfravær.

Revisor anbefaler at Namsos kommune:

1. Fortsetter arbeidet med å implementere interne rutiner i avdelingene
2. Senker avdelingsledernes terskel for å kontakte personalavdelingen
3. Fortsetter arbeidet med å sikre riktig kompetanse ved sykefravær

Namsos kommunestyre vedtok 21.10.21 å ta forvaltningsrevisjonens rapport til orientering og ba om at kommunedirektøren følger opp anbefalingene. Videre ba kommunestyret om at kommunedirektøren innen 30.04.22 leverte en skriftlig rapport til både revisjon og kommunestyret om hvordan anbefalingene følges opp.

Saksfremlegget beskriver oppfølging av anbefalingene i form av roller og aktiviteter:

Anbefaling 1 og 2

Namsos kommune fortsetter arbeidet med å implementere interne rutiner i avdelingene og senker avdelingsledernes terskel for å kontakte personalavdelingen

Roller	**Aktivitet**
Personalavdelingen	- dialog med de ulike ledernivåene og delta på møter på tjenestestedene - dialog med legene ang skjema *Leder før lege* og *Alternative oppgaver* - gjennomføre webinar for partsgruppene og med samarbeidspartnerne om ulike personalpolitiske tema - informasjon om oppgavefordeling på personalavdelingen - være tilgjengelig for lederne og bistå ved behov
Ledere ulike nivå	- gjennomgang interne rutiner og retningslinjer i partssamarbeidet alle nivå - ta tidlig kontakt for råd og veiledning
Tillitsvalgte	- deltar på webinar - delta i partssamarbeid alle nivå - være samarbeidspartnere og støttespillere i partsgruppene - være pådrivere og forslagsstillere i AMU

Anbefaling 3:

Namsos kommune fortsetter arbeidet med å sikre riktig kompetanse ved sykefravær

Roller	**Aktivitet**
Personalavdelingen	- bistå ved tilsettinger og vurdere rekrutteringstiltak - sikre godt samarbeid i omplasseringssaker - bidra i strategisk kompetanseplanlegging - redegjøre og skaffe til veie nødvendig statistikk
Ledere ulike nivå	- bemannings- og kompetanseplanlegging - tema i partssamarbeidet alle nivå - vurdering av ulike tiltak for mer tilgang til vikarer
Tillitsvalgte	- være samarbeidspartnere og forslagsstillere i partssamarbeidet alle nivå

Behandling i Namsos kommunestyre - 19.05.2022:

Rapportering tas til orientering.

Tilbakemelding - statsforvalterens tilsyn landbruksforvaltning

Behandles i utvalg	Møtedato	Saknr
Kontrollutvalget i Namsos kommune	30.08.2022	24/22

Saksbehandler Einar Sandlund
Arkivkode FE-033, TI-&58
Arkivsaknr 20/227 - 4

Forslag til vedtak:
Kontrollutvalget tar tilbakemelding gitt 15.06.22 til orientering og ber om å få en orientering om kommunens landbruksforvaltningens oppgaver, ressurser og utfordringer på et senere møte.

Vedlegg
Kst-behandling forvaltningskontroll landbruk
Tilbakemelding på endelig rapport etter forvaltningskontroll på landbruksområdet - Namsos kommune

Saksopplysninger
Kontrollutvalget fattet i sak 20/22 slikt vedtak:
Kontrollutvalget viser til Statsforvalterens tilsynsrapport på landbruksforvaltning og ber om til neste møte å få kopi av kommunedirektørens tilsvar til rapporten.

Skriftlig tilbakemelding til Statsforvalteren ble gitt 15.06.22, jfr. vedlegg.
Orienteringssak og tilbakemelding er vedlagt.

Vurdering
Sekretariatet viser til tilbakemeldingen gitt til Statsforvalteren og anbefaler kontrollutvalget å ta den til orientering. Videre bør kontrollutvalget i et senere møte be om å få en orientering om kommunens landbruksforvaltningens oppgaver, ressurser og utfordringer.

Emne: VS: Tilbakemelding på endelig rapport etter forvaltningskontroll på landbruksområdet - Namsos kommune
Kopi: Sigrid T. Angen <Sigrid-T.Angen@namsos.kommune.no>, Thomas Aarskog <Thomas.Aarskog@namsos.kommune.no>
Til: Einar Sandlund <Einar.Sandlund@konsek.no>
Sendt: 15.08.2022 12:44:06
Fra: Per Olav Meosli <Per-Olav.Meosli@namsos.kommune.no>
Hei.

Videresender tilbakemelding på endelig rapport etter forvaltningskontrollen på landbruk.

Mvh
Per Olav Meosli

Fra: Per Olav Meosli
Sendt: onsdag 15. juni 2022 22:20
Til: sftlpost@statsforvalteren.no
Kopi: Sakshaug, Odd Lutnæs <fmtlols@statsforvalteren.no>
Emne: Tilbakemelding på endelig rapport etter forvaltningskontroll på landbruksområdet - Namsos kommune

Hei.

Generell tilbakemelding på endelig rapport:
Kommunen tar til etterretning de feil og mangler som forvaltningskontrollen avdekker. De fleste avvik bunner i mangelfullt internkontrollsystem med utdaterte saksbehandlingsrutiner. Arbeidet med å utvikle et adekvat internkontrollsystem på landbruksområdet, med oppdatering av saksbehandlingsrutiner og kontrollplan er igangsatt, og søkes implementert innen 1. september. Disse vil bli en del av kommunens internkontrollsystem.

