Forvaltningsrevisjonsrapport - Informasjonssikkerhet og personvern

Behandles i utvalg	Møtedato	Saknr
Kontrollutvalget i Overhalla kommune	10.06.2026	16/26

Saksbehandler	Einar Sandlund
Arkivkode	FE-217 TI-&58
Arkivsaknr	25/213 - 10

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

1) *Kommunestyret tar forvaltningsrevisjonsrapporten Informasjonssikkerhet og personvern til orientering.*
2) Kommunestyret ber kommunedirektøren iverksette en gjennomgang av styringssystemet for informasjonssikkerhet og personvern i kommunen som omfatter::
• Gjennomgang og revidering av styrende dokumenter, som involverer organisasjonen
• Vurdering av personvernfunksjonen med tanke på uavhengighet og ressurstilgang
• Vurdering av behov for rutiner og prosedyrer knyttet til behandlingsprotokoller databehandleravtaler og vurdering av personvernkonsekvense
• Utarbeiding av systematisk opplæring i informasjonssikkerhet og personvern, som også omfatter bruk av KI
- *Ta initiativ til gjennomgang og revidering av alle avtaler med vertskommunen som gjelder tekniske og organisatoriske tiltak for informasjonssikkerhet og personvern.*

3) Kommunestyret ber kommunedirektøren innen 01.08.27 om skriftlig rapport til kontrollutvalget på hvordan forholdene i pkt. 2 er fulgt opp

Vedlegg
Rapport fra forvaltningsrevisjon - informasjonssikkerhet og personvern

Saksopplysninger
Kommunelovens § 23-3 sier at det skal gjennomføres forvaltningsrevisjon i kommunen.
Kontrollutvalget fattet slikt vedtak i sak 25/25:
1. Kontrollutvalget bestiller forvaltningsrevisjon av informasjonssikkerhet og digitalisering.
2. Det gis følgende innspill til prosjektplanen:
☐Ledelsens styringssystem for informasjonssikkerhet og personvern, grensesnittet mot Namsos og avklaring av ansvaret mellom de to kommunene.
☐Tekniske og organisatoriske tiltak
1. Revisjonen bes utarbeide prosjektplan til kontrollutvalgets møte den 11.11.25

Kontrollutvalget godkjente prosjektplanen i sak 17/25 med slikt vedtak:
1. Prosjektplan datert 24.11.25 godkjennes med slike endringer:
- Rapporten skal vise et sikret bilde av kommunens ansatte sin bevissthet og holdning for å sikre informasjonssikkerheten og personvernet
2. Rapporten forventes levert sekretariatet 15.05.26 innenfor den angitte ressursbruk på 300 timer.
3. Kontrollutvalget bes å bli orientert underveis for å kunne ta stilling til evt. behov for endringer i problemstillinger og prosjektplanen.

Endelig rapport ble oversendt 11.05.26. Rapporten besvarer følgende problemstillinger, jfr. vedtatt prosjektplan:
1) Har Overhalla kommune etablert et styringssystem for informasjonssikkerhet og personvern som tilfredsstiller kravene i regelverket (systematisk rammeverk)?
2) Har Overhalla kommune etablert tilfredsstillende avtaler med og oppfølging av Namsos kommune (vertskommunen), som sikrer organisatoriske og tekniske tiltak for informasjonssikkerhet og personvern?

Avgrensning og presisering av undersøkelsen er beskrevet i kap. 1.3 og 1.4. Nærmere beskrivelse og vurdering av metodene er beskrevet i kap. 1.5.
Revisor har innhentet data gjennom intervjuer og dokumentgjennomgang. Revisor vurderer at det samlet sett gir nok faktagrunnlag for vurderingene i rapporten.

Kommunedirektøren har avgitt høringssvar 05.05.26, jfr. rapportens vedlegg 2.
Revisor har ut fra høringssvaret gjort mindre endringer i rapporten. Dette er nærmere beskrevet i kap. 1.6.

Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket?

