RM Revisjon Midt-Norge

Informasjonssikkerhet og personvern

Malvik kommune

Forvaltningsrevisjon



2026

FR1374

FORORD

Revisjon Midt-Norge SA gjennomfører denne forvaltningsrevisjonen på oppdrag fra Malvik kommunes kontrollutvalg i perioden februar 2025 til september 2026.

Vi vil takke alle som har bidratt med informasjon og tilrettelegging for intervjuavtaler og tilgang til system og styrende dokument.

Alle rapporter fra Revisjon Midt-Norge SA publiseres på www.revisjonmidtnorge.no.

Trondheim, 08.09.2026

Anna Ølnes

Oppdragsansvarlig forvaltningsrevisor

Anne Grete Wold

Prosjektmedarbeider

SAMMENDRAG

Med bakgrunn i bestilling fra kontrollutvalget i sak 54/25 og godkjent prosjektplan i sak 3/26, er forvaltningsrevisjonen gjennomført med utgangspunkt i følgende 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?

I den **første problemstillingen** konkluderer revisor med at Malvik kommune i hovedsak har etablert et styringssystem som ivaretar krav i regelverket. Systemet har beskrivelse av sikkerhetsmål og sikkerhetsorganisasjon, men mangler beskrivelse av sikkerhetsstrategi. Informasjonssikkerhet og personvern inngår i kommunens internkontroll. Revisor konkluderer med at regelverket for personopplysninger i varierende grad er fulgt opp, med tanke på behandlingsprotokoller, personvernkonsekvensutredninger og databehandleravtaler.

Kommunen har opplæringstiltak i informasjonssikkerhet og personvern, herunder bruk av KI, men ansattes gjennomføring følges i liten grad opp.

I den **andre problemstilling** konkluderer revisor med Malvik kommune i all hovedsak har etablert avtaler med og oppfølging av VarIT som bidrar til å sikre organisatoriske og tekniske tiltak for informasjonssikkerhet og personvern. Samarbeidet er regulert gjennom vertskommuneavtaler, og det er etablert faste arenaer for samhandling mellom kommunen og VarIT. Revisjonen viser også at grunnprinsipper for sikkerhetsstyring i hovedsak er ivaretatt gjennom samarbeidet.

Samtidig avdekker revisjonen enkelte mangler i kommunens oppfølging av samarbeidet. Det er ikke utarbeidet virksomhetsplan med mål og resultatkrav slik avtalen forutsetter, og rapportering til kommunestyret skjer ikke i samsvar med avtalens bestemmelser. Videre gjenstår det arbeid med å avklare ansvar for overvåking av operasjonell teknologi og med å styrke arbeidet knyttet til håndtering, gjenoppretting og læring etter sikkerhetshendelser.

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

I første kapittel redegjør revisor for kontrollutvalgets bestilling, I tillegg gir revisor en kort, overordna innføring i temaet og begreper. Her beskriver revisor også Malvik kommunes organisering av ansvar og oppgaver for informasjonssikkerhet og personvern.

I samme kapittel redegjør revisor for metoder som er brukt for å samle inn og analysere dataene (informasjonsgrunnlaget) som ligger til grunn for vurderinger, konklusjoner og anbefalinger.

I kapittel 2 presenterer revisor utledede revisjonskriterier data og vurderinger knyttet til den første problemstillinger. I kapittel 3 presenteres utledede revisjonskriterier, data og vurderinger for den andre problemstillingen.

I vedlegg 1 presenteres en mer fullstendig utledning av revisjonskriteriene som er brukt i forvaltningsrevisjonen.

En foreløpig rapport har vært sendt til kommunedirektøren for uttalelse. Kommunedirektørens skriftlige uttalelse er lagt ved rapporten i vedlegg 2.

INNHOLDSFORTEGNELSE

FORORD 2
SAMMENDRAG 3
INNHOLDSFORTEGNELSE 5
1 INNLEDNING 7
1.1 Bestilling 7
1.2 Problemstillinger 7
1.2.1 Avgrensing 7
1.3 Om temaet 7
1.4 Kommunens organisering 11
1.5 Metode 12
1.5.1 Oppstartsmøte 12
1.5.2 Intervju 12
1.5.3 E-poster med spørsmål 13
1.5.4 System– og dokumentgjennomgang 13
1.5.5 Vurdering av metode 13
1.6 Uttalelse om rapport 14
1.7 Begrepsavklaringer 14
2 STYRINGSSYSTEM 16
2.1 Problemstilling 16
2.2 Sikkerhetsmål, -strategi og -organisering 16
2.2.1 Revisjonskriterier 16
2.2.2 Funn 16
2.2.3 Revisors vurdering 20
2.3 Internkontroll 20
2.3.1 Revisjonskriterier 20
2.3.2 Funn 21
2.3.3 Revisors vurdering 23
2.4 Personvern 24
2.4.1 Revisjonskriterier 24
2.4.2 Funn 25
2.4.3 Revisors vurdering 29
2.5 Opplæring og informasjon 31
2.5.1 Revisjonskriterium 31
2.5.2 Funn 31
2.5.3 Revisors vurdering 34
3 VERTSKOMMUNESAMARBEID 35
3.1 Problemstilling 35
3.2 Avtaler med vertskommunen 35
3.2.1 Revisjonskriterier 35
3.2.2 Funn 35
3.2.3 Revisors vurdering 39
3.3 Vertskommunesamarbeid om organisatoriske og tekniske tiltak 40
3.3.1 Revisjonskriterier 40
3.3.2 Funn 40
3.3.3 Revisors vurdering 45
4 KONKLUSJONER OG ANBEFALINGER 47

4.1 Konklusjon 47
4.2 Anbefalinger.....47
Kilder.....49
VEDLEGG 1 – UTLEDNING AV REVISJONSKRITERIER 50
VEDLEGG 2 – UTTALELSE.....60

Figurer

Figur 1. Sammenhengen mellom informasjonssikkerhet og personvern. 9
Figur 2. Beskyttelsesbehov for personvern og informasjonssikkerhet.....10
Figur 3. Styringssystem for informasjonssikkerhet, Malvik kommune. 17
Figur 4. Kommunens styrende dokumenter i informasjonssikkerhet og personvern. 18
Figur 5. Prosedyre for vurdering av personvernkonsekvenser (DPIA). 28

1 INNLEDNING

1.1 Bestilling

Revisjon Midt-Norge mottok i brev fra kontrollutvalgets sekretariat, datert 09.12.2025, bestilling av forvaltningsrevisjon om informasjonssikkerhet. Bestillingen ble vedtatt i kontrollutvalgets møte den 03.12.2025, sak 54/25.

Revisor la fram prosjektplan med forslag til innretting i kontrollutvalgets møte den 11.02.2026, sak 3/26. Kontrollutvalget sluttet seg til prosjektplanen. Forvaltningsrevisjonen er gjennomført i tråd med den godkjente prosjektplanen.

1.2 Problemstillinger

Forvaltningsrevisjonen er gjennomført med utgangspunkt i følgende problemstillinger:

3) Har Malvik kommune etablert et styringssystem for informasjonssikkerhet og personvern som tilfredsstiller krav i regelverket (systematisk rammeverk)?
4) Har Malvik kommune etablert tilfredsstillende avtaler med og oppfølging av VarIT (Stjørdal kommune), som sikrer organisatoriske og tekniske tiltak for informasjonssikkerhet og personvern?

De to problemstillingene er belyst i kapittel 3 og 4.

1.2.1 Avgrensing

Vi har avgrenset forvaltningsrevisjonen mot digitalisering, som er å ta i bruk teknologi til å forbedre, forenkle og fornye. Det handler om å tilby nye og bedre tjenester som legger til rette for økt verdiskaping og innovasjon.[1] Informasjonssikkerhet og personvern er også viktig i utviklings- og forbedringsarbeid, men digitalisering er et så stort tema i seg selv, at vi i forståelse med kontrollutvalget har holdt det utenfor. Når det gjelder problemstilling om vertskommunesamarbeid, har vi ikke gått i dybden på organisatoriske og tekniske sikkerhetstiltak.

1.3 Om temaet

I dette kapittelet redegjør revisor for hva informasjonssikkerhet og personvern er.

Informasjonssikkerhet og informasjonsverdier

Informasjonssikkerhet handler om å verne alle typer informasjon. Eksempler på informasjonsverdier er data (digital og fysisk informasjon), fysisk IT-utstyr og infrastruktur, systemer, konfigureringer, programvare, applikasjoner og til og med menneskelige ressurser

[1] https://www.sintef.no/fagomrader/digitalisering/

(Jøsang 2025). Ulike typer informasjon vil ha ulik verdi og dermed forskjellig beskyttelsesbehov. Videre skriver Jøsang (2025) at det ikke er noen tydelig avgrensning av hva som kan være informasjonsverdi.

KS beskriver begrepet informasjonsverdi på følgende måte:

> *All informasjonen kommunen eier og behandler har en verdi. Verdien varierer ut fra typen informasjon og hvilken type virksomhet informasjonen tilhører. Informasjon i denne sammenhengen er alt fra kunnskap, personopplysninger, forretningshemmeligheter, beregningsmodeller, informasjon om hvordan saksbehandlingen skal gjennomføres, IKT-systemer hvor informasjon blir behandlet, teknisk infrastruktur mv. Det å kjenne sine verdier er viktig i informasjonssikkerhetssammenheng, ettersom det avgjør hvordan den skal beskyttes. Beskyttelsesgraden vurderes ut ifra hvor viktig informasjonen er, og hvordan behovet for konfidensialitet, tilgjengelighet og integritet skal bli ivaretatt*.[2]

Vi kan oppsummere at informasjonssikkerhet handler om beskyttelse av informasjonsverdier, og at informasjonsverdier handler om mer enn digitale informasjonsverdier.

Ny lov om digital sikkerhet trådte i kraft fra 01.10.2025.[3] Loven er en del av regjeringens helhetlige satsing på digital sikkerhet og beredskap, og skal bidra til å styrke motstandskraften i viktige samfunnsfunksjoner.

Loven gjelder for tilbydere av samfunnsviktige tjenester innen energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur, samt tilbydere av de digitale tjenestene, digitale markedsplasser, skytjeneste, og digitale søkemotorer.[4] Det er ikke utledet kriterier fra loven i denne forvaltningsrevisjonen

Personvern

Kommunene tar hånd om en mengde personopplysninger, og det kan være risiko for at personopplysninger kommer på avveie. Personvern henger sammen med informasjonssikkerhet, som vi skal belyse i dette delkapitlet. Personopplysningsloven, som innlemmer personvernforordningen (GDPR), regulerer behandlingen av personopplysninger, jf. § 1 i personopplysningsloven. Personopplysninger er enhver opplysning som kan knyttes til en identifisert eller identifiserbar person, jf. personvernforordningen artikkel 4 nr. 1. Personvernet skal verne om personopplysninger (formålsbestemmelsen i artikkel 1) og er

[2] KS, Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

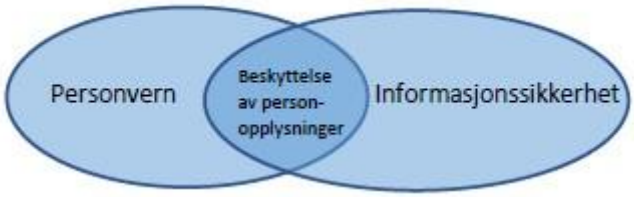
[3] Lov om behandling av personopplysninger (personopplysningsloven). Justis- og beredskapsdepartementet. 2018

[4] https://www.regjeringen.no/no/aktuelt/ny-lov-om-digital-sikkerhet-trer-i-kraft-i-dag/id3121009/

knyttet til blant annet den enkeltes rett til privatliv. (Se blant annet Den europeiske menneskerettskonvensjonen, EMK artikkel 8 og grunnloven § 102)

Et viktig element i personvernet er at den enkelte skal ha kontroll over og i størst mulig grad kunne bestemme over egne personopplysninger. Dette fremgår blant annet innledningsvis til personvernforordningen, punkt 1 og 7. Personopplysningsloven skal regulere og sikre at innsamlingen og bruken av personopplysninger i minst mulig grad går ut over vårt personvern og våre rettigheter. Personvernforordningen er utformet for å beskytte personopplysninger. Forordningen stiller krav til personvernet som kommunen må etterleve, blant annet innbyggernes rett til innsyn i egne personopplysninger og til å kreve retting av opplysninger, jf. artikkel 15-17 i personvernforordningen. Det er tre sentrale prinsipper for behandlingen av personvernopplysninger, og disse er lovlighet, rettferdighet og åpenhet. (jf. personvernforordningen artikkel 5). Det er flere prinsipper enn disse. Datatilsynet har en oversikt.[5]

Personvern og informasjonssikkerhet er to fagområder som har mye til felles, men som også er forskjellige.[6] Det kan illustreres i figuren nedenfor:



Figur 1. Sammenhengen mellom informasjonssikkerhet og personvern.

Kilde: KS, Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

KS understreker at det er viktig å være oppmerksom på at informasjonssikkerhet er mer enn personopplysningssikkerhet, på samme måte som personvern er mer enn informasjonssikkerhet. KS beskriver personvern som en menneskerettighet knyttet til grunnleggende friheter som privatliv, selvbestemmelse og selvutfoldelse. Personvern handler om menneskets rett til, og ønske om, å ha kontroll på informasjon om seg selv; **hvem vet hva om meg, hva brukes informasjonen til og hvordan brukes den**.

Retten til å vite hva opplysninger brukes til gjelder ovenfor kommunen så vel som ovenfor private virksomheter. Det er viktig at kommunen har kontroll på hvilke plikter som følger med når personopplysninger behandles og hvilke rettigheter innbyggere og ansatte har.[7]

[5] https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/

[6] KS, Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

[7] KS, Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

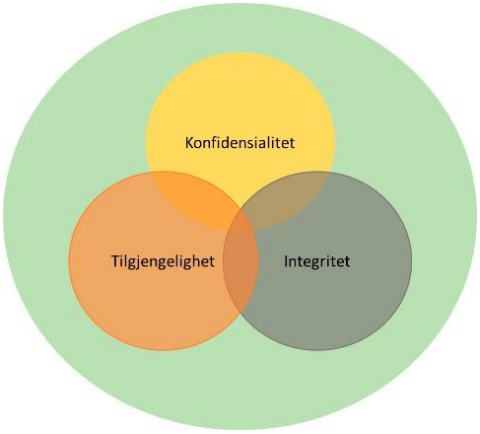
Det er lovpålagt med personvernombud for alle offentlige virksomheter.[8] Personvernombudene er sentrale i virksomhetenes etterlevelse av personvernlovgivningen, og skal ha en uavhengig rolle. Ombudets rolle er å gi råd til ledelsen og andre i virksomheten, men også å kontrollere etterlevelsen av regelverket. I tillegg skal de være kontaktpunkt for de registrerte og Datatilsynet.

Beskyttelsesbehov

I KS verktøykasse for personvern og informasjonssikkerhet beskrives og illustreres beskyttelsesbehovet. Beskyttelsesbehovet kan deles i tre:

- **Konfidensialitet**: informasjon er beskyttet mot uautorisert innsyn
- **Integritet**: informasjonen er riktig, komplett og til å stole på
- **Tilgjengelighet**: informasjonen er tilgjengelig når det er behov for den.[9]

Figuren nedenfor illustrerer beskyttelsesbehovet (grønt felt), med de tre elementene (gul, oransje og grå sirkel, som i noen grad overlapper hverandre):



Figur 2. Beskyttelsesbehov for personvern og informasjonssikkerhet.

Kilde: KS, Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

Nasjonal sikkerhetsmyndighets (NSM) grunnprinsipper for IKT-sikkerhet

NSM har fastsatt grunnprinsipper for informasjonssikkerhet[10]. De fire grunnprinsippene er:

[8] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/personvernombud/hvem-ma-hapersonvernombud/trinn-for-trinn-veileder/

[9] KS, Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

[10] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/introduksjon/

- **Identifisering og kartlegging:** Identifisering og kartlegging (oversikt over) av styringsstrukturer, leveranser og understøttende systemer, i tillegg til enheter (f.eks. pc-er), programvare og tilganger.
- **Beskytte og opprettholde:** Ivareta sikkerhet i anskaffelses- og utviklingsprosesser, sikker IKT-arkitektur, beskytte nettverk, beskytte e-post og nettleser.
- **Oppdage og overvåke:** Oppdage og fjerne kjente sårbarheter og trusler, sikkerhetsovervåkning, gjennomføre inntrengningstester.
- **Håndtere og gjenopprette:** Forberede virksomheten på håndtering av hendelser, kontrollere og håndtere hendelser, evaluere og lære av hendelser.

