

Behandling av rapport fra forvaltningsrevisjon - informasjonssikkerhet

Behandles i utvalg	Møtedato	Saknr
Kontrollutvalget i Malvik kommune	14.10.2026	51/26
Saksbehandler	Ragnhild Torsdatter Grønvold	
Arkivkode	FE-217	
	TI-&58	
Arkivsaknr	25/357 - 7	

Forslag til vedtak

1. Kontrollutvalget tar rapporten om informasjonssikkerhet og personvern i Malvik kommune til orientering.

2. Kontrollutvalget anbefaler kommunestyret å vedta følgende:

Kommunedirektøren skal

- a) beskrive og implementere en sikkerhetsstrategi som viser hvordan kommunen skal nå vedtatte sikkerhetsmål
- b) sørge for at kommunestyret mottar rapportering om personvernombudets virksomhet og om VarITs virksomhet i samsvar med inngåtte avtaler
- c) utarbeide og ajourføre behandlingsprotokoller, databehandleravtaler og personvernkonsekvensvurderinger (DPIA)
- d) legge til rette for opplæring i informasjonssikkerhet og personvern, herunder KI, og følge opp de ansattes gjennomføring av opplæringen
- e) avklare roller og ansvar i samarbeidet med VarIT

3. Kontrollutvalget ber kommunedirektøren rapportere skriftlig til kontrollutvalget om oppfølgingen av kommunestyrets vedtak innen 1. april 2027

Vedlegg

Rapport - Informasjonssikkerhet og personvern

Kommunedirektørens uttalelse til endelig rapport - forvaltningsrevisjon informasjonssikkerhet

Saksopplysninger

Bakgrunn

Kontrollutvalget vedtok i sak 54/25 å bestille en forvaltningsrevisjon om informasjonssikkerhet og personvern. Prosjektplanen ble godkjent i sak 3/26. Bakgrunnen for bestillingen var behovet for å undersøke om kommunen har etablert et styringssystem som sikrer etterlevelse av krav til informasjonssikkerhet og personvern, og om samarbeidet med Værnesregionen IKT (VarIT) gir tilfredsstillende ivaretagelse av organisatoriske og tekniske sikkerhetstiltak.

Problemstillinger

1) Har Malvik kommune etablert et styringssystem for informasjonssikkerhet og personvern som tilfredsstiller krav i regelverket (systematisk rammeverk)?

2) Har Malvik kommune etablert tilfredsstillende avtaler med og oppfølging av VarIT (Stjørdal kommune), som sikrer organisatoriske og tekniske tiltak for informasjonssikkerhet og personvern?

Revisor har laget revisjonskriterier for å vurdere de to problemstillingene, se grunnlag for disse i vedlegg 1.

Om rapporten

Rapporten Informasjonssikkerhet og personvern ert utarbeidet av Revisjon Midt-Norge SA på oppdrag fra kontrollutvalget. Revisjonen er gjennomført i perioden februar 2025 til september 2026. Rapporten bygger på dokumentgjennomgang, intervjuer, gjennomgang av systemene Compilo og Drafit samt innhentet informasjon fra kommunen og VarIT.

Hovedfunn

For den første problemstillingen konkluderer revisor med at kommunen i hovedsak har etablert et styringssystem som ivaretar kravene i regelverket. Kommunen har beskrevet sikkerhetsmål og sikkerhetsorganisasjon, og informasjonssikkerhet og personvern inngår i kommunens internkontroll. Samtidig mangler styringssystemet en beskrivelse av sikkerhetsstrategi.

Revisjonen viser videre at kommunen har etablert rutiner og systemer for personvernarbeidet, men at etterlevelsen varierer. Arbeidet med behandlingsprotokoller, databehandleravtaler og personvernkonsekvensvurderinger (DPIA) er ikke fullt ut gjennomført og ajourført.

Kommunen har også gjennomført flere opplæringstiltak innen informasjonssikkerhet, personvern og bruk av kunstig intelligens. Revisor peker imidlertid på at kommunen i liten grad følger opp om ansatte faktisk gjennomfører opplæringen.

For den andre problemstillingen konkluderer revisor med at kommunen i all hovedsak har etablert avtaler og samhandling med VarIT som bidrar til å ivareta organisatoriske og tekniske sikkerhetstiltak. Det er etablert faste samarbeidsarenaer, og grunnprinsippene for sikkerhetsstyring er i hovedsak ivaretatt.