Kommentar til merknad 1 som gjelder tilskuddsordning - AR 5:
Kommunen skal revidere de skriftlige rutinene for ajourhold i samsvar med mal utarbeidet av NIBIO. Landbruk har akkurat blitt samorganisert med blant andre kart og oppmåling, slik at rutine for ajourhold vil utarbeides i samarbeid med flere faggrupper.

Kommentar til merknad 2 som gjelder tilskudd til gjennomført tiltak – SMIL:
Vi tar merknaden til etterretning, og skal legge inn de spesifikke krav til kontroll, dokumentasjon og godkjenning av ekstrakostnader ved gjennomføring av prosjekt, i vårt internkontrollsystem.

Spesifikk kommentar til avvik 4 (SMIL):
Avvik 4 i kontrollen, som sier at det er utbetalt for mye i tilskudd, mener vi er feil. Tilskuddsbeløpet ble ved en feil oppført i rubrikk for kostnader uten å bli rettet. Det ble beregnet tilskudd på kr.114.500 av riktig kostnadsoverslag på kr.229.000
Om kommunen behandler saken på nytt, vil resultatet bli det samme siden endelig grunnlag for beregning av tilskudd (kr.229.000.-) er riktig.

Mvh
Per Olav Meosli

Bestilling av forvaltningsrevisjon -

Behandles i utvalg	**Møtedato**	**Saknr**
Kontrollutvalget i Namsos kommune	30.08.2022	25/22

Saksbehandler Einar Sandlund
Arkivkode FE-217, TI-&58
Arkivsaknr 22/153 - 1

Forslag til vedtak:

1. Kontrollutvalget bestiller forvaltningsrevisjon av kvaliteten i pleie- og omsorgstjenesten og gir følgende innspill til prosjektplanen:

-
-

2. Revisjonen bes utarbeide prosjektplan til kontrollutvalgets møte den 22.01.22.

Saksopplysninger
Kommunelovens § 23-3 sier at det skal gjennomføres forvaltningsrevisjon i kommunen. Kommunestyret behandlet den 29.10.20 i sak 155/20 plan forvaltningsrevisjon 2020-2024.

Kontrollutvalget fattet i sak 02/22 den 19.01.22 slikt blant annet slikt vedtak:
1. Prioritering av forvaltningsrevisjoner endres slik:
1) Barnefattigdom(Oppvekst barn og unge; sårbarhet, tverrsektorielt samarbeid, fattigdom)
2) Kvalitet i helse og omsorgstjenestene
3) Psykisk helse, rus
4) Barnevern
Kontrollutvalgets vedtak pkt. 1 sendes kommunestyret til orientering.

Endringen i forvaltningsrevisjonsplanen ble gjort ut fra at gjenstående prosjekter sto i uprioritert rekkefølge. Forvaltningsrevisjon Barnefattigdom er igangsatt med forventet levering november 2022. Revisjonen har avsatt 2200 timer til forvaltningsrevisjon i Namsos 2020 – 2023. Av dette er det utført og disponert ca. 1400 timer. Det gjenstår da ca. 3 forvaltningsrevisjoner/eierskapskontroller hvor av rapporten fra det siste går over i neste valgperiode. Neste prioriterte prosjekter er da hhv. *Kvalitet i helse og omsorgstjenestene, samt Psykisk helse, rus.*

Plan for forvaltningsrevisjon sier følgende om Kvalitet i helse og omsorgstjenestene:
Tjenestene utgjør en sammensatt, stor og vesentlig omfattende del av kommunens tjenestetilbud. Pandemien har gitt, og gir tjenestene, utfordringer. Pleie- og omsorg er en stor del av omsorgstjenestene og er det området som bør prioriteres. Sekretariatet mener at området gis 2. prioritet med bestilling og prosjektplan behandles høsten 2022.

Covid-19 viser at kommunen også må være forberedt på uforutsette situasjoner. Dette stiller vesentlige krav til å vurdere utfordringsbildet, planverk, ressurser og utførelse.

- *Risikoanalyser/utfordringsbilder som plangrunnlag?*
- *Planprosessen; sikres brukere og andre medvirkning?*
- *Implementering av nasjonalt gitte kvalitetskrav og innhold i helse- og omsorgstjenestene?*
- *Rutiner for å sikre oppdatert og relevant planverk?*
- *Avviksmeldinger og oppfølging*

Plan for forvaltningsrevisjon sier følgende om Psykisk helse, rus**:**
Psykisk helse og rusomsorg er tjenester hvor kommunen har hatt ventelister til tross for opptrappingsplan fra staten. Det har vært utfordrende innenfor en trang økonomi å følge opp med nye tiltak og dermed økt satsing innfor rus/psykisk helse. Det er en vekst i tjenestemottakere innenfor rus og psykisk helsetjenester. Ut fra dette anbefales prosjektet å gis 3. prioritet og bestilling foretas i november 22. Kommunen har hatt ventelister og vekst i antall brukere. Det er utfordringer med nye tiltak/økt satsning innenfor rus og psykiatri. Tilsyn har avdekket avvik på oppbygging av tjenesten.

• Har kommunen ruspolitisk handlingsplan og hvordan følges evt. denne opp?
• Har kommunen organisert tjenestetilbudet til personer med psykiske problemer og/eller rusmiddelproblemer på en tilfredsstillende måte?
• Har kommunen tilfredsstillende rutiner for å identifisere og følge opp personer med psykiske problemer og/eller rusmiddelproblemer?
• Har kommunen tilstrekkelig kompetanse til å gjennomføre kartlegginger av psykiske problemer og rusmiddelproblemer?
• Har kommunen tilfredsstillende tilbud til personer med psykiske problemer og/eller rusmiddelproblemer?
• Hvordan sikrer kommunen at innbyggere i målgruppen for tjenestene får tilstrekkelig informasjon om tjenestene kommunen tilbyr?
• Hvordan er samsvaret mellom budsjett og bruk av midler til psykisk helsearbeid og rusomsorg i kommunen?