Internkontroll

Kommunedirektørens ansvar for internkontroll følger av kommuneloven[11], kapittel 25. I tillegg er internkontroll regulert av eForvaltningsforskriften [12] på informasjonssikkerhetsområdet. Forskriften har hjemmel i forvaltningsloven § 15a om elektronisk kommunikasjon. Forskriften krever at forvaltningsorganet skal ha en internkontroll på informasjonssikkerhetsområdet som bør være integrert som en del av virksomhetens helhetlige styringssystem.

(se liste med begrepsavklaringer i kapittel 1.5)

1.4 Kommunens organisering

Kommunedirektøren i Malvik er øverste, administrative leder, med en strategisk ledergruppe bestående av tre kommunalsjefer, en organisasjonssjef og en økonomisjef. De tre kommunalsjefene leder hvert sitt område: helse og velferd, oppvekst og samfunn. Organisasjonssjefen leder kommunedirektørens fagstab, HR, servicetorg og Værnesregionen dokumentasjonssenter. Økonomisjefen leder kommunens økonomi- og finansforvaltning, inklusive innkjøp.

Fra og med 01.01.2025 utføres IKT-tjenester i Malvik kommune i et vertskommunesamarbeid gjennom Værnesregionen IKT (VarIT). Kommunestyret vedtok den 17.06.2024 en vertskommuneavtale mellom Malvik kommune (samarbeidskommune) og Stjørdal kommune (vertskommune). På VarITs nettsider står følgende:

Tjenestesenteret forestår leveranser av felles drifts- og vedlikeholdstjenester, samt utvikling og skal sørge for at kommunene når sine strategiske mål om:

- Forbedret effektivitet og ressursutnyttelse i egen organisasjon.

[11] Lov om kommuner og fylkeskommuner. Kommunal- og distriktsdepartementet. 2018

[12] Forskrift om elektronisk kommunikasjon med og i forvaltningen. Digitaliserings- og forvaltningsdepartementet. 2004.

- Økt tilgjengelighet og bedre kvalitet med hensyn til service til innbyggere og næringsliv.
- Utnytte moderne IT-løsninger som et verktøy til å styrke et aktivt lokal- og brukerdemokrati.
- Økt verdiskapning og innovasjon.

VarIT har hovedkontor i Stjørdal rådhus.

Malvik kommune har også personvernombud gjennom Værnesregionen. På kommunens nettside framgår det personvernerklæring, med forskjellige opplysninger om personvern, deriblant navn og kontaktinformasjon for personvernombudet. I tillegg til personvernombudet i Værnesregionen, er det lokale personvernkontakter innenfor alle rammeområdene, og i tillegg til fire virksomheter innen oppvekst og kultur. Ansvar for og organisering av informasjonssikkerhet er nærmere berørt i kapittel 2.2.

1.5 Metode

Forvaltningsrevisjonen er gjennomført i henhold til NKRFs standard for forvaltningsrevisjon, RSK 001. Revisor har vurdert egen uavhengighet overfor Malvik kommune, jf. kommuneloven § 24-4 og forskrift om kontrollutvalg og revisjon kapittel 3.
Vi har brukt flere metoder for å samle inn og analysere data til dette prosjektet.

1.5.1 Oppstartsmøte

Det ble gjennomført oppstartsmøte med kommunedirektøren den 09.03.2026. I tillegg til kommunedirektøren, deltok organisasjonssjef (revisors kontaktperson), digitaliseringsleder, personvernombudet, IT-leder (de to sistnevnte fra Værnesregionen). Oppstartsmøtet inneholdt gjensidig informasjonsutveksling om blant annet revisjonskriterier, metodisk opplegg og Malvik kommunes organisatoriske ivaretakelse av informasjonssikkerhet og personvern. Det ble skrevet referat fra møtet, som er verifisert av kommunedirektøren.

1.5.2 Intervju

Det er gjennomført individuelle intervju med følgende personer i følgende funksjoner:

- Organisasjonssjef,som også er CISO og sikkerhetsansvarlig i Malvik kommune. I rapporten omtales han som organisasjonssjef
- Tre kommunalsjefer for oppvekst, helse og velferd og samfunn
- Digitaliseringsleder
- IT-leder og sikkerhetsansvarlig i VarIT[13]

[13] Sikkerhetsansvarlig i Malvik og sikkerhetsansvarlig i VarIT er to forskjellige funksjoner/personer

- Personvernombud (Værnesregionen)

Intervjuene med kommunalsjefene og digitaliseringsleder ble gjennomført som videomøter. De øvrige ble intervjuet i fysisk møte. IT-leder og sikkerhetsansvarlig i VarIT ble intervjuet sammen. Det ble skrevet referat fra intervjuene, som er korrigert og godkjent av intervjuobjektene.

Hensikten med intervjuene har vært å få utdypende informasjon om informasjonssikkerhet og personvern i kommunen, og informantenes erfaring med å ivareta informasjonssikkerhet og personvern innenfor sitt område.

1.5.3 E-poster med spørsmål

Vi har sendt e-post med ti spørsmål til personvernkontaktene i kommunen. Det er sju personvernkontakter, hvorav fire på enhetsnivå innen oppvekst. Vi har mottatt svar fra alle sju personvernkontaktene. Hensikten med spørsmålene har vært å få informasjon om personvernkontaktenes opplevelse av rollen sin, og kontakt med ledelse og ansatte innenfor sitt område og personvernombudet.

1.5.4 System– og dokumentgjennomgang

Revisor har hatt lesetilgang til kvalitetssystemet Compilo og personvernsystemet Visma Draftit. I Compilo har vi funnet oversikt over oppbygging av styringssystem for informasjonssikkerhet og personvern, og tilhørende styrende dokumenter, prosedyrer og rutiner. I Draftit har vi funnet oversikt over behandlinger (protokoller og DPIAer).

Vi har også fått oversendt dokumentasjon gjennom vår kundeportal, Verji. Dette er vertskommuneavtale, referat fra møter og eposter med ulike informasjonstiltak. I tillegg har vi søkt etter dokumentasjon i virksomhetsstyringssystemet Framsikt og i andre områder på kommunens hjemmesider.

Hensikten med gjennomgang av systemer og dokumentasjon har vært å få kjennskap til hvordan systemet for informasjonssikkerhet og personvern er bygd opp i kommunen, og hvordan informasjonssikkerhet og personvern er beskrevet i styringsdokument og interne rutiner og prosedyrer.

En foreløpig rapport, uten revisors vurdering, konklusjon og anbefalinger, ble sendt til kommunedirektøren til faktaverifisring. Vi fikk noen korrigeringer og supplerende informasjon i den sammenhengen.

1.5.5 Vurdering av metode

Revisor har brukt ulike metoder for å få et tilstrekkelig informasjonsgrunnlag for å konkludere på problemstillingene. Det vil alltid være funksjoner og personer som kan gi ytterligere informasjon, og det kan være flere system, styrende dokumenter og praksis som beskriver

informasjonssikkerhet og personvern. Revisor mener at kildene for informasjon, både intervjuinformasjon og skriftlig dokumentasjon, er de mest sentrale kildene og tilstrekkelige for å belyse problemstillingene.

1.6 Uttalelse om rapport

En foreløpig rapport ble sendt til kommunedirektøren for uttalelse den 28.08.2026. Kommunedirektøren har gitt skriftlig uttalelse, datert 07.09.2026. Uttalelsen er vedlagt rapporten (vedlegg 2). Kommunedirektøren har ikke påpekt behov for endringer i den endelige rapporten.

1.7 Begrepsavklaringer

Informasjonssikkerhet

Beskyttelse av informasjonens konfidensialitet, integritet og tilgjengelighet (personvernforordningen)[14].

Konfidensialitet

Innebærer at informasjonen er beskyttet mot uautorisert innsyn

Integritet

Innebærer at informasjonen og informasjonsbehandlingen er riktig, komplett og til å stole på

Tilgjengelighet

Innebærer at informasjonen er tilgjengelig når det er behov for den.[15]

Begreper fra personvernforordningen GDPR (General Data Protection Regulation).

GDPR er en forkortelse for personvernforordningen, som er en lov som EU har vedtatt. Personvernforordningen er tatt inn i den norske lov om personopplysninger. I stedet for paragrafer henviser forordningen til artikler.

Personopplysning

Enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, eksempelvis et navn, et identifikasjons nummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet. (Personvernforordningen artikkel 4).

[14] EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) [PVF, GDPR]

[15] KS, Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

Behandling

Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, eksempelvisinnsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammen stilling eller samkjøring, begrensning, sletting eller tilintetgjøring. (Personvernforordningen artikkel 4).

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. (Personvernforordningen artikkel 4).

Behandlingsprotokoll

Den behandlingsansvarliges representant skal føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar. Det stilles også krav til hva behandlingsprotokollen skal inneholde. (Personvernforordningen artikkel 30).

Databehandler

En fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige.
(Personvernforordningen artikkel 4).

DPIA[16] – personvernkonsekvensvurdering

Dersom det er sannsynlig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet. (Personvernforordningen artikkel 35).

Grunnprinsippene for IKT-sikkerhet (NSM)

- Identifisere og kartlegge: Ha oversikt over enheter, programvare og tilganger
- Beskytte og opprettholde: sikkerhet i anskaffelser, utviklingsprosesser, IKT-arkitektur, nettverk, e-post og nettleser.
- Oppdage og overvåke: Oppdage og overvåke sårbarheter og trusler, gjennomføre inntrengningstester
- Håndtere og gjenopprette: forberede (beredskap) på hendelser, håndtering av og evaluering/læring etter hendelser.

[16] DPIA = Data Protection Impact Assessment

2 STYRINGSSYSTEM

2.1 Problemstilling

Det er utarbeidet følgende problemstilling:

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

2.2 Sikkerhetsmål, -strategi og -organisering

2.2.1 Revisjonskriterier

- Kommunen skal ha et styringssystem som omfatter informasjonssikkerhet, som angir
  - Sikkerhetsmål
  - Sikkerhetsstrategi
  - Sikkerhetsorganisasjon, hvor roller og ansvar framgår

Utledningen av revisjonskriteriene finnes i vedlegg 1.

2.2.2 Funn

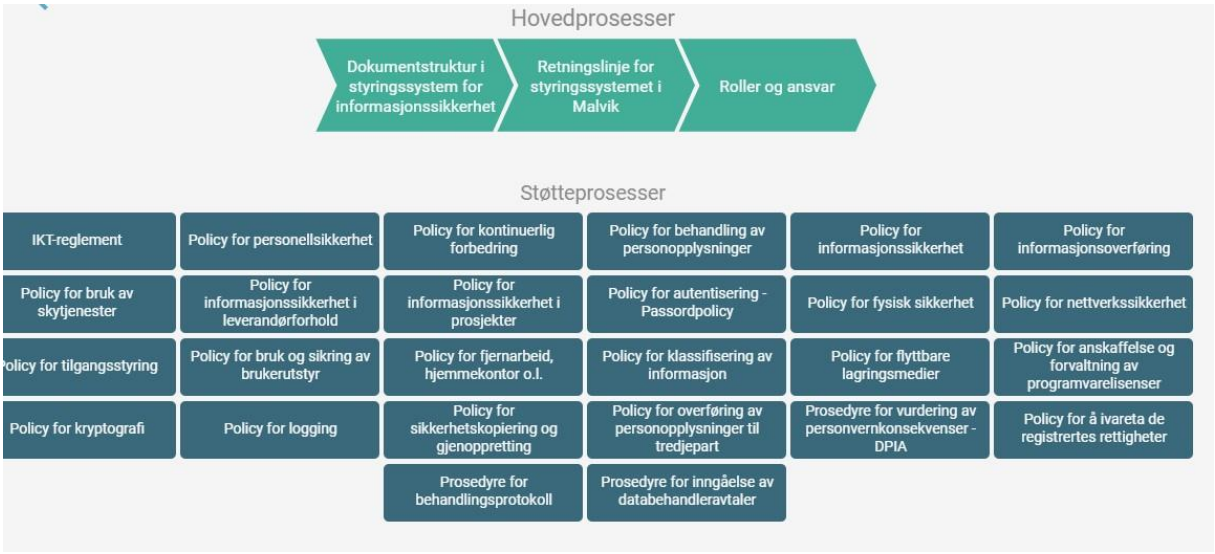
I kvalitetssystemet Compilo er styringssystemet for informasjonssikkerhet illustrert på denne måten (se figur nedenfor):



Figur 3. Styringssystem for informasjonssikkerhet, Malvik kommune.

Kilde: Compilo, Malvik kommune

Systemet er delt inn i styrende dokumenter, gjennomførende dokumenter og kontrollerende dokumenter. Organisasjonssjefen forteller at det er jobbet gradvis med systemet siden 2021. Det første som kom på plass var kontrollerende dokumenter, for å sikre håndtering av hendelser og avvik. Figuren nedenfor illustrerer innholdet boksen for styrende dokumenter.



Figur 4. Kommunens styrende dokumenter i informasjonssikkerhet og personvern.

Kilde: Compilo, Malvik kommune

Her er policydokument for mange områder, som IKT-reglement, policy for personellsikkerhet, policy for kontinuerlig forbedring, policy for behandling av personopplysninger, policy for informasjonssikkerhet for å nevne noen av dokumentene.

Policyen for informasjonssikkerhet lister opp tre *informasjonssikkerhetsmål:*

Informasjonssikkerhet: Følgende informasjonssikkerhetsmål gjelder for alt arbeid med informasjonssikkerhet:

- Kommunen skal sikre konfidensialiteten, integriteten og tilgjengeligheten i all sin informasjonsbehandling.
- Kommunen skal sikre kontinuiteten til kritiske systemer og tjenester.
- Kommunen skal sikre at personvernet til de registrerte ivaretas.

Målsettingen med **Policyen for behandling av personopplysninger** å sikre at alle behandlinger skjer i samsvar med personopplysningsloven, herunder:

- Sikre og dokumentere at alle behandlinger er lovlige, og har tydelige definerte og legitime formål.
- Sikre etterlevelse av personvernregelverket.

I et referat fra ledelsens gjennomgang den 23.03.2026 framgår det at sikkerhetsmålene er tatt opp til vurdering, og at konklusjonen er at målene fortsatt skal være gjeldende.

I boksen for **Roller og ansvar** framgår følgende om *sikkerhetsorganisasjonen*:

> Sikkerhetsorganisasjonen er den delen av kommuneorganisasjonen som er ansvarlig for å utvikle, implementere, overvåke og forvalte styringssystemet for

informasjonssikkerhet. Medlemmer av sikkerhetsorganisasjonen skal ha spesifikke roller og ansvar, og skal samarbeide for å sikre at kommunen har et effektivt styringssystem. Sikkerhetsorganisasjonen bør etablere faste samarbeidsarenaer.

Sikkerhetsorganisasjonen består av:

- Kommunedirektørens strategiske ledergruppe (representant fra gruppen)
- Sikkerhetsansvarlig i Malvik (Organisasjonssjef - CISO)
- Digitaliseringsleder
- IT-leder Værnesregionen IT (VarIT)
- Personvernombud (Værnesregionen)

I tillegg framgår det at flere ansatte vil være involvert i informasjonssikkerhetsarbeidet. En del ansatte vil for eksempel involveres i risikovurderinger, andre vil involveres i gjennomføring av sikkerhetstiltak, mens alle ansatte vil måtte forholde seg til sikkerhetsinstruksen.

Det framgår ikke i noen av de styrende dokumentene hva som er *sikkerhetsstrategi.* Organisasjonssjefen forteller at kommunen ikke har sett behov for det.