Ledelsessystem for informasjonsikkerhet
Revisor har gjort slike vurderinger:

- *Kommunen har dokumentert et ledelsessystem for informasjonssikkerhet og personvern,*
  men revisor stiller spørsmål ved hvor oppdatert det er, om det holdes levende, og forankringen i organisasjonen
- *Kommunens ledelsessystem inneholder sikkerhetsmål om å sikre konfidensialitet, integritet*
  og tilgjengelighet. Revisor viser til vurderingen ovenfor, vurderer at sikkerhetsmålene er lite
  kjent i organisasjonen.
- *Kommunens ledelsessystem har delvis beskrevet hvordan sikkerhetsmålene skal nås*
  (sikkerhetsstrategi).
- *Kommunen har et ledelsessystem som delvis beskriver en sikkerhetsorganisasjon.*

Revisors overordna konklusjon på den første problemstillingen er at Overhalla kommune har etablert sentrale elementer i et styringssystem for informasjonssikkerhet og personvern.

Informasjonssikkerhet i systemet for internkontroll
Revisor har gjort slike vurderinger:

- *Kommunens internkontrollsystem, Compilo, inneholder regelverk, prosedyrer og rutiner for*
  *informasjonssikkerhet, men det kan være mangelfull*t.
- *Kommunen har nylig vedtatt helhetlig ROS-analyse, hvor flere elementer som vedrører*
  *informasjonssikkerhet og personvern er tatt inn. Kommunen gjennomfører delvis risikovurderinger, inklusive personvernkonsekvenser(DPIA-*er).
- *Kommunen har informasjonssikkerhet og personvern som egen avvikskategori i Compilo.*
  Det meldes få avvik innen denne avvikskategorien. Revisor registrerer at informantene tror at avvik innen informasjonssikkerhet og personvern er underrapportert.

Personvern
Revisor har gjort slike vurderinger:

- *Kommunen har personvernombud som langt på veg støtter den behandlingsansvarlige i å oppfylle pliktene i kommunen etter personvernregelverket, men denne har ikke definerte ressurser til å utføre funksjonen og. tilnærming til rollen er ikke nødvendigvis risikobasert.*
- *Kommunen har et system for (regneark) for behandlingsprotokoller som delvis er fulgt opp, men disse mangler obligatorisk informasjon på mange av kategoriene.*
- *Kommunen har langt på veg praksis for å inngå databehandleravtaler, men det er uklart om kommunen har et system for dette.*
- *Kommunen har langt på veg praksis for å gjennomføre vcurdering av DPIA-er, men kommunen har i varierende grad system for dette. Etter revisors vurdering er det i stor grad praksis i organisasjonen med å gjennomføre DPIA er, men med unntak av helse, er det i varierende grad skriftlige rutiner og maler for dette.*

Opplæring i informasjonssikkerhet og personvern

Revisor har gjort slike vurderinger:

- *Kommunen har delvis sørget for opplæring i informasjonssikkerhet og personvern for ledere og ansatte.*
- *Kommunen har en enkel policy, som er under utvikling, for bruk av kunstig intelligens(KI). KI bukes til ulike oppgaver, men det er uklart om ansatte har fått opplæring eller informasjon utover sikkerhetsinstruksen og dokumentet som heter Bruk av KI.*

Har Overhalla kommune etablert tilfredsstillende avtaler med og oppfølging av Namsos kommune (vertskommune), som sikrer organisatoriske og tekniske tiltak for informasjonssikkerhet og personvern?

Samarbeidsavtalen

Revisor har gjort slike vurderinger:

- *Det ble inngått en skriftlig samarbeidsavtale mellom Overhalla kommune og Namsos kommune senest i 2019. Revisors vurdering er at samarbeidsavtalen mellom Overhalla kommune og vertskommunen ikke er oppdatert etter gjeldende regelverk og sikkerhetsbehov*
- *beskriver ikke selve samarbeidsavtalen hvilke oppgaver og myndighet vertskommunen har for å sikre informasjonssikkerhet og personvern, Den viser til leveranseavtale, som er vedlegg til samarbeidsavtalen.*
- *følges ikke samarbeidsavtalen opp med rapportering og samhandling som systematisk ivaretar informasjonssikkerhet og personvern.*