Vurdering
Sekretariatet viser til prioritering av forvaltningsrevisjoner i KU-sak 02/22. Helse- og omsorgstjenestene har et vidt spekter av tjenester og er viktig for liv og helse. Pleie- og omsorg er den største av tjenestene mht. brukere, ansatte og økonomi. Helsetjenesten omfatter flere deltjenester som lege, helsesykepleier, skolehelsetjeneste, psykisk utviklingshemmede, funksjonshemmede.

Psykiatri/rus er en del av helsetjenesten og er som nevnt prioritert som eget neste forvaltningsrevisjonsprosjekt. Bestilling av denne kan foretas på første møte i 2023.

Sekretariatet er av den oppfatning at prioriteringsrekkefølgen av prosjekter fortsatt er aktuell vedr. bestilling av forvaltningsrevisjon og at kvalitet i pleie- og omsorgstjenesten bør prioriteres ut fra tjenestens utfordringer og omfang. Kontrollutvalget anbefales å bestille forvaltningsrevisjon av kvaliteten i pleie- og omsorg og å komme med innspill til prosjektplan som revisor bes å komme med til novembermøtet i kontrollutvalget.

Budsjett 2023 og økonomiplan 2023-26 for kontrollarbeidet

Behandles i utvalg	Møtedato	Saknr
Kontrollutvalget i Namsos kommune	30.08.2022	26/22

Saksbehandler Einar Sandlund
Arkivkode FE-033
Arkivsaknr 20/183 - 42

Forslag til vedtak:
1. Kontrollutvalget slutter seg til det framlagte forslag til driftsbudsjett for 2023 for kontrollarbeidet i kommunen, med en total ramme på kr 1 742 000.-.
2. Budsjettforslaget tar ikke høyde for ekstraordinære ressursbehov i kontrollsammenheng.
3. Forslaget oversendes kommunedirektøren for videre behandling i samsvar med § 2 i forskrift om kontrollutvalg.

Saksopplysninger
Saksbehandling og saksgang for budsjettet for kontrollarbeidet går fram av § 2 i forskriften om kontrollutvalg og revisjon:

§ 2.Kontrollutvalgets rolle i fastsettelsen av budsjettet for kontrollarbeidet
Kontrollutvalget skal utarbeide forslag til budsjett for kontrollarbeidet i kommunen eller fylkeskommunen. Forslaget skal følge innstillingen til årsbudsjettet etter kommuneloven § 14-3 tredje ledd til kommunestyret eller fylkestinget.
Forskriften pålegger kontrollutvalget å fremme forslag til budsjett for kontrollarbeidet i kommunen. Utvalgets ansvar og oppgaver er i det alt vesentlige lovregulert. Utvalgets ansvarsområde kan deles inn i tre områder, kontrollutvalgets egne aktiviteter, kjøp av sekretariatstjenester og kjøp av revisjonstjenester.

I forslaget til total ramme er det ikke lagt opp til større vesentlige endringer i utvalgets samlede aktivitetsnivå for 2023. I kontrollarbeidssammenheng er de største postene kjøp av sekretariats- og revisjonstjenester; ellers inneholder budsjettet poster for kontrollutvalgets egen drift. Alle kostnader mht. kontroll og tilsyn skal føres på funksjon 110.

Kontrollutvalgets egne utgifter
Budsjettet gjelder hovedområdene lønn, andre driftsutgifter, samt kjøp av varer og tjenester. I lønn inngår bl.a. fast årlig godtgjørelse, tapt arbeidsfortjeneste, møtegodtgjørelse, reiseutgifter og tilhørende sosiale kostnader. Satsene for godtgjøring til folkevalgte er fastsatt av kommunestyret. I andre driftsutgifter inngår bevertning, faglitteratur/tidsskrifter og kurs-/oppholdsutgifter mv. Kontrollutvalget er et viktig organ og må ha ressurser til faglig oppdatering i form av å delta på kurs og konferanser. Det er lagt opp til 6 møter i 2023. Det er i budsjettet generelt lagt inn ca. 3% utgiftsøkning pr. år.

Kontrollutvalgssekretariat
Kontrollutvalgets sekretariat, Konsek Trøndelag IKS (Konsek) utgjør kontrollutvalgets operative ledd. Konsek har ansvar for saksutredning og generell tilrettelegging for utvalgets arbeid. Representantskapet i Konsek vedtok i repr.skapsmøtet april 2022 budsjett for 2023 og økonomiplan 2023-2026. Det er lagt opp til ca. 3% økning pr. år.

Revisjon
Revisjon Midt-Norge SA har opplyst at beløpet for revisjonstjenester 2023*(se nedenfor, samt økonomiplan 2023 – 2026, blir fastsatt i årsmøtet høsten 2022. En tar derfor foreløpig utgangspunkt i beløpet for revisjonstjenester som er angitt i årsmøtet våren 2022.

Budsjettforslag 2023 med økonomiplan 2023 - 2026:

Budsjett	Budsjett 2022	**Forslag 2023**	Forslag 2024	Forslag 2025	Forslag 2026
Kontrollutvalgets egne utgifter til møteavvikling, kurs, m.v	116 000	**120.000**	124.000	128.000	132.000
Kjøp av sekretariatstjenester	349 000	**359.000**	370.000	381.000	393.000
Kjøp av revisjonstjenester	1 238 000	**1.263000**	1 289000	1315000	1 344000
Total ramme kontrollutvalget	1 703000	**1 742000**	1 783000	1 824000	1 869000

Vurdering
I kontrollarbeidssammenheng er de største postene kjøp av sekretariats- og revisjonstjenester; ellers inneholder budsjettet poster for kontrollutvalgets egen drift. Budsjettforslaget bygger på erfaring fra kontrollutvalgets egenaktivitet og tidligere regnskapstall. Antallet møter og evt. besøk ved kommunale avdelinger/institusjoner kan øke hvis konkrete saker eller problemstillinger oppstår. Budsjettforslaget tar ikke høyde for ekstraordinære ressursbehov i kontrollsammenheng. Kontrollutvalget legger fram et forslag til spesifisert budsjett for kontrollarbeidet. Kommunestyret fastsetter den totale rammen.