Organisasjonssjefen forteller at det er han som har arbeidet fram alle dokumentene hvor kommunedirektør eller organisasjonssjefeneier policyen. En god del av dokumentene, særlig den som handler om teknisk sikkerhet, er utarbeidet av informasjonssikkerhetsteamet i VarIT, fordi disse gjelder på tvers av alle kommuner i det interkommunale IT-samarbeidet. Organisasjonssjefen sier at dokumentene er forankret i strategisk lederteam, som også har vært orientert underveis i prosessen, selv om det ikke har vært noen stor medvirkning fra øvrige kommunalsjefer. Styringssystemet ble vedtatt i strategisk lederteam den 30.9.2024. Etter dette ble virksomhetsledere orientert om internkontrollrutiner, ledelsens gjennomgang, behandlingsprotokoller samt styringssystem for informasjonssikkerhet i felles møte den 16.10.2024. Oppsummert vet ledere at systemet og dokumentene finnes, men det kan være en utfordring å huske å bruke det.

Organisasjonssjefen sier at styringssystemet er tydelig avklart for Malvik sin del. Malvik etterspør VarITs sikkerhetsvurderinger opp mot egen internkontroll. Det vises ellers til kapittel 3, hvor samarbeidet med VarIT er nærmere vurdert.

To av kommunalsjefene bekrefter at de kjenner til det overordna systemet i Compilo, men begge forteller at de må slå opp for å få informasjon om detaljer.

Også digitaliseringsleder kjenner til at kommunen har et etablert system for informasjonssikkerhet og personvern. Han har en utvidet forståelse av hva informasjonssikkerhet innebærer. Han skiller gjerne mellom «papirbasert» sikkerhet og teknisk

sikkerhet. I det papirbaserte systemet blir det ofte søkelys på sjekklister som man blir målt på, snarere enn på hva som faktisk bidrar til reell sikkerhet. Etter digitaliseringsleders syn, er kommunen «compliant»[17], men verdien er begrenset, ettersom risikoer og teknologi endrer seg kontinuerlig. Digitaliseringsleder trekker fram virksomhetsarkitektursystemet Ardoq[18], som han mener kan svare ut disse dilemmaene.

Ledelsen i VarIT har oversendt de retningslinjene og rutinene som er utarbeidet av dem til Malvik kommune.

Personvernombudet har vært med på utarbeiding av prosedyrer som har vært innom VarIT, og som har blitt generert av Stjørdal kommune. Hun har ikke helt oversikt over Malvik

kommune sin dokumentasjon. Personvernombudet sitter i sikkerhetsorganisasjonen i Malvik kommune, men har ikke vært på møter i denne sammenheng. Hun ble innkalt på ledelsens gjennomgang for personvern og informasjonssikkerhet i 2026, men kunne ikke delta.

2.2.3 Revisors vurdering

- Kommunen skal ha et styringssystem som omfatter informasjonssikkerhet, som angir
    - Sikkerhetsmål
    - Sikkerhetsstrategi
    - Sikkerhetsorganisasjon, hvor roller og ansvar framgår

Etter revisors vurdering har kommunen beskrevet sikkerhetsmål og sikkerhetsorganisasjon, hvor roller og ansvar er beskrevet. Kommunen har ikke beskrevet sikkerhetsstrategi.

Kommunens styringssystem angir sikkerhetsmål og beskriver sikkerhetsorganisasjonen. Systemet inneholder ikke sikkerhetsstrategi. Etter revisors vurdering vil en sikkerhetsstrategi synliggjøre hvordan kommunen skal nå sikkerhetsmålene.

Revisor vurderer at revisjonskriteriet i hovedsak er oppfylt.

2.3 Internkontroll

2.3.1 Revisjonskriterier

• Informasjonssikkerhet skal inngå i kommunens internkontrollsystem. Den skal inneholde:

- Oversikt over regelverk, prosedyrer og rutiner for informasjonssikkerhet og personvern

[17] Følger lover og forskrifter
[18] Plattform for virksomhetsarkitektur

- Risiko- og sårbarhet og beredskap for informasjonssikkerhet og personvern
- System for håndtering av avvik innen informasjonssikkerhet og personvern

Utledningen av revisjonskriteriene finnes i vedlegg 1.

2.3.2 Funn

I dette kapitlet presenteres data om internkontroll av informasjonssikkerhet og personvern.

Som tidligere nevnt, har Malvik kommune Compilo som kvalitetssystem. Compilo er bygd opp med et dokumentbibliotek, hvor informasjonssikkerhet og personvern har en hovedmappe. De overordna styringsdokumentene ble beskrevet i kapittel 2.2. Blant de styrende dokumentene finner vi også prosedyre for vurdering av personvernkonsekvenser (DPIA), prosedyre for behandlingsprotokoll og prosedyre for databehandleravtaler.

Videre, er det en kategori for gjennomførende dokumenter og en boks for kontrollerende dokumenter. Gjennomførende prosesser (støtteprosesser) er ulike prosedyrer, for eksempel prosedyre for risikostyring av informasjonssikkerheten, prosedyre for sårbarhetskartlegging av IT-systemer, prosedyre for innhenting av trusselinformasjon, for å nevne noen. I kontrollerende dokumenter finner vi prosedyre for avvikshåndtering ved brudd på informasjonssikkerhet, prosedyre for varsling av personopplysningssikkerheten, prosedyre for å melde avvik til Datatilsynet, prosedyre for ledelsens gjennomgang, prosedyre for kontroll av leverandør. I tillegg finnes det maler for ulike referater, deriblant mal for referat fra ledelsens gjennomgang.

Organisasjonssjefen opplyser at Compilo er det stedet dokumentene er samlet. På Innsida (intranett?) er det lagt til en kategori for informasjonssikkerhet og personvern. Dette er gjort i samarbeid med personvernombudet. Her finnes det blant annet noen kompetanseplattformer, og det står også noe om styringssystemet og hvor det finnes. I den grad folk bruker Innsida, blir informasjon distribuert. Organisasjonssjefen mener at flere ledere er mer oppmerksomme på dette nå. Kommunen har ikke dokumentasjon på om ansatte har tilegnet seg kunnskap, men det er ønske om å få til et lederdashbord på dette, gjennom KS Kunnskap.

Organisasjonssjefen forteller at det er metadata på alle dokumenter. Det er angitt dato for neste revisjon, og det er dokumentansvarlig som velger dato. Dokumentet som omhandler roller og ansvar er revidert nylig, blant annet etter at digitaliseringsleder kom på plass i 2025.
Den rollen er lagt inn i sikkerhetsorganisasjonen. Utover det er det ikke gjort store justeringer.

Kommunalsjefene kjenner til at styrende dokumenter, prosedyrer og beskrivelse av roller ligger i Compilo, men alle tre viser til at det er omfattende dokumentasjon, og at det viktigste er å finne de rette dokumentene når de trenger de.

I Compilo finner vi dokumentet Helhetlig ROS-analyse, opprettet i januar 2025. Det er flere hendelser som direkte eller indirekte berører informasjonssikkerhet og personvern: sabotasje

IT, sabotasje mot vannforsyningen, cyberhacking, langvarig bortfall av strøm og telenett er hendelser som er oppført i oversikten. Overordna beredskapsplan finnes også i Compilo, opprettet i juni 2026. Denne inneholder beskrivelser av kommunens visjon og mål for beredskapsarbeidet, ansvar og oppgaver og plan for krisekommunikasjon. I dette dokumentet framgår ikke beredskap for konkrete hendelser. Organisasjonssjefen, som også er sikkerhetsansvarlig i Malvik kommune, sitter i kriseledelsen. Det framgår at kriseledelsen, ved anledning kan utvides, blant annet med IKT-avdeling.

Organisasjonssjefen sier at kommunen er i ferd med å bygges helhetlig ROS helt på nytt. Det er en del nye områder som må tas inn. Det er åpenbare sårbarheter. De holder nå på å planlegge en større øvelse med kunnskapspåfyll i forkant, knyttet til bortfall av e-kom (situasjoner der man ikke kan bruke mobilnett, internett eller andre former for elektronisk kommunikasjon). Scenario er at kommunen har bortfall av e-kom på 1 måned, men selve øvelsen vil bli gjennomført i løpet av 1 dag. Da skal beredskapsplaner og tiltakskort ute i virksomhetene testes. Det starter med workshops, område for område, der beredskapsplaner og tiltakskort revideres eller bygges på nytt før dette testes i øvelsen. Forberedelsene begynner i juni. Øvelsen er planlagt gjennomført i november/desember i 2026.

I Compilo finner vi prosedyre for risikostyring av informasjonssikkerheten. Innledningsvis går det fram at dokumentet definerer hvordan risikostyring av informasjonssikkerheten skal gjennomføres. I prosedyren er det listet opp ulike situasjoner som krever risikovurdering.

Kommunalsjef for helse og velferd sier at informasjonssikkerhet inngår i kommunens helhetlige ROS. Trusselbildet er blant annet gjennomgått i beredskapsråd, og vurderinger er tatt inn i beredskapsplanene. Det er etablert samarbeid med beredskapsansvarlig, som deltar jevnlig i ledergruppen.

Det blir også gjennomført ROS-vurderinger i forkant av perioder med økt sårbarhet, som ferieavvikling ved sommer og jul.

Kommunalsjef for oppvekst forteller at det er gjennomført overordnet ROS med representanter fra rektorgruppa, knyttet til bortfall av strøm, vann med mer. Det er sjelden det er stor risiko knyttet til bortfall av strøm/internett i skolene. Det er ikke fare for liv og helse. Over tid vil det være krevende for alle ansatte å få gjort jobben sin hvis systemene går ned. Mye av det de holder på med er sky-lagret og det blir kommunisert via digitale kanaler. Det vil få konsekvenser for kvaliteten i opplæringen.

Ellers har kommunalsjefen i rollen som rektor ivaretatt et arbeid, på vegne av rektorene, med å systematisere beredskapsplan og internkontroll/HMS i skolene, slik at det er felles system i Compilo. De har jobbet med dette et helt år med dette, men informasjonssikkerhet og personvern har ikke vært så mye i fokus i det arbeidet.

Videre, forteller kommunalsjefen at risikotenkning ofte er tema i ulike sammenhenger, og viser til en nylig prosjektsøknad rundt KI-agenter, hvor risiko fort kom opp når det gjaldt hvordan prosjektet kunne rigges.

Kommunalsjef for samfunn bekrefter at det har vært gjennomgang av helhetlig ROS, og at vann og vannforsyning er vurdert som størst risiko innenfor hennes område. Dette gjelder også informasjonssikkerhet, der hacking av systemene for vannforsyning kan få store konsekvenser.

I Compilo finner vi dessuten avvikssystemet. Avvik innen informasjonssikkerhet og personvern er delt i to hovedkategorier: Informasjonssikkerhet – sikkerhetshendelse, og Informasjonssikkerhet – personvern (GDPR). Innen denne første kategorien er det fem underkategorier, inklusive annet-kategori (mistet IKT-utstyr, passord på avveie, phishing og virusangrep). I den andre hovedkategorien er det underkategorier i tre nivå, til sammen 25 underkategorier.

Hittil i 2026 (23. juni) har det vært 3 avvik i kategorien sikkerhendelse, og 13 avvik i kategorien personvern (GDPR). I 2025 var de tilsvarende tallene for hele året 7 og 31. Avvike, både i 2025 og hittil i 2026 har vært fra lav til middels alvorlighetsgrad, men ingen med høg alvorlighetsgrad.

Organisasjonssjef forteller at forståelsen ikke er helt avklart hos alle som registrerer avvik. Det er en egen hovedkategori for informasjonssikkerhet og personvern i Compilo. Ut fra rapporteringen ser vi at det meldes avvik på dette uten at det er forståelse for hva et brudd kan være. Ledere har blitt flinkere til å endre kategori hvis det er feilregistrert. Alle avvik innenfor kategoriene personvern og informasjonssikkerhet blir automatisk sendt til personvernombudet og organisasjonssjefen, som går gjennom og gir tilbakemelding/veiledning.

Kommunalsjefene viser til at det er gode prosedyrer for å melde avvik på informasjonssikkerhet og personvern. Virksomhetene innen helse og velferd har mest erfaring med å melde avvik. I 2026 ble det meldt mange avvik på informasjonssikkerhet og personvern. Kommunalsjefen sier at det noen ganger handler om utstyr, og ikke personvern. Hun mener likevel at det er bra at ansatte melder avvik, det fører til økt bevisstgjøring.

Kommunalsjef for oppvekst forteller at det er kontinuerlig diskusjon om hva som er avvik på personvernbestemmelsene, særlig i det tverrfaglige samarbeidet mellom tjenestene. Det er jobbet mye med samtykke.

2.3.3 Revisors vurdering

- Informasjonssikkerhet skal inngå i kommunens internkontrollsystem. Den skal inneholde:
    - Oversikt over regelverk, prosedyrer og rutiner for informasjonssikkerhet og personvern
    - Risiko- og sårbarhet og beredskap for informasjonssikkerhet og personvern
    - System for håndtering av avvik innen informasjonssikkerhet og personvern

Etter revisors vurdering inngår informasjonssikkerhet og personvern i kommunens system for internkontroll

Det digitale kvalitetssystemet, Compilo, inneholder regelverk, prosedyrer og rutiner som gjelder for informasjonssikkerhet og personvern. Etter revisors vurdering er systemet omfattende, og bygd opp med en rekke detaljerte retningslinjer, prosedyrer og rutiner. Informanter sier at det er enkelt å søke opp og/eller finne aktuell dokumentasjon når en er kjent med at dokumentasjonen finnes i systemet.

Revisor vurderer at temaer som gjelder risiko rundt informasjonssikkerhet er berørt i den helhetlige risiko- og sårbarhetsanalysen. Kommunens ledelse, ved organisasjonssjefen, har oppmerksomhet på områder innen informasjonssikkerhet og personvern og hva som bør være med i neste gjennomgang av helhetlig ROS. Overordna beredskapsplan finnes også i kvalitetssystemet Compilo. Revisor vurderer det som positivt at kommunen planlegger en større øvelse knyttet til bortfall av e-kom, som er situasjoner der man ikke kan bruke mobilnett, internett eller andre former for elektronisk kommunikasjon.

Etter revisors vurdering er det lagt til rette for rapportering og håndtering av avvik, ved at det er etablert to hovedkategorier: Informasjonssikkerhet – sikkerhetshendelse og Informasjonssikkerhet – personvern/GDPR. Begge kategoriene har underkategorier. Etter det revisor vurderer, gjenstår det en god del arbeid for at ansatte får riktig forståelse av hva som er avvik innen informasjonssikkerhet og personvern.

Revisor vurderer at kriteriet om at informasjonssikkerhet skal inngå i kommunens internkontrollsystem er oppfylt.

2.4 Personvern

2.4.1 Revisjonskriterier

- Kommunen skal ha et personvernombud
    - Det skal sikres nødvendig uavhengighet for personvernombudet
    - Personvernombudet skal sikres nødvendige ressurser for å utføre minimumoppgaver
    - Kommunen skal ha rutiner for personvernombudets arbeid som sikrer involvering, og det bør være regelmessig dialog med ledelsen.
- Kommunen skal føre protokoll over hvilke personopplysninger de behandler, som minimum inneholder obligatorisk informasjon.
- Kommunen skal ha databehandleravtaler som minimum inneholder obligatorisk informasjon.

- Kommunen skal gjennomføre en vurdering av personvernkonsekvenser før behandlinger som sannsynligvis vil medføre høy risiko for fysiske personers rettigheter og friheter.

Utledningen av revisjonskriteriene finnes i vedlegg 1.