Leveranseavtalen

Revisor har gjort slike vurderinger:

- *ivaretar leveranseavtalen delvis tekniske og organisatoriske tiltak for informasjonssikkerhet og personvern. Leveranseavtalen har ikke blitt oppdatert etter 2019, da den ble revidert sammen med samarbeidsavtalen. Det er ikke betryggende at vertskommunens IT-tjeneste knapt nok kjenner til avtalen.*
- *framstår samarbeidet om tekniske og organisatoriske sikkerhetstiltak med liten grad av systematikk og dokumentasjon.*
- *ivaretar leveranseavtalen delvis oversikt enheter, programvare og tilganger, men tjenestene som utføres for Overhalla kommune, er ikke forankret i avtalen.*

- *berører leveranseavtalen i liten grad sikkerhet i anskaffelser, IKT arkitektur og sikkerhetsoppdateringer (beskytte og oppdatere).*
- *inneholder leveranseavtalen kontroll av viktige sikkerhetstilstander ved at det er satt opp brannmurer for hovednett og gjestenett, og at årlig vedlikehold av brannmur, antivirus og sikkerhetsløsning inngår i avtalen. Utskifting av brannmur inngår i en utskiftingsplan*
- *inneholder leveranseavtalen ikke beskrivelse av håndtering, gjenoppretting og læring av hendelser (håndtering og gjenoppretting).*

Databehandleravtale

- *Revisor vurderer at kommunen har databehandleravtale med vertskommunen, men vtalen, framstår ikke og avtalens vedlegg, oppdatert i tråd med hva Overhalla kommune har etterlyst av behov.*

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

Rapporten viser at kommunen opp mot krav i lovverket har på plass en del sentrale elementer i styringssystemet for informasjonssikkerhet og personvern. Sekretariatet viser allikevel til revisor vurdering at sikkerhetsmålene kan være lite kjent blant ansatte og at det er en oppfatning at avvik innen personvern og informasjonssikkerhet kan være underrapportert. Videre er personvernombudets organisering, rolle, ansvar og ressurser viktig for å ivareta for utførelsen av kommunens tjenester. Utviklingen og endringene innen informasjonssikkerhet og personvern skjer hurtig og gir store utfordringer.

Sekretariatet vil peke på vertskommunesamarbeidet med Namsos på IKT, informasjonssikkerhet og personvern var et vesentlig moment for kontrollutvalget i forvaltningsrevisjonsprosjektet.

Rapporten viser at det etter sekretariatets oppfatning her er flere moment som det bør tas tak i. Blant annet gjelder dette samarbeidsavtalen som revisor vurderer trenger oppdatering og oppfølging av selve avtalen med systematisk rapportering og samhandling for å ivareta informasjonssikkerheten og personvernet. Sekretariatet vil også peke på at det er flere forhold i leveranseavtalen som revisor vurderer kan bli bedre, blant annet tjenester, systematikk og dokumentasjon.

Sekretariatet vil ut fra et helhetlig syn peke spesielt på følgende av revisors vurderinger og oppfølgingen av disse:
- *Kommunen har informasjonssikkerhet og personvern som egen avvikskategori i Compilo. Det meldes få avvik innen denne avvikskategorien.*
- *Personvernombudets rolle og ressurser*
- *Opplæring og informasjon bruk av KI*
- *Samarbeidsavtalen med Namsos*
- *Leveranseavtalen med Namsos.*

Kontrollutvalget anbefales å slutte seg til den fremlagte rapport. Saken anbefales videre oversendt kommunestyret med innstilling på å ta forvaltningsrevisjonsrapporten til orientering, samt å be kommunedirektøren følge opp rapportens anbefalinger i innstillingens pkt. 2.

Kommunestyret anbefales til slutt å be kommunedirektøren innen 01.08.27 gi skriftlig rapport til kontrollutvalget på hvordan anbefalingene er fulgt opp.