Vedlegg - Detaljbudsjett 2023 – Kontrollarbeidet Namsos kommune

Beskrivelse	2022	**2023**
Ledergodtgjørelse	16.000	**16.000**
Møtegodtgjørelse	31.000	**31.000**
Erstatning for tapt arbeidsfortjeneste	9.000	**8.000**
Arbeidsgiveravgift	3.000	**3.000**
Faglitteratur/tidsskrifter	6.000	**6.000**
Bevertning	5.000	**5.000**
Kursavgifter og oppholdsutgifter	35.000	**38 000**
Kjøregodtgjørelse	4.000	**5 000**
Reiseutgifter	7.000	**8 000**
Kjøp av tjenester fra KonSek Trøndelag IKS	349.000	**359 000**
Kjøp av tjenester fra Revisjon-Midt-Norge SA	1.238.000	**1 263 000**
Sum bevilgning - kontroll og tilsyn (funksjon 110)	*1.703.000*	**1 742 000**

Referatsaker august 22

Behandles i utvalg	Møtedato	Saknr
Kontrollutvalget i Namsos kommune	30.08.2022	27/22

Saksbehandler Einar Sandlund
Arkivkode FE-033, TI-&17
Arkivsaknr 22/146 - 3

Forslag til vedtak
Referatene tas til orientering

Vedlegg
Loven sier ikke noe om hva forslagsrett betyr
Møteoffentlighet – tidspunkt for møter i folkevalgte organer
Må velge hele utvalget på nytt
Retten til å signere er ikke regel om myndighet til å avgjøre
Må kommunale oppgavefellesskap lage årsregnskap
Avslag på etterlønn var ulovlig vedtak
Ytringsfriheten kan ikke begrenses mer for folkevalgte enn andre

Saksopplysninger
Det kan bli fremlagt ytterligere referater i møtet.

Vurdering
Referatene anbefales tatt til orientering

Loven sier ikke noe om hva «forslagsrett» betyr

Kommunal Rapport 13.06.2022, Jan Fridthjof Bernt, professor emeritus ved Universitetet i Bergen.

Kommunedirektøren har møte- og talerett, men ikke forslagsrett. Samtidig legger jo kommunedirektøren fram forslag til vedtak, hvordan skal man forstå dette?

SPØRSMÅL: Under møtet i kommunestyret fremsatte kommunedirektøren følgende forslag mens en sak var under behandling:

«Kommunestyret ber administrasjonen om å gjøre vurderinger knyttet til barnets beste i behandlingen av eventuell søknad om bytte av hovedmål til nynorsk i de tre kommende årene fra 2022/2023 gjeldende fra og med 5. til og med 7. trinn dette skoleår. For egen språkgruppe vil det kreves et minimum av 10 elever med enkeltvedtak om bytte av hovedmål til nynorsk.»

Dette ble vedtatt med 10 mot 9 stemmer (med ordførerens dobbeltstemme.)

Jeg viser til kommuneloven:
Kommuneloven §6–1: Ordføreren har **møte-, tale- og forslagsrett** i alle kommunale eller fylkeskommunale folkevalgte organer unntatt kommune- og fylkesråd og organer under dem. I kontrollutvalget har ordføreren likevel bare møte- og talerett.

Kommuneloven §13-1: Kommunedirektøren har **møte- og talerett** i alle kommunale eller fylkeskommunale folkevalgte organer, med unntak av kontrollutvalget. Kommunedirektøren kan la en av sine underordnede utøve denne retten på sine vegne.

Spørsmålene er da:
Har kommunedirektøren forslagsrett i et kommunestyremøte etter at saken det gjelder, er åpnet og tatt opp til behandling?

Hvis svaret er nei på dette spørsmålet; er vedtaket som er gjort, gyldig?

SVAR: Her er lovteksten i kommuneloven ufullstendig og unødig vanskelig å forstå for uinnvidde. Loven har ingen generelle bestemmelser om hvem som har forslagsrett og hva dette innebærer, bare de to særreglene som er gjengitt ovenfor. Disse er imidlertid unntak fra to etablerte ulovfestede prinsipper for saksbehandling i kollegiale organer:

(i) Hvis ikke annet er bestemt, kan bare medlemmer av organet delta under saksbehandlingen i organet – altså med møterett og talerett.

Møte- og talerett betyr rett til å til være til stede i møtet, og til å delta i debatten om de sakene som behandles der. Utgangspunktet er klart nok at dette har alle medlemmer av organet, og ingen andre. Men her utvider de to bestemmelsene kretsen av personer med slik rett, ved at både ordfører og kommunedirektør eller andre fra administrasjonen gis rett til å møte og delta i forhandlingene i *alle* folkevalgte organer i kommunen, med unntak av organer som inngår i parlamentarisk styringsform, og for kommunedirektøren heller ikke kontrollutvalget.

(ii) Loven sier ikke noe om hva «forslagsrett» betyr, og her kan det lett oppstå misforståelser, og også her må vi ta utgangspunkt i de generelle, ulovfestede, prinsippene om dette:
I et møte må alle som deltar med talerett, fritt kunne gi uttrykk for sitt syn på hva som bør gjøres og dermed også på hvilket vedtak som bør treffes. Det gjelder også kommunedirektøren, selv om hun ikke er gitt «forslagsrett».