2.4.2 Funn

Funn om personvernombud og personvernkontakter

Det ble i april 2025 signert en vertskommuneavtale (Værnesregionen Personvernombud), mellom Stjørdal kommune som vertskommune og Malvik kommune. Malvik kommune har personvernombud innenfor samarbeidet i Værnesregionen. Funksjonen som personvernombud er organisert under kommunedirektøren i Stjørdal kommune sitt ressursteam. I intervju forteller personvernombudet at funksjonen som personvernombud utgjør 50 % av en hel stilling. Det er uendret etter at Malvik gikk inn i samarbeidet i tillegg til de andre kommunene. Personvernombudets rolle er beskrevet i vertskommuneavtalen og det styrende dokumentet Roller og ansvar (sikkerhetsorganisasjon) i Compilo for Malvik kommune. Der går det fram at personvernombudet skal:

- Informere og gi råd til kommunens ledelse og ansatte om de forpliktelsene som følger av personvernregelverket, jfr. GDPR artikkel 39
- Kontrollere kommunens overholdelse av personvernregelverket
- Bistå med rådgivning av risikovurderinger (ROS-analyse/DPIA), og kontrollere gjennomføringen av den.
- [Være] Faglig støtte til rammeområdenes personvernkontakter.
- Ved behov, rådføre seg med Datatilsynet
- Prioritere innsatsen dit hvor personvernrisikoen er størst.
- Bistå med råd i arbeidet med oversikt over behandlingene.
- Ta imot henvendelser fra de registrerte om alle spørsmål knyttet til behandling av deres opplysninger, og om utøvelsen av rettighetene de har i henhold til personvernforordningen.

I intervju med personvernombudet kommer det fram at det er uklarheter i tolkningen av vertskommuneavtalen, blant annet om når det skal det inngås databehandleravtale i vertskommunesamarbeidene. Hun forteller at det er uklart for mange hvem som er databehandleransvarlig i slike kommunesamarbeider. Personvernombudet sier at hun ikke har helt oversikt over Malvik sin dokumentasjon i styringssystemet, men at hun har bidratt med å korrigere endringer i dokumentet Roller og ansvar. Personvernombudet forteller at det i ulike dokumenter kan framstå at hun har ansvar for personvernkontaktene, og at det er hun som har ansvar for behandlingsprotokoller.

Ifølge personvernombudet er det klart uttrykt at funksjonen skal ivareta minimumsoppgaver som følge av kravene i personopplysningsloven. Ombudet skal jobbe risikobasert. Daglig handler det om å svare på spørsmål fra kommunene. Hun utarbeider også artikler til Innsida på tema og spørsmål som går igjen. Videre, er hun jevnlig til stede i rådhuset i Malvik kommune. I vertskommuneavtalen framgår det at personvernombudet skal rapportere til kommunedirektøren i hver deltakerkommune. Videre framgår det at kommunedirektøren i vertskommunen skal rapportere til kommunestyrene i samarbeidet per tertial og avlegge årsrapport. Revisor har blitt forelagt årsrapport fra personvernombudet for 2025. Den omfatter arbeidet i alle deltakerkommunene. Revisor har gjennomgått årsmelding for Malvik kommune for 2025. Rapport for personvernombudets virksomhet er ikke en del av dette dokumentet. Revisor har gjennomgått sakslister og protokoller i politisk møtekalender for kommunestyret for perioden april 2025 – juni 2026. Det framgår ikke at det er lagt fram tertialrapporter og årsrapporter for personvernombudet i kommunestyret. På spørsmål om det er lik forståelse av minimumsoppgaver, forteller personvernombudet at det fortsatt er mange som sliter med å forstå hva personvernombudets rolle egentlig er. Personvernombudet har en veiledningsrolle, og ikke en utførende rolle. Dette kan nok oppleves litt flytende. Hun opplever at kommunene og samarbeidsorganet kan ha ulik forståelse av hvem som har ansvar.

Personvernombudet forteller at hun står faglig fritt og kan ivareta uavhengighet i rollen.

I tillegg til personvernombudet, er det egne **personvernkontakter** innenfor hvert av rammeområdene i Malvik kommune. Personvernkontaktene skal i henhold til dokumentet Roller og ansvar ta imot henvendelser fra de registrerte om alle spørsmål knyttet til behandling av deres opplysninger, og om utøvelsen av rettighetene de har i henhold til personvernforordningen. Videre skal de gi råd og veiledning til ansatte i personvernspørsmål, bidra til å få oversikt over behandlingene, bistå med rådgivning av ROS-analyse/DPIA og rådføre seg med personvernombudet ved behov.

Basert på svar på revisors spørsmål i epost fra sju personvernkontakter, oppgir de fleste at de har vært personvernkontakt siden høsten 2025 eller siden funksjonen ble opprettet. Svarene viser en variasjon i hvor aktivt rollen utøves. Noen personvernkontakter har konkrete oppgaver knyttet til behandlingsprotokoller, databehandleravtaler, DPIA-er, digitale verktøy og vurdering av apper/webapplikasjoner, særlig innen skoleområdet. Andre oppgir at de foreløpig ikke har vært involvert i slike oppgaver, eller at de ikke har mottatt henvendelser.

Funn om behandlingsprotokoller

I Compilo er det en prosedyre for behandlingskontroll. Der går det fram hva som er formål med behandlingsprotokoller, mål og skjema for mal for utfylling av behandlingsprotokollen. I

skjemaet er det listet 18 aktiviteter som skal fylles ut. Det skilles ikke mellom obligatoriske og anbefalte aktiviteter.

Kommunens behandlingsprotokoller ligger i Visma Draftit. Det er 39 behandlinger i systemet. 22 av disse står oppført som ferdig.[19] Fem behandlinger står oppført under «revidering», som betyr at dato for revidering har passert. Fem protokoller står oppført under «utbedring». Det som kjennetegner disse, er at det ikke er utfylt informasjon for disse. Ni behandlinger står oppført som utkast, og sju av disse er tomme. For to behandlinger er det fylt ut formål med behandlingen for.
Organisasjonssjefen bekreftet at kommunens virksomheter er i prosess med å fylle ut behandlinger i Draftit, og at de i varierende grad er i mål med det.

Av kommunalsjefene er der bare kommunalsjef for helse og velferd som mener at de innenfor hennes område er ajour med dette arbeidet.

Funn om databehandleravtaler

I Compilo ligger det prosedyre for databehandleravtaler. Det går fram av prosedyren at det er utelukkende Malvik kommune som er part i en databehandleravtale, ikke Værnesregionen eller andre foretak. Det går videre fram når databehandleravtale skal inngås, at kommunen må godkjenne leverandøren og hvem som er ansvarlig for å inngå databehandleravtale. Det er kommunedirektøren som er ansvarlig for innholdet i prosedyren, og alle som inngår avtale med eksterne om behandling av personopplysninger på vegne av kommunen, skal følge prosedyren [retningslinjen]. Videre går det fram at Malvik kommune bruker DFØ[20] sin mal på databehandleravtale. Ifølge organisasjonssjefen er databehandleravtalene lenket opp til systemet som hører til den enkelte behandling direkte fra sak/arkivsystem Elements. Revisor har ikke hatt tilgang til, eller gjennomgått Elements med tanke på databehandleravtaler.

Organisasjonssjefen sier at han ikke har oversikt på databehandleravtalene, det er det kommunalsjefene, som systemeiere, som ivaretar. De eier både selve avtalen og eventuelle databehandleravtaler som hører til det aktuelle systemet.

Kommunalsjef for helse og omsorg mener at det har vært en grundig gjennomgang innen hennes område, og de er så å si i mål med dette. Alle systemer er gjennomgått i DraftIT og det er registrert databehandleravtaler.

Etter et tilsyn fra Datatilsynet i skolene, ble det satt i verk et arbeid med blant annet databehandleravtaler. Ifølge kommunalsjef oppvekst var lite på plass, og databehandleravtaler

[19] Per 10.07.2026
[20] DFØ = Direktoratet for forvaltning og økonomistyring

har blitt prioritert først når det gjelder oppfølging av tilsynet. Foreløpig, forteller kommunalsjefen, er avtalene i Teams, men de skal inn i Draftit etter hvert.

Kommunalsjef for samfunn viser til at det er den virksomheten som anskaffer og bruker systemet som sørger for databehandleravtaler. Hun mener at dette skal være i orden. Hun har ikke vært inne og sjekket om det er på plass.

Funn om personvernkonsekvensvurderinger (DPIA)

I Compilo er det en prosedyre for vurdering av personvernkonsekvenser (DPIA), med mal for vurdering av personvernkonsekvenser, se figuren nedenfor.

Vurdering av personvernkonsekvenser				
Innledende DPIA	**Systematisk beskrivelse**	**Nødvendighet og rimelighet**	**Risiko for de registrerte**	**Ledelsens validering**
Foreligger det høy risiko?	Systematisk beskrivelse av behandlingen (art, omfang, formål og sammenheng)	Oppfyller behandlingen personvern-prinsippene Står behandlingen i et rimelig forhold til formålene	Hva er personvernkonsekvensene for de registrertes rettigheter og friheter?	Hva er innstillingen til ledelsen? Hvilke vurderinger har ledelsen gjort? Har ledelsen godkjent DPIA?

Figur 5. Prosedyre for vurdering av personvernkonsekvenser (DPIA).

Kilde: Compilo, Malvik kommune

Tabellen er etterfulgt av en beskrivelse av de ulike fasene i DPIA-vurderingene. Det er også en veileder for DPIA i Compilo, som skal bidra til at malen blir brukt konsistent mellom virksomhetene. De skal også sikre at nødvendige personvernvurderinger gjennomføres på en god måte.

Det er én[21] utfylt DPIA som er oppført i Draftit. Den er for Bedriftshelsetjenesten.

Organisasjonssjefen sier at det har vært kontakt med leverandør for mulig import av DPIA basert på ulike maler som er tilgjengelig hos KS, DFØ og flere. Bakgrunnen for henvendelsen til Draftit er at KS med flere opererer med såkalte 80 % DPIA som hjelper oss langt på vei med å få gjennomført risikovurderingene. En importmulighet vil spare alle brukere av Draftit for mye arbeid, ifølge organisasjonssjefen.

[21] Fire etter 28.08.2026

Personvernombudet forteller i intervju at det jobbes med en del DPIA, men at det ikke er ferdigstilt så mange. Hun har ikke uttalt seg om noen DPIA-er i Malvik kommune det siste året. Hun kan få spørsmål om å se over aktuelle DPIA for å se om noe mangler. DPIA-ene framstår ofte som generelle, og hun har gitt tilbakemelding om flere punkter som må fylles inn før hun kan uttale seg. Hun prøver å veilede, slik at kommunene blir bedre til å gjøre jobben selv. Hun har ikke oversikt over behandlingsaktiviteter, og derfor heller ikke hvilke DPIA som mangler. Manglende oversikt over behandlingsaktiviteter, DPIA-er og digitale læringsverktøy var et tema hun ønsket å synliggjøre i årsrapporten fra personvernombudet.

Kommunalsjef oppvekst og kultur forteller at arbeidet med DPIA-er foreløpig er lagt noe på is. Kommunen har valgt å prioritere ferdigstillelse av databehandleravtalene. Hun sier at det finnes en plan for videre arbeid hvor VarIT deltar, men at hun ikke kjenner detaljene i gjennomføringen.

2.4.3 Revisors vurdering

Personvernombud og personvernkontakter

- Kommunen skal ha et personvernombud
  - Det skal sikres nødvendig uavhengighet for personvernombudet
  - Personvernombudet skal sikres nødvendige ressurser for å utføre minimumoppgaver
  - Kommunen skal ha rutiner for personvernombudets arbeid som sikrer involvering og regelmessig dialog med ledelsen.

Revisor vurderer at kommunen har etablert en ordning med personvernombud.

Ordningen med personvernombud gjennom Værnesregionen ble etablert i 2025, og er relativt ny. Det framstår som at det kan være behov for avklaring av ansvaret mellom personvernombudet, vertskommunen og ledelsen i Malvik kommune på flere områder, som ansvar overfor personvernkontakter, ansvar for protokoller og databehandleravtaler.

Revisor vurderer revisjonskriteriet som oppfylt, men at det kan være behov for ytterligere ansvarsavklaringer mellom personvernombudet, vertskommunen og Malvik kommune.

Revisor vurderer at personvernombudet er sikret uavhengighet, ved at det er organisert gjennom vertskommunesamarbeid i Værnesregionen.

Revisor baserer sine vurderinger på at personvernombudet er organisert utenfor Malvik kommunes organisasjon, og at personvernombudet ikke har andre funksjoner i Malvik kommune som stille spørsmål ved uavhengigheten.

Revisor vurderer at revisjonskriteriet er oppfylt.

Revisor vurderer at personvernombudet i hovedsak er sikret minimumsressurser for å utføre funksjonen som personvernombud.

Personvernombudet har 50 % stillingsressurs for seks kommuner. Revisors forbehold gjelder om det er tilstrekkelig ressursomfang, ettersom at det ikke ble utvidet ressurser for å utføre funksjonen etter at Malvik gikk inn i samarbeidet i tillegg til de fem andre kommunene.

Malvik kommune har syv personvernkontakter i egen organisasjon som skal ivareta løpende rådgivning i personvernspørsmål overfor ansatte innen sitt virksomhetsområde, og bistå med å holde oversikt over behandlinger innenfor sitt område. Etter revisors vurdering styrker ordningen med personvernkontakter veiledning og rådgivning rundt personvern og personopplysninger i organisasjonen.

Revisor vurderer at revisjonskriteriet i hovedsak er oppfylt.

Revisor vurderer at det er etablert rutiner for personvernombudets arbeid, som sikrer involvering og regelmessig dialog med ledelsen.

Etter revisors vurdering er dette sikret gjennom samarbeidsavtalen (vertskommuneavtale) og beskrivelse av personvernombudets rolle i dokumentet Roller og ansvar. Personvernombudet er jevnlig til stede i rådhuset i Malvik kommune, og er der tilgjengelig for ledelsen. Personvernombudet har tettest kontakt med organisasjonssjefen. Etter revisors vurdering har personvernombudet rapportert til deltakerkommunene i personvernombudets årsrapport for 2025. Det har ikke vært saker i kommunestyret i perioden etter at ordningen ble etablert som tilsier at kommunestyret får rapport fra vertskommunen per tertial eller årsrapport.

Personvernombudet har i liten grad en formalisert kontakt med personvernkontaktene. Personvernkontaktrollen framstår som etablert, men fortsatt relativt ny og ulikt praktisert på tvers av områdene, noe som tyder på at ordningen fortsatt er i en innførings- og modningsfase.

Til tross for manglene som er påpekt, vurderer revisor at revisjonskriteriet i hovedsak er oppfylt.

Protokoll over behandlinger

- Kommunen skal føre protokoll over hvilke personopplysninger de behandler, som minimum inneholder obligatorisk informasjon.

Revisor vurderer at kommunen i noen grad fører protokoll over personopplysninger som de behandler

Etter revisors vurdering er det etablert system for å føre protokoll over behandlinger, men i praksis føres det i varierende grad protokoller over behandlinger av personopplysninger i virksomhetene. 39 protokoller er en liten del av alle system som det bør være protokoller for i en kommune som Malvik.

Revisor vurderer t revisjonskriteriet er delvis oppfylt.

Databehandleravtaler

- Kommunen skal ha databehandleravtaler som minimum inneholder obligatorisk informasjon

Revisor vurderer at arbeidet med databehandleravtaler delvis er fulgt opp.

Databehandleravtaler for det enkelte system er knyttet til sak- og arkivsystemet. Revisor har ikke sjekket det systemer. Kommunalsjefene har i varierende grad oversikt over databehandleravtaler innenfor sitt område.

Revisor vurderer at revisjonskriteriet er delvis oppfylt.

Vurdering av personvernkonsekvenser (DPIA)

- Kommunen skal gjennomføre en vurdering av personvernkonsekvenser ved behandlinger som vil medføre høy risiko for fysiske personers rettigheter og friheter

Revisor vurderer at DPIA-er i varierende grad gjennomføres.

Det er fra øverste ledelse lagt til rette med beskrivelser i prosedyre for hvordan DPIA skal utføres. I praksis er det i varierende grad prioritert

Revisjonskriteriet er delvis oppfylt.

2.5 Opplæring og informasjon

2.5.1 Revisjonskriterium

- Kommunen bør sørge for at ansatte får tilstrekkelig opplæring i og informasjon om informasjonssikkerhet og personvern, herunder om bruk av kunstig intelligens.

Mer om utledningen av revisjonskriterium finnes i vedlegg 1.