Samtidig avdekkes enkelte mangler. Det er ikke utarbeidet virksomhetsplan med mål og resultatkrav slik vertskommuneavtalen forutsetter. Videre skjer ikke rapportering fra vertskommunen til kommunestyret i samsvar med avtalens bestemmelser. Revisor peker også på behov for tydeligere ansvarsavklaringer mellom kommunen og VarIT, særlig knyttet til operasjonell teknologi samt håndtering, gjenoppretting og læring etter sikkerhetshendelser.

Funn som ikke er omtalt i revisors vurderinger

I rapporten beskrives det at personvernombudet i liten grad har en formalisert kontakt med personvernkontaktene, og at personvernkontaktordningen fortsatt er i en innførings- og modningsfase. Revisor omtaler dette i vurderingene, men uten å knytte forholdet til en anbefaling.

Revisor peker på at personvernombudet har 50 prosent stillingsressurs fordelt på seks kommuner, og stiller spørsmål ved om ressursen er tilstrekkelig etter at Malvik kommune ble del av samarbeidet. Revisor vurderer likevel revisjonskriteriet som i hovedsak oppfylt. Rapporten gir ikke grunnlag for å konkludere med at ressursnivået er uforsvarlig, men forholdet bør følges med på gjennom kommunens egen oppfølging av personvernarbeidet.

Revisors anbefalinger

Med bakgrunn i vurderinger og konklusjoner anbefaler revisor kommunedirektøren å:

- Beskrive sikkerhetsstrategi for å nå sikkerhetsmålene
- Sørge for at kommunestyret får avtalt rapportering om personvernombudet og VarITs virksomhet
- Utarbeide og ajourføre behandlingsprotokoller, databehandleravtaler og konsekvensvurderinger for personvern (DPIA)
- Følge opp ansattes opplæring og informasjon om informasjonssikkerhet og personvern
- Avklare uklarheter i roller og ansvar i samarbeidet med VarIT

Kommunedirektørens uttalelse

Kommunedirektøren uttalte seg til foreløpig rapport den 7. september 2026. Revisjonens funn tas til etterretning, heter det, samtidig som det vises til hvordan en allerede har til hensikt å følge opp det manglene revisjonen har funnet. Det er også presisert at det ikke kan settes en eksakt sluttdato for når arbeidet med informasjonssikkerhet og personvern kan avsluttes. Det er vist til at dette er kontinuerlige prosesser som krever vedvarende oppfølging. Uttalelsen er vedlegg 2 til rapporten. Uttalelsen førte ikke til endringer i den endelige rapporten. Den endelige rapporten er forelagt kommunedirektøren, som ikke hadde ytterligere å tilføye.

Sekretariatets vurderinger

Sekretariatet vurderer at rapporten besvarer begge problemstillingene som kontrollutvalget har bestilt undersøkt. Revisjonskriteriene er tydelige, og det er en klar sammenheng mellom problemstillingene, revisors funn, vurderinger, konklusjoner og anbefalinger.

Rapporten viser at kommunen de senere årene har gjennomført et omfattende arbeid for å etablere et systematisk rammeverk for informasjonssikkerhet og personvern. Revisor konkluderer med at styringssystemet i hovedsak tilfredsstiller kravene i regelverket. Samtidig viser rapporten at det fortsatt er svakheter i den praktiske oppfølgingen av personvernregelverket, særlig når det gjelder behandlingsprotokoller, databehandleravtaler og personvernkonsjekvensvurderinger.

Sekretariatet mener at revisors anbefaling om å utarbeide en sikkerhetsstrategi er viktig. En sikkerhetsstrategi vil tydeliggjøre hvordan kommunen skal nå vedtatte sikkerhetsmål og bidra til en mer helhetlig styring av arbeidet.

Når det gjelder samarbeidet med VarIT, viser rapporten at kommunen har fått et sterkere fagmiljø og bedre grunnlag for sikker drift. Samtidig framkommer det at enkelte formelle krav i samarbeidsavtalen ikke er oppfylt. Sekretariatet mener det er viktig at kommunen følger opp manglende virksomhetsplan og rapportering til kommunestyret, slik at kommunestyret får nødvendig informasjon om virksomheten i samarbeidstjenesten.

Sekretariatet vurderer videre at funnene om uklare roller og ansvar mellom kommunen og VarIT, særlig innen operasjonell teknologi og håndtering av sikkerhetshendelser, er fanget opp gjennom revisors anbefaling om å avklare roller og ansvar i samarbeidet.

På denne bakgrunn anbefaler sekretariatet at kontrollutvalget tar rapporten til orientering og sender saken videre til kommunestyret med forslag om å følge opp revisors anbefalinger.