Forslagsrett er her en særlig rett til å formulere et forslag til vedtak og kreve det tatt opp til votering. Denne retten har bare medlemmene av vedkommende folkevalgte organ, samt ordføreren.

Kommunedirektøren har ingen slik forslagsrett, verken før eller under møtet. Hun vil svært ofte legge fram sitt forslag til vedtak i sin innstilling i sakspapirene, men dette er ikke forslag som må tas opp til votering hvis ikke ordfører eller annet medlem av organet tar det opp og fremsetter det som sitt. Oftest vil ordføreren sette det fram til votering, men noen ganger vil hun kunne velge å fremsette et modifisert eller helt annet forslag, gjerne ut fra det som fremkommer av opplysninger og synspunkter under debatten.

Kommunedirektøren kan også under debatten om forslaget selv formulere et nytt forslag til vedtak for å se om det kan få tilslutning, men hvis ikke ordfører eller noen annen fremsetter det som sitt forslag, skal det ikke bli votert over dette. Hvis ordfører setter det under votering, vil det imidlertid bli oppfattet som godt nok, selv om ordfører ikke vil stemme for dette, men bare ønsker å få avklart om det er tilslutning til dette.

(iii) Hvis ordfører eller annet medlem fremsetter et forslag i saken som klart avviker fra det som er utredet av kommunedirektøren i saksforelegget til møtet, må kommunestyret ta stilling til om det anser dette alternativet som tilstrekkelig utredet, eller om det her er nødvendig med en ytterligere saksutredning til et senere møte før det treffes vedtak. Innenfor vide rammer er det kommunestyret selv som avgjør om det synes en sak er tilstrekkelig utredet, men hvis det viser seg at vedtaket er truffet på uriktige eller klart ufullstendige premisser når det gjelder saksforhold, konsekvenser eller rettsspørsmål, vil det kunne føre til at vedtaket var ugyldig, og saken må behandles på nytt i et senere møte.

§ 11-5: Møteoffentlighet – tidspunkt for møter i folkevalgte organer

Tolkningsuttalelse | Dato: 20.06.2022

Mottaker: Lillehammer kommune
Vår referanse: 22/4255-2

Spørsmål om møteoffentlighet - kan ulike møter i folkevalgte organer i kommunen avholdes på samme tidspunkt?
Vi viser til henvendelse 10. mai 2022 fra det politiske sekretariatet i Lillehammer kommune som spør om kommunen bryter reglene om møteoffentlighet når ulike politiske møter avholdes på samme tidspunkt. Bakgrunnen for henvendelsen er at sekretariatet har fått inn dette spørsmålet fra en som ikke får muligheten til å overvære alle de politiske møtene når de avholdes parallelt.

Departementets vurdering
Regelen om møteoffentlighet for folkevalgte organer i kommunen er tatt inn i kommuneloven § 11-5. Bestemmelsens første ledd lyder:

«Alle har rett til å være til stede i møter i folkevalgte organer dersom ikke noe annet følger av denne paragrafen».
Det følger av dette at allmennheten har rett til å være til stede når folkevalgte organer i kommunen har møter.
Spørsmålet er om denne retten medfører en plikt for kommunen til å avholde de politiske møtene til ulike tidspunkter, slik at innbyggerne får anledning til å følge alle møtene. Dette er ikke direkte regulert i kommuneloven. Ordlyden i kommuneloven § 11-5 oppstiller ikke en plikt for kommunen til å sørge for en slik koordinering av møtene i de folkevalgte organene. Problemstillingen er heller ikke berørt i forarbeidene til loven eller rettspraksis.

Etter departementets vurdering tilsier heller ikke reelle hensyn en slik utvidende tolkning. Departementet ser at det vil være uheldig for innbyggere som ønsker å følge flere møter når møtene avholdes samtidig. Disse får ikke anledning til å være til stede i alle møtene. Kommunen unnlater likevel ikke allmennheten innsikt og kontroll med de folkevalgtes virksomhet, selv om den enkelte ikke får fulgt alle møtene. Kommunen må ta mange hensyn når den planlegger møtene, og det vil ikke alltid være mulig å få møtekabalen til å gå opp uten at noen møter overlapper i tid.
Departementet kan derfor ikke se at det er holdepunkter for å tolke § 11-5 slik at den inneholder en plikt for kommunene til å holde møtene på ulike tidspunkter.
Selv om møter legges til samme tid, rokker ikke dette ved innbyggernes rett til å være til stede i møtene. Etter dette er departementets vurdering at det ikke er strid med kommuneloven § 11-5 om møteoffentlighet å avholde møter i ulike folkevalgte organer på samme tidspunkt.

Med hilsen
Siri Halvorsen (e.f.)
avdelingsdirektør

Ida Bakke Husom
seniorrådgiver

Må velge hele utvalget på nytt

Kommunal Rapport 20.06.2022, Jan Fridthjof Bernt, professor emeritus ved Universitetet i Bergen.

Hva gjør vi med medlemmer som ikke møter opp på møtene?

SPØRSMÅL: Vi har et kommunalt medvirkningsråd (ikke lovpålagt) som har sju medlemmer, der ett av de fem medlemmene fra brukerorganisasjonene aldri møter. Vedkommende melder ikke forfall til møtene, responderer ikke på innkallinger, og svarer ikke på våre henvendelser på telefon eller e-post. Rådet er opprettet med hjemmel i kommuneloven § 5–7.