2.5.2 Funn

I dokumentet Roller og ansvar, er det tydeliggjort at sikkerhetsansvarlig i Malvik kommune (organisasjonssjef) blant annet har ansvar for å påse at det gjennomføres opplæringstiltak for

å ivareta tilfredsstillende informasjonssikkerhet og personvern. Dokumentet beskriver også at IT-leder har, sammen med øvrige ansatte i IT-avdelingen, ansvar for å bistå med faglig støtte til resten av organisasjonen, for eksempel opplæringstiltak. Videre har systemansvarlig ansvar for å bidra til gjennomføring av opplæringstiltak, både i bruk av systemet og for å ivareta tilfredsstillende informasjonssikkerhet og personvern. Leder med personalansvar skal ifølge dokumentet sørge for at ansatte gjennomgår nødvendig opplæring innen informasjonssikkerhet og personvern. Ansatte har ansvar for å delta i opplæringen.

Kommunen har utarbeidet en strategisk kompetanseplan, som er vedtatt i kommunestyret i mai 2026. Her er informasjonssikkerhet eksplisitt nevnt som en del av den digitale kompetansen kommunen trenger: Digital kompetanse skal bidra til produktivitet, kvalitet og informasjonssikkerhet. Ansatte skal kunne bruke digitale verktøy effektivt, sikkert og profesjonelt og ha forståelse for risiko knyttet til digital teknologi. Personvern er ikke nevnt eksplisitt eller er konkretisert som eget opplæringsområde i kompetanseplanen.

Kommunen har utarbeidet en veileder i kunstig intelligens (KI). Formålet med veilederen beskrives i følgende punkt:

- Sikre at ansatte bruker, og innbyggere behandles, av KI-verktøy på en sikker og ansvarlig måte.
- Sikre at ansatte og virksomhetsområder i kommunen som benytter KI har kontroll på at systemer som benytter kunstig intelligens i virksomheten opererer innenfor prinsippene for ansvarlig og pålitelig bruk av KI.
- Sikre at KI brukes på en måte som er åpen og ansvarlig. Dette betyr at man både som ansatt og innbygger skal være informert om hvordan KI blir brukt i og av kommunen, og hvem som er operativt ansvarlig for bruken av de ulike verktøyene ved behov for informasjon.
- Sikre at KI-løsninger kommunen benytter følger nasjonale krav og anbefalinger, og at kommunens retningslinjer for bruk av KI etterfølges, med særlig oppmerksomhet på personvernrelaterte problemstillinger
- Sørge for at kunstig intelligens som utvikles og brukes i kommunens regi bygger på etiske prinsipper, og respekterer menneskerettighetene, personvernet og demokratiske prinsipper.

I veilederen framgår det kjøreregler, om hva som bør gjøres og hva som ikke bør gjøres. Videre er det utvidete retningslinjer som gjelder for de som skal anskaffe, forvalte eller implementere KI i Malvik kommune.

Ifølge organisasjonssjefen ønsker kommunen å få opp modenheten og at ansatte utforsker potensialet som ligger i KI, men da innenfor tydelig rammer. Han sier at VarIT også ønsker å etablere et digitaliseringsråd, fordi de ser at KI brukes utenfor infrastrukturen.

Han viser også til at tre ansatte tar kurs på ved NTNU (NorwAI) om innovasjon med store språkmodeller.

Organisasjonssjefen sier at det ikke er oversikt over den eksakte bruken av KI i organisasjonen. Copilot er det lisensierte produktet som skal/kan brukes. De som ønsker lisensversjonen av Copilot må be spesifikt om det. Alle har tilgang til Copilot i Edge når de er pålogget.

Kommunalsjef for oppvekst forteller at noen skoler har hatt deltakere i kurs om bruk av KI i opplæringen. Rådgiver i administrasjonen i oppvekst har utarbeidet en veileder for bruk av KI i opplæringen.

Også ved de andre rammeområdene har det vært opplæringstiltak i KI, og det brukes i varierende grad.

På kommunens intranett - Innsida – er det en egen fane som omhandler informasjonssikkerhet og personvern som er tilgjengelig for alle ansatte. Her er det tilgang på kurs både i personvern og informasjonssikkerhet via kursportalen GLUP[22]

Det har vært gjennomført Nano-opplæring om informasjonssikkerhet i 2024/2025, som ble distribuert på e-post til alle ansatte.

Revisor har fått oversendt dokumentasjon på at kommunen i 2023 gjennomførte simulert phising via epost. De som klikket på lenken (ca. 13 %), ble rutet videre til opplæring som omhandlet phising.
I et skjema for dokumentasjon som vi har fått oversendt fra organisasjonssjefen, går det fram at alle virksomhetsledere fikk tilbud om kurs i regi av Nasjonal sikkerhetsmyndighet (NSM) i 2022, som omhandlet grunnprinsipper for informasjonssikkerhet. Kommunen har ikke fått noen oversikt fra NSM om deltakelsen. Det går fram at samtlige kommunalsjefer og kommunedirektør gjennomførte kurset.

Det blir i intervju fortalt at lederne flere ganger er blitt informert om gratis kursing gjennom Digital Norway og Visma Draftit. Kommunen har ingen kompetanseportal der de kan se graden av gjennomføring. Det er derfor ikke mulig å spore hvor mange ansatte som faktisk har gjennomført kursene. Kommunen innfører KS kunnskap i 2026 i samarbeid med øvrige kommuner i Værnesregionen

[22] GLUP = læringsplattform for offentlig sektor distribuert av Smartskill.

Flere av personvernkontaktene forteller at de har fått informasjon om rolle og rolleforståelse gjennom møte med personvernombudet, digitale kurs, konferanse eller samtaler med leder. Samtidig oppgir enkelte at de ikke har fått egen eller utfyllende opplæring, og at de ønsker mer avklarte forventninger til rollen.

2.5.3 Revisors vurdering

- Kommunen bør sørge for at ansatte får tilstrekkelig opplæring i og informasjon om informasjonssikkerhet og personvern, herunder opplæring i bruk av kunstig intelligens.

Revisor vurderer at kommunen legger til rette for opplæring i informasjonssikkerhet, også i KI, men mangler oversikt over ansattes gjennomføring av kompetansetiltak innen disse områdene.

Informasjonssikkerhet inngår som en del av den generelle digitale kompetansen i strategisk kompetanseplan.

Personvern kan anses implisitt berørt gjennom krav om sikker bruk av digitale systemer og risikoforståelse i digitalt arbeid.

Det er utarbeidet veileder i bruk av KI, og kommunen har til en viss grad opplæringstiltak for ledelse og ansatte i bruk av KI. Etter revisors vurdering følger ledelsen ikke opp hvem/hvor mange som har gjennomført opplæringen.

Revisjonskriteriet er i hovedsak oppfylt.

3 VERTSKOMMUNESAMARBEID

3.1 Problemstilling

Det er utarbeidet følgende problemstilling:

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

3.2 Avtaler med vertskommunen

3.2.1 Revisjonskriterier

- Det skal være inngått samarbeidsavtale og eventuelt andre avtaler som er tydelig på myndighet, ansvar og oppgaver, og som er oppdatert i henhold til gjeldende regelverk.
- Det bør være regelmessig samhandling mellom VarIT og Malvik kommune, hvor informasjonssikkerhet og personvern er ivaretatt.
- Malvik kommune bør påse at tjenestene fra VarIT styres etter en virksomhetsplan med mål og resultatkrav.
- Malvik kommune bør påse at kommunedirektøren i vertskommunen rapporterer til kommunestyret i Malvik per. tertial (herunder årsrapport) i henhold til avtalen.

Utledning av kriterier finnes i vedlegg 1.

3.2.2 Funn

Samarbeidsavtale

Fem kommuner (samarbeidskommuner [23]) har inngått samarbeidsavtale med Stjørdal kommune (vertskommune) om IKT-tjenester i Værnesregionen IKT (VarIT). Avtalen har lik ordlyd for alle samarbeidskommunene, men er en bilateral avtale mellom Stjørdal kommune som vertskommune og den enkelte samarbeidskommune. Avtalen som Malvik kommune har inngått med Stjørdal kommune, er hjemlet i kommuneloven § 20-2 om administrativt vertskommunesamarbeid og er datert i mai 2024.

Avtalens formål (kapittel 1) er blant annet beskrevet slik: «Værnesregionen IKT skal bidra til at kommunene når følgende mål:

- Kostnadseffektiv utførelse av tjenesten.
- En tjeneste med god service og tilgjengelighet for brukerne.

[23] Kommunene Tydal, Frosta, Meråker, Selbu og Malvik

- Økt kvalitet og høy faglig kompetanse.
- Redusert sårbarhet i tjenesteytingen.
- Utvikle tjenesten i tråd med sentrale føringer.»

Vertskommunens ansvar overfor samarbeidskommunen er regulert i kapittel 5 i avtalen. Den sier at vertskommunen ved kommunedirektøren skal:

- Være arbeidsgiver for ansatte, administrasjon og leder i Værnesregionen IKT.
- Drifte alle tjenester i samarbeidet basert på nødvendige delegasjoner.
- Stille til disposisjon nødvendige bygg og utstyr for det interkommunale samarbeidet.
- Stille til disposisjon nødvendige støttefunksjoner for drift av det interkommunale samarbeidet.
- Utarbeide en virksomhetsplan med mål og resultatkrav. Planen skal beskrive de tiltak som planlegges for å få en god måloppnåelse, herunder forventet ressursinnsats.
- Inngå nødvendige kontrakter /avtaler for drift av Værnesregionen IKT på vegne av deltakerkommunene.
- Organisere kunde- og publikumskontakt for alle kommuner i forbindelse med de oppgaver som er lagt til vertskommunen, herunder veiledning, utarbeide relevant informasjonsmateriale m.m.
- Ha arkivansvar for Værnesregionen IKT påse at arkivering utføres i henhold til arkivloven.
- Annet arbeid som står i naturlig sammenheng med avtalens virkeområde, herunder innkjøp av utstyr, konsulenttjenester m.m.
- Utarbeide regnskap for drift av Værnesregionen IKT. Regnskapet føres som eget regnskap i vertskommunens driftsregnskap.
- Utarbeide budsjett for tjenesten etter politiske føringer gitt i strategisamlinger med alle kommuner.

I kapittel 6 er det beskrevet hvilke oppgaver som ikke faller inn under vertskommunens ansvar. Det kan for eksempel være vedtak av planer for den enkelte deltakerkommune, og nivå på tjenesteinnhold og tjenester direkte rettet mot den enkelte innbygger.

I kapittel 7 er organiseringen av Værnesregionen IKT beskrevet. Tjenesten er underlagt en enhetsleder i vertskommunen, som har delegert myndighet for drift, personal og økonomi. De ansatte skal som hovedregel møte ved hovedkontoret (vertskommunen). Den enkelte deltakerkommune stiller med lokaliteter/avdelingskontor ved behov, og med nødvendig utstyr for tjenesten i den enkelte kommune.

Det finnes også en generell samarbeidsavtale mellom Malvik kommune og Stjørdal kommune om vertskommunesamarbeid i Værnesregionen. I intervju sier IT-leder i VarIT at det har blitt tatt opp i arbeidsutvalget for Værnesregionen at den generelle avtalen skal gjennomgås.

Organisasjonssjefen i Malvik forteller at han ikke var involvert i arbeidet med den overordna vertskommuneavtalen, men deltok aktivt i prosessen med vertskommuneavtale om IKT. Prosessen pågikk i omtrent ett år, og startet med en utredning om det ville være økonomisk og forvaltningsmessig fornuftig å gå inn fra Malvik sin side. Kommunen hadde en del etterslep når gjaldt sikkerhetsanskaffelser. Anskaffelsene ble satt på vent, inntil det ble tatt beslutning om kommunen skulle bli en del av IT-samarbeidet i Værnesregionen. Saken ble lagt fram til politisk behandling i 2024. Det var Malvik sin daværende IT-leder og leder i VarIT som gjorde den store kartleggingsjobben både i forhold til tekniske løsninger og mulige økonomiske fordeler av et samarbeid. Organisasjonssjefen beskriver sammenslåingen som en omfattende prosess, der infrastruktur, systemer og applikasjoner skal forvaltes fra samme sted er et omfattende arbeid. Jobben med migrering startet i januar.2025, og blir avsluttet våren 2026.

Organisasjonssjefen forteller videre at det er inngått nødvendige avtaler for drift av IKTtjenester, og at flere avtaler er blitt systematisert og harmonisert etter at kommunen gikk inn i samarbeidet. Han viser til pågående arbeid med å få bedre oversikt over hvilke avtaler som ligger innenfor og utenfor samarbeidet.

Ifølge IT-leder i VarIT er ikke avtalen om IKT evaluert siden Malvik kom inn. Hun er [u]sikker på om avtalene er revidert tidligere. IT-leder gir uttrykk for at det mangler synliggjøring i avtalene at kommunene må følge rutiner og retningslinjer hos VarIT, da dette er uklart. Hun mener at det burde være slik at alt innenfor sikkerhet og personvern er gjeldende på tvers og for alle VarIT-kommunene.

IT-leder forteller at det er usikkert om det finnes en databehandleravtale med Malvik. Alt av fagsystem må ha en databehandleravtale, og dette hadde Malvik kommune selv før de kom inn. Systemer som blir anskaffet nå, er det VarIT som har ansvar for databehandleravtale for.

Regelmessig samhandling mellom VarIT og Malvik kommune

Flere informanter beskriver i intervju at ansvarsfordelingen mellom kommunen og VarIT i hovedsak er kjent og fungerer tilfredsstillende som grunnlag for samarbeidet. VarIT opplyser at de har ansvar for drift, sikkerhet og fagutvikling, og at de stiller sikkerhetskrav ved anskaffelser og leverandøravtaler.

VarIT opplyser at hver kommune har en egen hovedansvarlig kontaktperson, at det blir gjennomført månedlige møter med kommuneansvarlige, og at VarIT deltar i kommunenes sikkerhetsorganisasjon.

Organisasjonssjefen beskriver faste månedlige møter med kommunens kontaktperson i VarIT, der aktuelle problemstillinger blir drøftet. Han opplyser også at spørsmål knyttet til utvikling, sikkerhet og eventuelle utfordringer blir løftet til arbeidsutvalget i Værnesregionen. Han sier at kommunen og VarIT har hatt diskusjoner knyttet til balansen mellom utvikling og sikker drift, særlig innen digital transformasjon og bruk av kunstig intelligens. Han viser til at slike spørsmål blir håndtert gjennom etablerte dialogarenaer.

Kommunalsjef samfunn opplyser at hun har kontakt med både leder i VarIT og Malviks kontaktperson i VarIT, blant annet knyttet til arbeid med digitalsikkerhetsregelverket. Hun beskriver også at leder for VarIT deltar i ledergruppen i Malvik kommune, der samarbeidet blir diskutert.

Kommunalsjef helse beskriver at rollene mellom kommunen og VarIT oppleves som avklart, samtidig som det på enkelte områder blir arbeidet med ytterligere tydeliggjøring av roller som systemeier og systemansvarlig.

Digitaliseringslederen i Malvik beskriver samhandlingen med VarIT som tidvis utfordrende. Han opplever at VarIT er et viktig fagmiljø og en viktig rådgiver i spørsmål om informasjonssikkerhet og teknologi. Samtidig mener han at beslutninger om [akseptert] risiko og utvikling må eies av kommunen. Han peker på at begrenset tilgang til enkelte systemer og data kan forsinke kommunens utviklingsarbeid, og etterlyser større rom for testing og innovasjon. Samtidig understreker han betydningen av gjensidig respekt for fagkompetansen på begge sider av samarbeidet.

I intervju med VarIT spurte revisor hva de mener haster for Malvik. Da blir det sagt at Malvik kommune er mye bedre rustet nå enn de var før de kom inn i VarIT. Regelverk og avklaring av bruk av KI, samt kompetanseløft på generell basis om informasjonssikkerhet (kompetanseplaner fra HR) ble nevnt som områder det haster å få avklart. VarIT forteller også at de er usikre på hvor mye ansatte i Malvik får med seg av hva VarIT legger ut på intranettet.

Virksomhetsplan

I kapittel 5 i samarbeidsavtalen er et av punktene formulert slik: «Vertskommunen ved kommunedirektøren skal (…) utarbeide en virksomhetsplan med mål og resultatkrav. Planen skal beskrive de tiltak som planlegges for å få en god måloppnåelse, herunder forventet ressursinnsats.» Organisasjonssjefen forteller i intervju at han ikke er kjent med at det er utarbeidet virksomhetsplan innenfor samarbeidet om IKT-tjenester. Leder for VarIT sier at hun heller ikke er kjent med dette.