Hvordan kan vi gå fram for å få valgt et nytt medlem til rådet uten at medlemmet søker fritak fra sitt verv?

SVAR: Medlemmer av utvalg etter § 5–7 velges av kommunestyret. Utvalget velges da som helhet etter reglene i lovens kapittel 7 og valget gjelder som utgangspunkt for hele – eventuelt resten av – valgperioden for kommunestyret. Det er ikke adgang til å foreta utskifting av enkeltmedlemmer annet enn ved vedtak av kommunestyret etter søknad om fritak fra medlemmet selv, se § 7–9 andre avsnitt.

Men hvis medlemmet mister sin valgbarhet, for eksempel ved utflytting fra kommunen, trer hun umiddelbart ut av vervet (§ 7–9 første setning), og det skal da velges et nytt medlem etter reglene i § 7–10 fjerde avsnitt.

I § 8–1 fastslås at den som velges, har plikt til å delta i organets møter hvis ikke hun har gyldig forfall. Manglende fremmøte kan anses som en tjenesteforsømmelse som vil kunne straffes etter straffeloven § 172 om «grovt uaktsomt tjenestefeil», eller § 173 bokstav a, om straff for «den som ved utøving av offentlig myndighet – mot bedre vitende grovt bryter sin tjenesteplikt».

Dette er imidlertid lite aktuelt i praksis, og vil i alle fall ikke medføre tap av vervet.

Hvis kommunestyret ønsker å skifte ut et medlem av et utvalg, må det derfor i tilfelle foreta et fullstendig nyvalg av hele utvalget, se § 5–7 siste avsnitt om adgang til å «omorganisere» utvalg. Valg skjer da etter reglene i §§ 7–4 til 7–7.

Ved et utvalg av den type det er her tale om, med medlemmer fra brukerorganisasjoner, vil jeg anta at man vil benytte avtalevalg etter § 7-7, men dette krever enstemmig vedtak i kommunestyret om å benytte denne valgformen. I motsatt fall må det benyttes forholdsvalg med lister etter reglene i §§ 7–4 og 7–5.

Retten til å signere er ikke regel om myndighet til å avgjøre

Kommunal Rapport 27.06.2022, Jan Fridthjof Bernt, professor emeritus ved Universitetet i Bergen.

Hvem bør signere på kommunens vegne?

SPØRSMÅL: Av kommunelovens § 6–1 fremgår det at ordføreren er rettslig representant for kommunen eller fylkeskommunen og underskriver på kommunens eller fylkeskommunens vegne hvis ikke myndigheten er tildelt andre.

Hvilke vurderinger bør en kommune legge til grunn for delegering/ikke delegering av hvem som skal være den rettslige representanten for kommunen?

Spørsmålet stilles blant annet ut fra at ordfører fort kan bli inhabil ved behandling av en sak dersom ordfører har signert en avtale som er i strid med politiske vedtak.

I tillegg kan det være utfordrende for en ny ordfører og forsvare en tidligere ordfører signering av avtaler som for eksempel bringes inn for domstolene.

SVAR: Bestemmelsen om hvem som underskriver på kommunens vegne, er ikke en regel om delegering av avgjørelsesmyndighet, men om hvem som er legitimert til å opptre på kommunens vegne når rette organ har truffet vedtak, med andre ord om når det er gitt en bindende meddelelse om kommunens vedtak i saken.

Signeringen av avtalen er da en rent formell handling, gjort etter at saken er ferdigbehandlet, og vil normalt bli foretatt av noen som ikke selv har noe ansvar for vedtaket.

Det er opp til kommunen hvem den vil tillegge denne funksjonen. Oftest vil det vel være kommunedirektøren eller lederen for vedkommende administrasjonsgren, men ved store og viktige avtaler, er det vel ganske vanlig at ordfører gjør dette.

Hvis det dokumentet som underskrives inneholder et vedtak eller en avtale som ikke stemmer med det som er vedtatt av det kompetente organ, får vi et spørsmål om kommunen likevel blir bundet av dette ut fra såkalte «legitimasjonsvirkninger» – om vern av den som i god tro har innrettet seg i tillit til det som står der.

Dette kan være en vanskelig problemstilling, og det sies ikke noe om dette her i loven.

Hvis det er tale om et rent privatrettslig forhold – som kjøp, salg, leie m.m. – er det nærliggende å bygge på det samme prinsipp som er formulert for kommunale foretak i § 9–18.

Her fastslås som utgangspunkt at «Hvis noen som representerer foretaket utad, har overskredet sin myndighet, blir en avtale eller annen privatrettslig disposisjon ikke bindende for kommunen eller fylkeskommunen». Men føyes så til: «Dette gjelder bare hvis den andre parten innså eller burde ha innsett at myndigheten ble overskredet, og at det derfor ville stride mot redelighet å gjøre disposisjonen gjeldende.»

Dette er i realiteten samme regel som vi finner for overskridelse av myndighet i aksjelovens § 6-33: «Har noen som representerer selskapet utad … ved disposisjon på selskapets vegne gått ut over sin myndighet, er disposisjonen ikke bindende for selskapet når selskapet godtgjør at medkontrahenten forsto eller burde ha forstått at myndigheten ble overskredet, og det ville stride mot redelighet å gjøre disposisjonen gjeldende».

Ved vedtak eller avtaler som også har offentligrettslig innhold, som tillatelser, dispensasjoner, godkjenningsvedtak m.m., må spørsmålet om legitimasjon avgjøres ut fra ulovfestede regler om når et forvaltningsvedtak blir ugyldig og til skade for en part som har vært i god tro.