Rapportering fra vertskommunen

Kapittel 8 i samarbeidsavtalen omhandler rapportering. Her går det fram at tjenesten skal rapportere til kommunedirektøren i vertskommunen, som skal rapportere til kommunestyrene

i deltakerkommunene hvert tertial, inklusive årsrapport. Revisor kan ikke finne at det er rapportert til kommunestyret om samarbeidet i kommunestyrets protokoller i 2025 og 2026.

3.2.3 Revisors vurdering

Følgende kriterier er vurdert i lys av funnene:

- Det bør være avtaler som er tydelig på myndighet, ansvar og oppgaver, og som er oppdatert i henhold til gjeldende regelverk, når det gjelder informasjonssikkerhet og personvern.

Revisor vurderer at Malvik kommune har inngått samarbeidsavtale (vertskommuneavtale) om IKT-tjenester, i tillegg til overordna vertkommuneavtale om tjenester i Værnesregionen, men avtalen er ikke tydelig nok på myndighet, ansvar og oppgaver.

Basert på intervjuinformasjon kan det tyde på at avtalene ikke er tilstrekkelig tydelige på ansvar, myndighet og oppgaver på enkelte områder innen informasjonssikkerhet og personvern.

Revisor vurderer at kriteriet er delvis oppfylt.

- Det bør være regelmessig samhandling mellom VarIT og Malvik kommune, hvor informasjonssikkerhet og personvern er ivaretatt.

Revisor vurderer at det er regelmessig samhandling mellom den sentrale ledelsen i Malvik kommune og VarIT.

Samhandlingen skjer gjennom faste, månedlige møter, faste kontaktpersoner i begge organisasjonene og deltakelse fra VarIT i kommunens sikkerhetsorganisasjon. Intervjudata viser at samhandlingen på noen punkter er utfordrende. Revisor vurderer at utfordringene i samhandlingen blant annet henger sammen med at ansvar og myndighet ikke er tilstrekkelig avklart, og at det eksisterer et spenningsforhold mellom krav til sikker drift og behovet for digital utvikling.

Revisor vurderer at kriteriet er innfridd.

- Malvik kommune bør påse at tjenestene fra VarIT styres etter en virksomhetsplan med mål og resultatkrav.

Revisor vurderer at Malvik kommune ikke påser at IKT-tjenesten styres etter en virksomhetsplan med mål og resultatkrav.

Vurderingen er basert på at informantene i intervjuer forteller at det ikke er utarbeidet en virksomhetsplan, slik samarbeidsavtalen stiller krav om.

Revisor vurderer at kriteriet ikke er innfridd.

- Malvik kommune bør påse at kommunedirektøren i vertskommunen rapporterer til kommunestyret i Malvik per. tertial (herunder årsrapport) i henhold til avtalen.

Revisor vurderer at Malvik kommune ikke påser at kommunedirektøren i Stjørdal rapporterer til kommunestyret i Malvik kommune.

Vurderingen bygger på at samarbeidsavtalen stiller krav om en slik rapportering. Revisor baserer vurderingen på at vi ikke finner saker i kommunestyret i 2025 og 2026 (e-innsyn), som tilsier at det er rapportert i henhold til samarbeidsavtalen.

Revisor vurderer at kriteriet ikke er innfridd.

3.3 Vertskommunesamarbeid om organisatoriske og tekniske tiltak

3.3.1 Revisjonskriterier

Malvik kommune bør forsikre seg om at sikkerhetsstyring av organisatoriske og tekniske tiltak i vertskommunesamarbeidet er ivaretatt, ved at det er:

- oversikt over enheter, programvare og tilganger (identifisere og kartlegge)
- sikkerhet i anskaffelser, tjenesteutsettelse, IKT-arkitektur og sikkerhetsoppdateringer (beskytte og oppdatere)
- kontroll av sikkerhetstilstand og ledelsens gjennomgang (oppdage)
- håndtering, gjenoppretting og læring av hendelser (håndtering og gjenoppretting).

Utledning av kriterier finnes i vedlegg 1.

3.3.2 Funn

Oversikt over enheter, programvare og tilganger (identifisere og kartlegge)

Følgende dokumentasjon fra VarIT er gjort tilgjengelig for revisor:

- Styrende retningslinjer for autentisering
- Retningslinje for autentiseringsinformasjon (passordpolicy)
- Retningslinje for tilgangsstyring
- Konto/databruker ansatt (arbeidsflyt for oppretting av konto)

Følgende dokument er gjort tilgjengelig via Malvik kommune sitt styringssystem, der det er anført at kommunedirektør eller kommunalsjef er ansvarlig for innholdet:

- Policy for fysisk sikkerhet

Følgende dokumenter er gjort tilgjengelig via Malvik kommune sitt styringssystem, der det er anført at VarIT er ansvarlig for innholdet:

- Policy for autentiseringsinformasjon (passordpolicy)
- Policy for tilgangsstyring
- Prosedyre for sårbarhetskartlegging av IT-systemer
- Prosedyre for tidssynkronisering

VarIT sier i intervju at de har oversikt over alle enheter. Det er en spesial-PC på vann og avløp i Malvik kommune som var utenfor domene som VarIT ikke har kontroll på, alt annet som er i domene har de kontroll på. På defender går de over til Centinell i løpet av mai og da får de alt inn i MS-portalen.

Når det gjelder oversikt over programvare, er dette noe varierende. Men VarIT sier at de har god kontroll, og at alle PCer knyttet til Intune. Dette er Microsofts skybaserte løsning for administrasjon og sikring av enheter og apper. De bruker også Admin by request[24] og har sporbarhet på tilgangene.

VarIT sier videre at tilgangsstyring skjer gjennom lønnssystemet. Det kan skje at noen får tilganger utenom, for eksempel studenter i helsetjenestene. Det er interne rutiner for at konsulenter ikke får tilgang i mer enn to uker om gangen. VarIT forteller at de har hatt opprydding av dette i Malvik. Etter deres vurdering har Malvik kommune hatt veldig mye å hente på sikkerhet ved å komme inn i samarbeidet.

Sikkerhet i anskaffelser, tjenesteutsettelse, IKT-arkitektur og sikkerhetsoppdateringer (beskytte og oppdatere)

Følgende dokument er gjort tilgjengelig via Malvik kommune sitt styringssystem, der kommunedirektør er ansvarlig for innholdet:

- Policy for anskaffelse og forvaltning av programvarelisenser

Følgende dokumenter er gjort tilgjengelig via Malvik kommune sitt styringssystem, der et er anført at VarIT er ansvarlig for innholdet:

- Policy for bruk og sikring av brukerutstyr
- Policy for flyttbare lagringsmedier
- Policy for informasjonsoverføring

[24] Admin By Request er et sikkerhetsverktøy for styring av administratorrettigheter. Hensikten er at brukere ikke skal ha permanente lokale administratorrettigheter, men kan få midlertidig tilgang når det er nødvendig.

- Policy for bruk av skytjenester
- Policy for informasjonssikkerhet i leverandørforhold
- Policy for kryptografi
- Policy for nettverkssikkerhet

I intervju med VarIT kommer det fram at de stiller sikkerhetskrav til leverandører og deltar i et økende antall anskaffelsesprosesser for å ivareta sikkerhet ved innkjøp av systemer og tjenester. Når det gjelder it-tjenestenes involvering i alle anskaffelser, sier VarIT at det kan glippe. Det er VR Innkjøp som har ansvar for å kople VarIT på, i tillegg til fagaktører.

Det kommer samtidig fram en usikkerhet knyttet til om avtalene i tilstrekkelig grad tydeliggjør at kommunene skal følge VarIT sine rutiner og retningslinjer. Informantene peker på at sikkerhet og personvern ideelt sett bør gjelde likt for alle kommunene i samarbeidet.

Organisasjonssjefen gir uttrykk for at så lenge VarIT blir involvert i anskaffelser, er han trygg på at sikkerheten blir ivaretatt. Det er ikke noe stort omfang av anskaffelser som ikke VarIT er involvert i. Den største bekymringen er at ansatte ikke bruker styringssystemet når anskaffelser skal gjøres. Styringssystemet skal hjelpe til med å gjøre de riktige valgene til rett tid. VarIT har ikke ansvar for anskaffelsen hvis ikke systemet skal brukes i alle kommuner, og da er de mer rådgiver overfor kommunen i forhold til hva som må være på plass. Han sier at det er opp til kommunens selv å beslutte om de skal gå for egne systemer eller ikke.

VarIT forteller at de drifter alt på vegne av Malvik kommune, inklusive servere og nettverk. Når det gjelder databehandleravtaler, opplyser VarIT at de har ansvar for databehandleravtaler til systemer som er anskaffet etter at kommunen kom inn i samarbeidet.

VarIT opplyser at de har brannmurer, sikker sone og antivirus i orden. Det er for eksempel geoblokking i Azure (Microsofts skyplattform), som begrenser tilgang basert på geografisk plassering. Sikkerhetsoppdateringer gjøres automatisk, men noen programmer må oppdateres manuelt 3-4 ganger i året. HelseCert er flink til å sende ut varslinger. Det blir sagt at VarIT har overordnet retningslinje for sikkerhetskopiering.

VarIT forteller videre at de som arbeider med nettverk er flinke til å dokumentere arkitekturen, og at de har god oversikt. De forteller at Malvik kommune ønsker å bruke Ardoq, som er et system for virksomhetsarkitektur. VarIT forteller at de har ikke rukket å prioritere å innføre dette.

Organisasjonssjefen i Malvik forteller i intervju at kommunen har anskaffet Ardoq for å få oversikt over systemer og avtaler. Før migreringen ble systemer, applikasjoner og teknisk infrastruktur dokumentert i Ardoq, for å få en oversikt over hva som skulle migreres eller ikke. Han sier at de akkurat nå «veiver vi litt i blinde» for å følge opp styringssystemet og databehandleravtaler, og at det nok mangler en helhetlig gjennomføring fordi dette arbeidet

skal gjøres i tillegg til alt annet ledelsen har ansvar for. Digitaliseringslederen i Malvik mener at VarIT har betydelig etterslep med å få kontroll på virksomhetsarkitekturen.

Kontroll av sikkerhetstilstand og ledelsens gjennomgang (overvåke og oppdage)

Følgende dokumenter er gjort tilgjengelig via Malvik kommune sitt styringssystem, der det er anført at VarIT er ansvarlig for innholdet:

- Policy for logging
- Prosedyre for innhenting av trusselinformasjon
- Prosedyre for håndtering av digitale bevis

I intervju med VarIT kommer det fram at de har et ansvar for sikkerhet på tvers av deltakerkommunene, og rapporterer om sikkerhet til kommunedirektørutvalget (AU). Dette indikerer løpende oppfølging og kontroll av sikkerhetstilstanden. Det framgår også av andre intervjuer at VarIT overvåker sikkerhetshendelser kontinuerlig, og samarbeider med Atea om overvåkning av forsøk mot brannmurer. Dette har blitt presentert av VarIT i kommunens beredskapsråd.

SOC-tjenesten[25] som Atea leverer vurderer VarIT som viktig. VarIT har blant annet fått beskjed fra SOC om sperring på grunn av virusangrep, noe som ble oppdaget før de selv oppdaget det. VarIT forteller at de har en driftsvaktordning, som rulleres av fem personer på IT. SOCtjenesten og ansatte i helse kan henvende seg til denne driftsvakta.

Organisasjonssjefen sier at han er mye tryggere på overvåkningen nå, enn det han var før kommunen gikk inn i VarIT. Det er viktig å være eksplisitt på hva det er viktig å overvåke særskilt, og det har vært hendelser som har gjort at enheter er tatt ut på grunn av infisering. Det som ikke blir overvåket nå, er VA-systemene, som er viktig infrastruktur og operasjonell teknologi (OT). Der har kommunen startet et arbeid for å få oversikt. VarIT har ikke hatt en tydelig rolle på operasjonell teknologi, så her må kommunen selv ta ansvar. Etter at digitalsikkerhetsloven trådte i kraft 1.10.2025, har det vært flere møter mellom Malvik kommune og VarIT for å få situasjonsforståelse rundt ansvaret som ligger til IT og ansvaret som ligger til den enkelte kommune rundt OT-sikkerhet. Dette har resultert i en enighet om å spleise på en dedikert ressurs i VarIT som kan sørge for nødvendig OT-kompetanse og OT-sikkerhet.

Håndtering, gjenoppretting og læring av hendelser (håndtering og gjenoppretting)

Revisor har fått oversendt Beredskapsplan IT fra VarIT. Den inneholder blant annet beskrivelse av ansvar, roller, risikovurderinger av mulige uønskede hendelser og respons hvis hendelser oppstår.

[25] SOC er en tjeneste for kontinuerlig overvåking, oppdagelse og håndtering av sikkerhetshendelser i IT-miljøet

I dokumentet Roller og ansvar står det at sikkerhetsleder (organisasjonssjefen i Malvik kommune) blant annet har ansvar for å identifisere risikoområder og foreslå sikringstiltak, og å påse at det gjennomføres risikovurderinger. Videre står det at IT-leder (VarIT) har ansvar for å vedlikeholde IT beredskapsplan og å gjennomføre IT beredskapsøvelser sammen med sikkerhetsleder (organisasjonssjefen i Malvik) og beredskapsleder. I dokumentet står det også at beredskapskoordinator i kommunedirektørens fagstab er beredskapsleder, og skal sikre at beredskapsplanen er oppdatert, og koordinere og gjennomføre regelmessige beredskapsøvelser for å sikre at kommunen er forberedt på håndtering av alvorlige sikkerhetshendelser.

Følgende dokumentasjon fra VarIT er gjort tilgjengelig for revisor:

- Retningslinje for sikkerhetskopiering og gjenoppretting
- Beskrivelse av backupløsninger i Værnesregionen IT

Følgende dokument er gjort tilgjengelig via Malvik kommune sitt styringssystem, der det er anført at VarIT er ansvarlig for innholdet:

- Policy for sikkerhetskopiering og gjenoppretting

I intervju med VarIT blir ikke konkrete rutiner for gjenoppretting etter hendelser eller læring etter hendelser omtalt. Det blir fortalt at sikkerhetsansvarlig i VarIT har begynt med plan for kritikalitet og prioritering for gjenopprettelse. Han mener at ledelsen i kommunene ikke tar nok ansvar for dette, og at alle kommuner helst bør ha lik prioritering. Det er laget rutiner for hvordan kommunene sammen skal håndtere dette, da det er mange roller og funksjoner som kommunene har felles. De skal øve på dette i september i år, i øvelse Sodd. I Malvik skal de gjennomføre øvelse senere i høst, som VarIT skal delta på.

I intervju med VarIT blir det beskrevet at VarIT og kommunene er godt samstemte og samarbeider tett om sikkerhet og utvikling på tvers av regionen. VarIT peker samtidig på uklarheter i avtaleverket og behov for tydeligere regulering av ansvar og etterlevelse av felles sikkerhetsrutiner. VarIT forteller at de ønsker å etablere et regionalt digitaliseringsråd for å prioritere og styre utviklingsoppgaver på tvers av kommunene, noe som kan bidra til mer systematisk styring av både risiko og utvikling.

Når det gjelder spørsmål om opprettelse av digitaliseringsråd, svarer organisasjonssjefen i Malvik at det ikke noe mer håndfast om dette per i dag. Det er blitt snakket om, og slik han har oppfattet det er det leder av VarIT som skal legge frem en sak for AU om dette. Videre forteller organisasjonssjefen at kommunen hittil ikke har hatt øvelser sammen med VarIT, men at beredskapsrådgiver har kontakt med VarIT i forbindelse med øvelsen som er under planlegging og som skal gjennomføres høsten 2026.

Organisasjonssjefen sier at kommunen selv har gjort vurderinger når det gjelder gjenoppretting, der helse er førsteprioritet. Hva VarIT vil prioritere ved behov for gjenoppretting, er ikke avklart eller tydeliggjort. Før kommunen kom inn i samarbeidet hadde VarIT en øvelse på dette, men han sier at det er behov for å få dette bedre tydeliggjort. VarIT har ikke delt sin hendelsesplan med kommunen, da det ligger konfidensiell informasjon der.

3.3.3 Revisors vurdering

Følgende kriterier er vurdert i lys av funnene:

Malvik kommune bør forsikre seg om at grunnprinsippene for sikkerhetsstyring er ivaretatt:

- oversikt over enheter, programvare og tilganger (identifisere og kartlegge)

Revisor vurderer at oversikt over enheter, programvare og tilganger i hovedsak blir ivaretatt.

Revisor bygger vurderingen på at Malvik kommune, gjennom VarIT, i hovedsak har etablert rutiner og tekniske løsninger som gir oversikt over enheter, programvare og tilganger. Tilgangsstyring er regulert gjennom retningslinjer og arbeidsflyter, og VarIT opplyser at de har god kontroll over enheter og programvare som inngår i deres domene. Samtidig viser funnene at oversikten ikke er fullstendig. Enkelte enheter ligger utenfor VarITs kontroll, oversikten over programvare beskrives som noe varierende.

Revisor vurderer at kriteriet i hovedsak er oppfylt, men at det fortsatt gjenstår arbeid med å sikre en samlet og helhetlig oversikt over alle systemer, enheter, programvare og tilganger, samt retningslinjer og policyer.

- sikkerhet i anskaffelser, tjenesteutsettelse, IKT-arkitektur og sikkerhetsoppdateringer (beskytte og oppdatere)

Revisor vurderer at sikkerheten i anskaffelser, tjenesteutsettelse, IKT-arkitektur og sikkerhetsoppdateringer i hovedsak blir ivaretatt.

Basert på funnene revisor har gjort, vurderer vi at sikkerhet i anskaffelser, tjenesteutsettelse, IKT-arkitektur og sikkerhetsoppdateringer i delvis blir ivaretatt gjennom VarIT. VarIT drifter sentral infrastruktur, stiller sikkerhetskrav til leverandører og har etablert tekniske sikkerhetstiltak. Slike tiltak er blant annet brannmurer, sikker sone, antivirus, geoblokking, sikkerhetskopiering og automatiske sikkerhetsoppdateringer. Fra kommunens side er uttrykt usikkerhet rundt ivaretakelse av iKT-arkitekturen.

Revisors vurdering er at verktøy for system- og avtaleoversikt er ikke fullt ut tatt i bruk slik kommunen ønsker. Det er også en risiko for at VarIT ikke alltid blir involvert i anskaffelser, og

det er noe uklart om avtalene tydelig nok forplikter kommunene til å følge VarIT sine rutiner og retningslinjer.

Revisor vurderer at kriteriet er delvis oppfylt.

- kontroll av sikkerhetstilstand og ledelsens gjennomgang (oppdage)

Revisor vurderer at det i hovedsak er kontroll på sikkerhetstilstand og ledelsens gjennomgang gjennom samarbeidet mellom Malvik kommune og VarIT, men at det fortsatt gjenstår avklaringer rundt operasjonell teknologi innen viktige infrastrukturområder.

Revisor vurderer at kontroll av sikkerhetstilstanden og evnen til å overvåke og oppdage sikkerhetshendelser i hovedsak er ivaretatt gjennom samarbeidet med VarIT. Vurderingen bygger på at VarIT overvåker sikkerhetshendelser kontinuerlig, benytter ekstern SOC-tjeneste, har etablert driftsvaktordning og rapporterer om sikkerhet til kommunedirektørutvalget, men det gjenstår fortsatt noe arbeid for å sikre tilstrekkelig overvåking av alle kritiske systemer.

Samtidig viser funnene at overvåking og ansvarsforhold knyttet til operasjonell teknologi (OT) ikke er fullt ut avklart. Det er igangsatt prosesser og dialog mellom Malvik kommune og VarIT for å avklare dette.

Revisor vurderer at kriteriet i hovedsak er oppfylt,

- håndtering, gjenoppretting og læring av hendelser (håndtering og gjenoppretting)

Revisor vurderer at prinsippet for håndtering, gjenoppretting og læring av hendelser i noen grad er ivaretatt.

Revisor baserer vurderingen på at kommunen i noen grad ivaretar dette grunnprinsippet gjennom beredskapsplaner, ansvarsforhold og samarbeid med VarIT. Det foreligger en IT-beredskapsplan i VarIT med beskrivelser av roller, ansvar, risikovurderinger og respons ved uønskede hendelser. Malvik kommune har også definert ansvar for beredskap, risikovurderinger og gjennomføring av øvelser i sitt styringssystem.

Samtidig viser funnene at flere sentrale forhold ikke fullt ut er avklart mellom kommunen og VarIT. Kommunen har etablert et grunnlag for håndtering av hendelser, men arbeidet med gjenoppretting, samordning av prioriteringer og systematisk læring etter hendelser framstår ikke som tilstrekkelig avklart.

Revisor vurderer at kriteriet delvis er oppfylt.

4 KONKLUSJONER OG ANBEFALINGER

4.1 Konklusjon

I den første problemstillingen har revisor undersøkt og vurdert om Malvik kommune har etablert et styringssystem for informasjonssikkerhet og personvern som tilfredsstiller krav i regelverket.

Revisor konkluderer med at Malvik kommune i hovedsak har etablert et styringssystem som ivaretar krav i regelverket. Systemet har beskrivelse av sikkerhetsmål og sikkerhetsorganisasjon, men mangler beskrivelse av sikkerhetsstrategi. Informasjonssikkerhet og personvern inngår i kommunens internkontroll. Revisor konkluderer med at regelverket for personopplysninger i varierende grad er fulgt opp, med tanke på behandlingsprotokoller, personvernkonsekvensutredninger og databehandleravtaler.

Kommunen har opplæringstiltak i informasjonssikkerhet og personvern, herunder bruk av KI, men ansattes gjennomføring følges i liten grad opp.

For den andre problemstillingen konkluderer revisor med Malvik kommune i all hovedsak har etablert avtaler med og oppfølging av VarIT, som bidrar til å sikre organisatoriske og tekniske tiltak for informasjonssikkerhet og personvern. Samarbeidet er regulert gjennom vertskommuneavtaler, og det er etablert faste arenaer for samhandling mellom kommunen og VarIT. Revisjonen viser også at grunnprinsipper for sikkerhetsstyring i hovedsak er ivaretatt gjennom samarbeidet.

Samtidig avdekker revisjonen enkelte mangler i kommunens oppfølging av samarbeidet. Det er ikke utarbeidet virksomhetsplan med mål og resultatkrav slik avtalen forutsetter, og rapportering til kommunestyret skjer ikke i samsvar med avtalens bestemmelser. Videre gjenstår det arbeid med å avklare ansvar for overvåking av operasjonell teknologi og med å styrke arbeidet knyttet til håndtering, gjenoppretting og læring etter sikkerhetshendelser.

4.2 Anbefalinger

Revisor anbefaler 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

Kilder

Datatilsynet. «Personvernombud». Åpnet 8. september 2026.

Datatilsynet. «Personvernprinsippene». Åpnet 8. september 2026.

Datatilsynet. «Virksomhetenes plikter etter personvernregelverket». Åpnet 8. september 2026.

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften). FOR-2004-06-25-988. Digitaliserings- og forvaltningsdepartementet.

Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften). FOR-2018-12-20-2053. Justis- og beredskapsdepartementet.

Jøsang, Audun. 2025. Cybersikkerhet: teknologier og styring. 3. utg.

Kommunal- og distriktsdepartementet. Internkontroll i kommunesektoren: Veileder om kommunelovens internkontrollbestemmelser.

KS. Kommunedirektørens internkontroll: Orden i eget hus.

KS. Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet.

Lov om behandling av personopplysninger (personopplysningsloven). LOV-2018-06-15-38. Justis- og beredskapsdepartementet.

Lov om digital sikkerhet (digitalsikkerhetsloven). LOV-2023-12-20-108. Justis- og beredskapsdepartementet.

Lov om kommuner og fylkeskommuner (kommuneloven). LOV-2018-06-22-83. Kommunal- og distriktsdepartementet.

Lov om nasjonal sikkerhet (sikkerhetsloven). LOV-2018-06-01-24. Justis- og beredskapsdepartementet.

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 vurderes i forhold til. Disse kriteriene skal være begrunnet i, eller utledet av, autoritative kilder innenfor det reviderte området. Slike autoritative kilder kan være lov, forskrift, forarbeider, rettspraksis, politiske vedtak (mål og føringer), administrative retningslinjer, samt statlige føringer og praksis. I denne forvaltningsrevisjonen har vi benyttet oss av følgende kilder til revisjonskriterier:

- Lov om nasjonal sikkerhet (Sikkerhetsloven)
- Lov om digital sikkerhet (Digitalsikkerhetsloven)
- Lov om behandling av personopplysninger (Personopplysningsloven)
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
- Forskrift om virksomheters arbeid med forebyggende sikkerhet (Virksomhetsikkerhetsforskriften)
- Lov om kommuner og fylkeskommuner (kommuneloven)
- Veileder i sikkerhetsstyring, Nasjonal sikkerhetsmyndighet[23]
- NSMs grunnprinsipper for IKT-sikkerhet, Nasjonal sikkerhetsmyndighet
- Virksomhetenes plikter knyttet til personvernregelverket, Datatilsynet
- KS: Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet
- KS: Kommunedirektørens internkontroll – orden i eget hus

Problemstilling 1: Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket?

Overordna styringssystem og rammeverk

Sikkerhetsloven stiller generelle krav til forebyggende sikkerhetsarbeid i kapittel 4. Sikkerhetsloven gjelder ikke nødvendigvis for kommuner, men den kan ha bestemmelser som kan være fornuftig for kommuner å etterfølge. Det samme gjelder Lov om digital sikkerhet (digitalsikkerhetsloven). Den gjelder også i begrenset grad for kommuner, men det kan også være fornuftig å følge bestemmelser i den loven. Sikkerhetsstyring er hjemlet i § 4-1; forebyggende sikkerhetsarbeid skal være en del av virksomhetens styringssystem. Virksomhetssikkerhetsforskriften, som er underlagt sikkerhetsloven, definerer i § 3 kravet om at virksomheter som omfattes av sikkerhetsloven, skal etablere et styringssystem for sikkerhet. Systemet skal sikre at virksomheten oppfyller kravene gitt i eller med hjemmel i loven.

Nasjonal sikkerhetsmyndighets veileder i sikkerhetsstyring skriver at sikkerhetsstyring handler om systematiske aktiviteter som er nødvendige for å oppnå og opprettholde et forsvarlig sikkerhetsnivå for virksomhetens skjermingsverdige verdier. Skjermingsverdige verdier er definert i sikkerhetslovens §§ 5-1 og 6-1. *I § 5-1: Informasjon er skjermingsverdig dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig.* Videre, i § 6-1, første ledd: *Et informasjonssystem er skjermingsverdig dersom det behandler skjermingsverdig informasjon, eller dersom det i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner.*

Nasjonal sikkerhetsmyndighets grunnprinsipper for sikkerhetsstyring (NSM 2020) er overordna for hele virksomheten og disse utfylles av grunnprinsipper for fysisk sikkerhet, IKTsikkerhet og personellsikkerhet.

Ifølge veilederen i sikkerhetsstyring omfatter sikkerhetsstyring alle aktiviteter som har betydning for det forebyggende sikkerhetsarbeidet. Sikkerhetsstyring skal gjennomføres planlagt og systematisk i form av et sikkerhetsstyringssystem som omfatter planlegging, etablering, gjennomføring og forbedring av det forebyggende sikkerhetsarbeidet. Utformingen av styringssystemet for sikkerhet skal omfatte følgende prinsipper:

- Risikostyring
- Sikkerhetsledelse
- Sikkerhetsorganisering
- Sikkerhetstiltak og prosedyrer
- Forhold til andre virksomheter
- Sikkerhetsoppfølging
- Sikkerhetsdokumentasjon

Datatilsynet anbefaler i sin veileder om virksomhetens plikter at det benyttes anerkjente standarder, rammeverk og veiledere som beskriver styringssystem for informasjonssikkerhet.

Sikkerhetsmål og sikkerhetsstrategi

Virksomhetsikkerhetsforskriften fastsetter krav om sikkerhetsmål i § 5. Virksomheten skal fastsette hvordan kravene til et forsvarlig sikkerhetsnivå skal oppfylles og kriterier for å evaluere om kravene er oppfylt.

eForvaltningsforskriftens § 15 omhandler internkontroll på informasjonssikkerhetsområdet for forvaltningsorgan. Første ledd krever at mål og strategier for informasjonssikkerhet er beskrevet (sikkerhetsmål og sikkerhetsstrategi). Dette skal danne grunnlaget for forvaltningsorganets internkontroll på området for informasjonssikkerhet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller

instruks. Kravene i personvernforordningen vil være aktuelle å innarbeide i en slik sikkerhetsstrategi.

Datatilsynet[26] skriver at sikkerhetsstrategien skal omfatte grunnleggende beslutninger om organisering og gjennomføring av sikkerhetsarbeidet. Dette gjelder blant annet fordeling og avklaring av arbeidsoppgaver mellom ledelse og driftspersonell, men også beslutning om eventuelt å ta i bruk eksterne leverandører i sikkerhetsarbeidet. Videre skal sikkerhetsstrategien gjøre rede for organisatoriske og tekniske strategiske valg. Strategien beskriver hvilke virkemidler virksomheten velger å bruke for å nå målene.

Sikkerhetsorganisasjon

Jamfør sikkerhetsloven § 4-1 er det er virksomhetens leder som har ansvaret for det forebyggende sikkerhetsarbeidet. I forskriften om virksomhetens sikkerhet stilles det i § 4 krav om styringsdokument. Leder av virksomheten skal fastsette et styringsdokument som beskriver hvilke deler av sikkerhetsloven som gjelder for virksomheten, roller og ansvar i virksomhetens forebyggende sikkerhetsarbeid og prinsipper for virksomhetens sikkerhetsarbeid. Styringsdokumentet skal gjøres kjent og tilgjengelig for blant annet alle ansatte. Virksomhetsikkerhetsforskriften § 6 definerer videre krav til roller og ansvar for det forebyggende sikkerhetsarbeidet. Det er leder sitt ansvar å fordele roller og ansvar, og at disse gjøres kjent i virksomheten.

Internkontroll

Internkontroll er hjemlet i kommuneloven § 25, der det står at internkontrollen skal være systematisk og tilpasset virksomhetens størrelse, egenart, aktiviteter og risikoforhold.
Kommunedirektøren er ansvarlig for internkontrollen og skal:

- utarbeide en beskrivelse av virksomhetens hovedoppgaver, mål og organisering
- ha nødvendige rutiner og prosedyrer
- avdekke og følge opp avvik og risiko for avvik
- dokumentere internkontrollen i den formen og det omfanget som er nødvendig
- evaluere og ved behov forbedre skriftlige prosedyrer og andre tiltak for internkontroll.

Andre ledd i § 15 i eForvaltningsforskriften krever at det skal være etablert internkontroll på området for informasjonssikkerhet. Internkontrollen skal være basert på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være integrert som en del av virksomhetens helhetlige styringssystem. Tredje ledd i § 15 krever at omfang og innretning på internkontroll skal være tilpasset risiko.

[26] www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/

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

Risikovurderinger

Risikovurderinger er en sentral del av internkontrollen. Kommuneloven og eforvaltningsforskriften (samt sikkerhetsloven og virksomhetsikkerhetsforskriften) krever at virksomheten regelmessig skal gjennomføre vurdering av risiko. Vurderingen danner grunnlaget for iverksetting av forebyggende sikkerhetstiltak. Videre skal virksomheten, som en del av vurderingen av risiko, kartlegge hvilke virksomheter den er avhengig av for å fungere som den skal. Vurderingen skal gjennomgås jevnlig og om nødvendig revideres. Kravet om vurdering av risiko er videre utdypet i virksomhetssikkerhetsforskriften § 12. Forskriften skriver i andre ledd at behovet for å gjennomføre en ny helhetlig vurdering av risikoen skal vurderes årlig.