Her er det stadig en viss usikkerhet om når en slik part kan vinne rett etter tilsagn i avtale eller vedtak, også fra noen som ikke hadde myndighet til å opptre på vegne av et offentlig organ. Men de beste grunner taler nok for at det her – på samme måte som ved rene saksbehandlingsfeil – må foretas en avveining av det motstående interesser, slik at borgeren også her må ha et visst vern mot at vedtaket blir opphevd på dette grunnlag.

Må kommunale oppgavefellesskap lage årsregnskap?

Kommunal Rapport 04.07.2022, Jan Fridthjof Bernt er professor emeritus ved Universitetet i Bergen.

SPØRSMÅL: Er det slik å forstå at et kommunalt oppgavefellesskap, som er eget rettssubjekt også skal utarbeide eget årsregnskap jf. § 14–6 i kommuneloven?

SVAR: I bestemmelsen i kommuneloven § 19–4 om samarbeidsavtalen mellom deltakere i et kommunalt oppgavefellesskap er det i tredje avsnitt fastsatt at det her skal angis om oppgavefellesskapet skal være eget rettssubjekt. Hvis det er angitt at det skal det være, betyr det at det er fullstendig atskilt fra deltakerkommunene, når det gjelder rettigheter og plikter, med unntak av ansvar for økonomiske forpliktelser.

Kommuneloven gjelder som alminnelig regel (§ 1-2) «for kommuners og fylkeskommuners virksomhet», noe som etter forarbeidene også omfatter «interkommunale samarbeid som er organisert etter regler i kommuneloven», og herunder også interkommunalt samarbeid som er «organisert som egne rettssubjekter», men bestemmelsen i § 14–6 gjelder tilsynelatende ikke for kommunale oppgavefellesskap, bare for «virksomhet som er en del av kommunen eller fylkeskommunen som rettssubjekt».

Dette vil, sies det i forarbeidene (NOU 2016:4, merknader til § 14-6) «for eksempel gjelde regnskaper … for kommunale oppgavefellesskap som *ikke* er egne rettssubjekter» (min utheving).

Men så er det med hjemmel i forskriftshjemmelen i siste avsnitt i § 14–6 fastsatt, i forskrift FOR-2019-06-07-714 om økonomiplan, årsbudsjett, årsregnskap og årsberetning for kommuner og fylkeskommuner mv., § 1–1 bokstav c, som generell regel at denne gjelder blant annet «årsregnskapet … til … kommunale oppgavefellesskap etter kommuneloven kapittel 19».

Og med denne litt underlige regelteknikken lander vi så vidt jeg kan forstå på at både § 14–6 og forskriften gjelder også for kommunale oppgavefellesskap som er egne rettssubjekter.

Avslag på etterlønn var ulovlig vedtak

KommunalRapport 01.08.2022, Jan Fridthjof Bernt er professor emeritus ved Universitetet i Bergen.

Kan kommunestyret innvilge fritak, men avslå etterlønn?

SPØRSMÅL: Jeg leser i Kommunal Rapport om en ordfører som søkte om fritak fra ordførervervet under forutsetning om innvilgelse av tre måneders etterlønn. Alternativt søkte han om fritak fra 1. august, med 1,5 måneders etterlønn.

Da kommunestyret skulle behandle saken, vedtok de å innvilge fritak fra ordførervervet for resten av valgperioden, men avslo – i strid med innstillingen fra kommunedirektøren – å gi noen etterlønn.

Kan kommunestyret gjøre dette?

SVAR: Fritak fra verv som folkevalgt kan etter kommuneloven § 7–9 andre avsnitt etter søknad gis til den som «ikke kan ivareta vervet sitt uten at det fører til vesentlig ulempe».

Kommunestyret har ingen plikt til å gi slikt fritak selv om lovens vilkår for dette er oppfylt, men om det skjer, er utgangspunktet søknaden om fritak fra den folkevalgte. Kommunestyret kan derfor ikke gi fritak med andre rammer eller annet innhold en det som er angitt der.

Hvis ikke dette er akseptabelt for kommunestyret, må de avslå søknaden og eventuelt be om en ny søknad som det kan innvilge.

Når ordfører her søker om slik etterlønn den første tiden etter at han fratrer, må det anses som en bindende forutsetning for søknaden, og vedtaket i kommunestyret må derfor anses som et avslag på denne.

Neste spørsmål bli så om kommunestyret hadde adgang til å avslå søknaden om etterlønn. Ut fra lovens ordlyd kan det se ut som om kommunestyret står fritt her. I kommuneloven § 8–8 første avsnitt står det at folkevalgte «som har vervet som sin hovedbeskjeftigelse, kan søke om ettergodtgjøring når de fratrer vervet».

Men i andre avsnitt omtales dette i en regel om avkorting som «Retten til ettergodtgjøring», og i forarbeidene fremgår det at det er slik loven skal forstås: Den folkevalgte må altså søke om etterlønn, men når det er gjort, har hun en rett til slik etter reglene i denne paragrafen.

Det betyr at kommunestyrets vedtak om fritak uten etterlønn var ulovlig, og søknad om fritak må behandles på nytt. I mellomtiden er utgangspunktet at når det ikke foreligger lovlig vedtak om fritak, er ordføreren fortsatt ordfører.

Men hvis ordfører rent faktisk har fratrådt på grunnlag av kommunestyrets vedtak, og ikke mottar godtgjøring fra kommunen etter dette, må han ha krav på etterlønn fra dette tidspunktet.

Slik godtgjøring vil han da ha krav på i alminnelig oppsigelsestid (tre måneder) hvis ikke annet er fastsatt i kommunal forskrift, se kommuneloven 8–6 første avsnitt andre setning.

Ytringsfriheten kan ikke begrenses mer for folkevalgte enn andre

KommunalRapport 08.08.2022, Jan Fridthjof Bernt er professor emeritus ved Universitetet i Bergen.

Kan formannskapet vedta hvordan en navngitt folkevalgt skal opptre?

SPØRSMÅL

Formannskapet har fattet vedtak om at en navngitt representant må forbedre sin opptreden på flere områder. Det gjelder blant annet måten vedkommende omtaler kommunen, vedtak og hvordan administrasjonen utfører vedtakene på. Kritikk er greit, heter det, men «må likevel gjøres uten personangrep, uthenging på sosiale medier eller direkte usannheter».

Er dette noe et formannskap kan vedta?

SVAR

Som alminnelig utgangspunkt har folkevalgte i en kommune stor frihet med hensyn til hva de vil uttale seg om, og herunder rette kritikk mot både administrasjon og folkevalgte, så lenge det er tale om saker eller forhold som har tilknytning til kommunens virksomhet.

Det kan ikke settes grenser for denne ytringsfriheten for folkevalgte ut over det som gjelder for alle andre, i praksis i første rekke brudd på lovfestet taushetsplikt (se særlig forvaltningsloven § 13) eller erstatningsansvar for ærekrenkende utsagn (skadeserstatningsloven § 3–6 a).

Brudd på lovfestede begrensninger i ytringsfriheten kan i tilfelle bare påtales i straffesak eller ved privat søksmål for domstolene fra den som er ærekrenket. Verken kommunedirektør, ordfører, formannskap eller kommunestyr kan pålegge folkevalgte å avstå fra kritiske ytringer.

Dette gjelder både i og utenfor møter i folkevalgte organer, men hvis det i et møte fremkommer ytringer som er ærekrenkende eller brudd på lovfestet taushetsplikt, skal møteleder gjøre oppmerksom på dette og anmode den folkevalgte om å avstå fra slike.

Ellers står det som rettslig utgangspunkt ethvert medlem av folkevalgt organ fritt å gi uttrykk for sin kritikk mot forhold i kommunen, og mot organer og enkeltpersoner – folkevalgte og tilsatte. Men da må hun selvsagt være forberedt på at det tas til motmæle mot slik kritikk, i eller utenfor møte.

Dette kan skje ved innlegg i møte eller ytringer i offentlig debatt, ved kommentar fra ordfører eller leder av folkevalgt organ. Unntaksvis kan det skje ved vedtak i folkevalgt organ, der dette avviser påstander eller vurderinger fremsatt av en folkevalgt i mediene eller annen offentlig debatt.

Ved motinnlegg fra administrasjon til diskusjonen om hva som er gjort eller som burde gjøres, vil det gjerne være riktig å imøtegå både den beskrivelse som er gitt av faktiske forhold, og skjønnsmessige vurderinger av fremtidig utvikling ved ulike handlingsalternativer.

Det kan også være behov for å imøtegå kritikk av enkeltpersoner – folkevalgte eller tilsatte – men svaret må forholde seg til saksforholdet i den fremsatte kritikken, ikke til kritikerens person.

Slik imøtegåelse av kritikk må også kunne skje i form av et vedtak i et folkevalgt organ, men også her er det viktig at vedtaket retter seg mot sak eller generelle saksforhold, og ikke får form av en generell karakteristikk av en enkelt folkevalgt. Det må således ligge utenfor et formannskaps kompetanse å uttale at man ber et navngitt medlem «forbedre sin opptreden».

Det som derimot må være helt greit, er at et formannskap vedtar en generell uttalelse der man etter å ha fastslått at «*Kritisk omtale av kommunen, politiske vedtak og administrativ utførelse av vedtak er en selvsagt del av en folkevalgts ombudsrolle*», legger til at «*Dette må likevel gjøres uten personangrep, uthenging på sosiale medier eller direkte usannheter*.»

Dette siste er imidlertid en skjønnsmessig etisk norm som ikke lar seg håndheve, men som er et godt prinsipielt utgangspunkt for kritikk og debatt om hva som forsvarlig opptreden.

Det bør vel føyes til at når det er tale om kritikk av navngitte folkevalgte, må terskelen for hva som kan aksepteres, være en god del høyere enn der slike angrep rettes mot tilsatte i kommunen.

Det er derfor helt på sin plass om formannskapet uttaler:

«*Som folkevalgt må arbeidsgiverrollen tas på alvor. Det innebærer at administrativ kritikk må fremmes imot kommunedirektøren, ikke mot andre enkeltansatte*.»

Alle tilsatte i kommunen handler på vegne av kommunedirektøren og er underlagt hennes instruksjonsmyndighet og kontroll, se kommuneloven § 13–1, der det fastslås at «*Kommunedirektøren skal lede den samlede kommunale eller fylkeskommunale administrasjonen*».

Se også siste avsnitt, der det nå er fastslått at «*Kommunedirektøren har det løpende personalansvaret for den enkelte, inkludert ansettelse, oppsigelse, suspensjon, avskjed og andre tjenstlige reaksjoner, hvis ikke annet er fastsatt i lov*».

Kritikk av tilsattes saksbehandling og ivaretakelse av andre funksjoner må dermed rettes til direktøren, også der utgangspunktet for denne er svikt fra en underordnet tilsatt – slik det jo oftest er. «Kommunestyret kjenner kun kommunedirektøren.»

Godkjenning av protokoll

Behandles i utvalg	Møtedato	Saknr
Kontrollutvalget i Namsos kommune	30.08.2022	28/22

Saksbehandler Einar Sandlund
Arkivkode FE-033, TI-&17
Arkivsaknr 22/146 - 2

Forslag til vedtak:
Protokollen godkjennes

Saksopplysninger:
Protokollen godkjennes i møtet.

Vurdering
Protokollen anbefales godkjent