Personvern

Personopplysningsloven har som formål å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Loven gjennomfører EUs personvernforordning i norsk rett. Personopplysningsloven er bygget på noen grunnleggende prinsipper, og alle som behandler personopplysninger må følge disse prinsippene.

Den behandlingsansvarlige og databehandleren skal utpeke et personvernombud når behandlingen utføres av en offentlig myndighet eller et offentlig organ. (artikkel 37 nr 1-a i forordningen)

Den behandlingsansvarlige skal sørge for at det blir etablert rutiner som sikrer at ombudet på riktig måte og til rett tid involveres i alle spørsmål som gjelder vern av personopplysninger. Tidlig involvering legger til rette for etterlevelse av regelverket og for at personvernhensyn blir ivaretatt når det utvikles nye løsninger.

For å sikre at personvernombudet blir informert og involvert i alle prosesser som er relevant skal virksomheten sørger for at:

- ombudet regelmessig blir invitert til å delta i møter med topp- og mellomledelsen (artikkel 38)
- ombudet er til stede og blir hørt når avgjørelser med mulige personvernkonsekvenser blir tatt (artikkel 39 nr 1-c)
- ombudet blir varslet når rutiner av betydning skal endres, eller nye IT-systemer og sikkerhetstiltak skal utvikles (artikkel 38 og 39)

- ombudets vurderinger blir hørt og tatt i betraktning. Hvis det er uenighet kan det være lurt å dokumentere begrunnelsen for at personvernombudets anbefaling ikke blir fulgt (artikkel 38 nr 3)
- ombudet blir informert og rådspurt ved mulige brudd på personopplysningssikkerheten (avvik), eller andre hendelser som kan ha personvernmessige konsekvenser (artikkel 39 a og e)

Virksomheten skal også stille til rådighet de ressursene som er nødvendig for at personvernombudet skal kunne utføre sine oppgaver. Dette inkluderer å gi tilgang til personopplysninger og behandlingsaktiviteter, og å gjøre det mulig for ombudet å opprettholde sin dybdekunnskap.

En av pliktene er at alle virksomheter som behandler personopplysninger, skal føre protokoll over behandlingsaktivitetene de har ansvar for (artikkel 30 i personopplysningsloven). Protokollen skal inneholde formålet med behandlingen, hvilke kategorier personopplysninger kommunen behandler, tidsfrister for sletting og beskrivelse av tekniske og organisatoriske sikkerhetstiltak. Dersom det er aktuelt, skal eventuelle databehandlere stå oppført i protokollen.

Datatilsynet har laget informasjon om pliktene en virksomhet har etter personvernregelverket. En av pliktene Datatilsynet referer til er vurdering av personvernkonsekvenser (DPIA – Data Protection Impact Assessment) (artikkel 35 i personvernforordningen). Artikkel 35 krever at virksomheten gjennomfører en vurdering av personvernkonsekvenser ved behandlinger som vil medføre høy risiko for fysiske personers rettigheter og friheter. Datatilsynet[27] skriver følgende om DPIA:
«En vurdering av personvernkonsekvenser er en prosess som skal beskrive behandlingen av personopplysninger, og vurdere om den er nødvendig og proporsjonal. Den skal også bidra til å håndtere de risikoene behandlingen medfører for enkeltpersoners rettigheter og friheter ved å vurdere dem og fastlegge risikoreduserende tiltak.» DPIA skal som minimum inneholde:

- En systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen.
- En vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene.
- En vurdering av risikoene for de registrertes rettigheter og friheter
- De planlagte tiltakene for å håndtere risikoene og for å påvise at forordningen overholdes.

[27] www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/

Opplæring

Sikkerhetsloven definerer i § 4-1 at virksomheten skal sørge for at ansatte, leverandører og oppdragstakere har tilstrekkelig risiko- og sikkerhetsforståelse. Kravet om ressurser og kompetanse er videre utdypet i virksomhetsikkerhetsforskriften § 7. Forskriften krever blant annet at de ansatte som får tilgang til skjermingsverdige verdier, får tilstrekkelig kompetanse om sikkerhet og kartlegge at personene kjenner til relevante sikkerhetstrusler og sikkerhetsbestemmelser. Veilederen fra NSM skriver at riktig kompetanse oppnås og opprettholdes gjennom planmessig opplæring, kvalifisering og kompetansevedlikehold.

Datatilsynet skriver at målet med brukeropplæring er å sørge for at brukerne er oppmerksomme på trusler mot personvernet og informasjonssikkerheten generelt. Brukerne må være gitt muligheten til å etterleve dette i sitt daglige arbeid gjennom tilpasset opplæring ut fra behovet. Brukerne bør få opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle risikoer.

Utleda revisjonskriterier for problemstilling 1

På bakgrunn av redegjørelsen over, er følgende revisjonskriterier utledet for den første problemstillingen.

- Kommunen bør ha et styringssystem for informasjonssikkerhet og personvern som angir
    - Sikkerhetsmål
    - Sikkerhetsstrategi
    - Sikkerhetsorganisasjon, hvor roller og ansvar framgår
- Informasjonssikkerhet skal inngå i kommunens internkontrollsystem. Den skal inneholde:
    - Oversikt over regelverk, prosedyrer og rutiner for informasjonssikkerhet og personvern
    - Risiko- og sårbarhet og beredskap for informasjonssikkerhet og personvern
    - System for håndtering av avvik innen informasjonssikkerhet og personvern
- Kommunen skal ha et personvernombud
    - Det skal sikres nødvendig uavhengighet for personvernombudet
    - Personvernombudet skal sikres nødvendige ressurser for å utføre minimumoppgaver
    - Kommunen skal ha rutiner for personvernombudets arbeid som sikrer involvering og regelmessig dialog med ledelsen.
- Kommunen skal føre protokoll over hvilke personopplysninger de behandler, som minimum inneholder obligatorisk informasjon.

- Kommunen skal ha databehandleravtaler som minimum inneholder obligatorisk informasjon
- Kommunen skal gjennomføre en vurdering av personvernkonsekvenser ved behandlinger som vil medføre høy risiko for fysiske personers rettigheter og friheter
- Kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet og personvern (herunder opplæring i bruk av kunstig intelligens – KI)

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

I den andre problemstillingen er vi opptatt av avtaler som kommunen har med Stjørdal kommune, som er vertskommune for IKT-tjenester i Malvik kommune via Værnesregionen IT (VarIT). Vi er opptatt av om avtalen, eller avtalene ivaretar organisatoriske og tekniske tiltak for informasjonssikkerhet og personvern.

Lov om kommuner og fylkeskommuner (kommuneloven)

Vertskommunesamarbeid er regulert i kommuneloven, kapittel 20. Det skilles mellom vertskommunesamarbeid med nemnd og administrativt vertskommunesamarbeid. Samarbeidet om IKT-tjenester er et administrativt vertskommunesamarbeid. Stjørdal kommune er vertskommune og Malvik kommune er samarbeidskommune. Det vil si at Malvik kommune får IKT-tjenester fra Stjørdal kommune. I denne forvaltningsrevisjonen er vi opptatt av om det er etablert avtaler mellom Malvik og Stjørdal kommuner, som er tydelige på ansvar og oppgaver, og som sikrer tekniske og organisatoriske tiltak for informasjonssikkerhet og personvern.

I kommuneloven, § 20-4, gjelder samarbeidsavtale mellom vertskommunen og samarbeidskommunen. I første ledd heter det:

- § 20-4, første ledd: Når et vertskommunesamarbeid opprettes, skal det inngås en skriftlig samarbeidsavtale mellom deltakerne i vertskommunesamarbeidet.

I § 20-4 tredje ledd, er det listet opp ni punkt, fra a) – i), om hva samarbeidsavtalen skal inneholde. I denne forvaltningsrevisjonen er det punkt c) og e) som vil bli undersøkt nærmere:

§ 20-4 Samarbeidsavtalen skal inneholde bestemmelser om:

c) hvilke oppgaver og hvilken myndighet som skal legges til vertskommunen
e) hvilke av vertskommunens vedtak deltakerne skal underrettes om

Internkontrollbestemmelsene i kommuneloven er også aktuelle når det gjelder vertskommunesamarbeid.

I kapittel § 25-1 i kommuneloven, første ledd, heter det at kommuner (og fylkeskommuner) skal ha internkontroll med administrasjonens virksomhet for å sikre at lover og forskrifter følges. Kommunedirektøren i kommunen er ansvarlig for internkontrollen. I denne forvaltningsrevisjonen er det kommunedirektøren i Malviks ansvar for internkontroll med IKTtjenestene som utføres av vertskommunen som er undersøkt.

Veileder om kommunelovens internkontrollbestemmelser utdyper kommunedirektøren i samarbeidskommunen (Malvik kommune) ansvar for oppgaver som utføres av vertskommunen (Stjørdal kommune). I kapittel 3.1 framgår følgende om ansvaret for internkontrollen:

> Av forarbeidene følger det også at ved vertskommunesamarbeid etter kommuneloven, vil det være den kommunen som utfører oppgaven (vertskommunen), som har internkontrollansvaret for oppgaven som gjøres i samarbeidet. Dette blir på samme måte som andre oppgaver kommunen utfører. I tillegg vil også de kommunene som ikke utfører oppgavene i samarbeidet (samarbeidskommunene) ha et visst internkontrollansvar. De kan jo ikke gi fra seg hele ansvaret for oppgavene selv om de gir fra seg utførelsen av oppgavene. Følgelig vil også kommunedirektøren i samarbeidskommuene ha et internkontrollansvar. Dette vil bli på samme måte som for andre interkommunale samarbeid og i praksis innebære et ansvar for å følge med på at samarbeidsavtalen blir fulgt, slik at innbyggerne i samarbeidskommunen får det de har krav på selv om det er vertskommunen som utfører oppgaven, se punkt 3.1.3.

I kapittel 3.1.3 framgår følgende:

> Når en kommune inngår et interkommunalt samarbeid for å løse en lovpålagt oppgave, oppstår det et spørsmål om hvor langt kommunedirektørens interkontrollansvar strekker seg i slike tilfeller overfor samarbeidet. Ved interkommunale samarbeid vil kommunedirektøren i de enkelte kommunene ha et ansvar til å følge opp samarbeidet og arbeidet der, på samme måte som ved bruk av private aktører, se nedenfor kapittel Kommunedirektøren må forsikre seg om at arbeidet i det interkommunale samarbeidet utføres på en slik måte at innbyggerne får det de har krav på etter lov og forskrift, uavhengig av hva slags organisasjonsform samarbeidet utføres i.

I denne forvaltningsrevisjonen ser vi på om det er nedfelt i samarbeidsavtale eller andre avtaler mellom Malvik kommune og Stjørdal kommune hva som er grenseoppgangen mellom samarbeidskommunen og vertskommunen om IKT-tjenester, og ansvar for tekniske og organisatoriske tiltak for informasjonssikkerhet og personvern.

Kommunal- og distriktsdepartementet har også utarbeidet en **veileder for interkommunalt samarbeid**,[28] hvor vertskommunesamarbeid er et av flere typer samarbeid som beskrives. I kapittel 5 i veilederen er vertskommunesamarbeid beskrevet nærmere. Kapittel 5.4.4 handler om eksempler på hva samarbeidsavtalen kan inneholde. Ett av punktene er retningslinjer for samhandling mellom deltakerkommunene.

I denne forvaltningsrevisjonen vurderes det om det er etablert regelmessig samhandling mellom Malvik kommune og tjenestene i Stjørdal kommune som utfører IKT-tjenester for Malvik kommune.

Det er utarbeidet en **samarbeidsavtale** mellom Malvik kommune og Stjørdal kommune om IKT-tjenester. Vi har tatt ut noen punkt i avtalen som vi undersøker nærmere.

Punkt 5, femte strekpunkt: Vertskommunen skal utarbeide en virksomhetsplan med mål og

resultatkrav. Planen skal beskrive de tiltak som planlegges for å få en god måloppnåelse, herunder forventet ressursinnsats.

Punkt 8: Værnesregionen IKT rapporterer til kommunedirektøren i vertskommunen. Vertskommunens kommunedirektør rapporterer over virksomheten inkludert regnskap til kommunestyrene i samarbeidet pr. tertial og avlegger årsrapport.

Nasjonal sikkerhetsmyndighet har utarbeidet **grunnprinsipper sikkerhetsstyring** (NSM 2020, oppdatert 2022).[29] NSMs grunnprinsipper for sikkerhetsstyring er et sett med prinsipper og anbefalte tiltak som beskriver hva virksomheten kan gjøre for å oppnå og opprettholde et akseptabelt sikkerhetsnivå.

Grunnprinsippene for IKT-sikkerhet er delt inn i fire kategorier som er utgangspunkt for revisjonskriteriene som er gjengitt under. I denne forvaltningsrevisjonen vurderer vi om samarbeidsavtalen og underliggende avtaler ivaretar tekniske og organisatoriske tiltak for informasjonssikkerhet og personvern:

- oversikt over enheter, programvare og tilganger (identifisere og kartlegge)
- sikkerhet i anskaffelser, tjenesteutsettelse, IKT-arkitektur og sikkerhetsoppdateringer (beskytte og oppdatere)
- kontroll av sikkerhetstilstand og ledelsens gjennomgang (oppdage)
- håndtering, gjenoppretting og læring av hendelser (håndtering og gjenoppretting)

[28] https://www.regjeringen.no/contentassets/866a6055967f4f82958407f9399a1c50/no/pdfs/veilederinterkommunalt-samarbeid.pdf

[29] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-sikkerhetsstyring/introduksjon/

Utfra disse kildene er følgende revisjonskriterier utledet:

- Det skal være inngått samarbeidsavtale og eventuelt andre avtaler som er tydelig på myndighet, ansvar og oppgaver, og som er oppdatert i henhold til gjeldende regelverk
- Det bør være regelmessig samhandling mellom VarIT og Malvik kommune, hvor informasjonssikkerhet og personvern er ivaretatt
- Malvik kommune bør påse at tjenestene fra VarIT styres etter en virksomhetsplan med mål og resultatkrav
- Malvik kommune bør påse at kommunedirektøren i vertskommunen rapporterer til kommunestyret i Malvik per. tertial (herunder årsrapport) i henhold til avtalen.
- Malvik kommune bør forsikre seg om at grunnprinsippene for sikkerhetsstyring er ivaretatt:
    - oversikt over enheter, programvare og tilganger (identifisere og kartlegge)
    - sikkerhet i anskaffelser, tjenesteutsettelse, IKT-arkitektur og sikkerhetsoppdateringer (beskytte og oppdatere)
    - kontroll av sikkerhetstilstand og ledelsens gjennomgang (oppdage)
    - håndtering, gjenoppretting og læring av hendelser (håndtering og gjenoppretting)

VEDLEGG 2 – UTTALELSE

MALVIK KOMMUNE
Kommunedirektøren

Dato: 07.09.2026
Vår referanse: 2026/857-3, 22338/2026
Saksbehandler: Jens Berget
Deres referanse:

REVISJON MIDT-NORGE SA
Brugata 2
7715 STEINKJER

Kommunedirektørens uttalelse til foreløpig rapport – Informasjonssikkerhet og personvern i Malvik kommune 2026

Kommunedirektøren viser til mottatt foreløpig rapport for forvaltningsrevisjon om informasjonssikkerhet og personvern i Malvik kommune.

Kommunedirektøren tar revisjonens funn, vurderinger og konklusjoner til etterretning. Det er positivt at revisjonen bekrefter at Malvik kommune i all hovedsak har etablert et styringssystem som ivaretar krav i regelverket, og at vertskommunesamarbeidet med Værnesregionen IKT (VarIT) i hovedsak bidrar til å sikre organisatoriske og tekniske tiltak for informasjonssikkerhet og personvern. Rapporten gir et konstruktivt grunnlag for kontinuerlig forbedring på områder der det er avdekket mangler eller behov for tiltak. Nedenfor følger kommunedirektørens kommentarer til de enkelte funnene, samt en redegjørelse for hvordan anbefalingene vil bli fulgt opp.

2. Kommentarer til funn og vurderinger

2.1 Styringssystem og internkontroll (Kapittel 2)

Revisjonen påpeker at kommunen har beskrevet sikkerhetsmål og sikkerhetsorganisasjon, men at det mangler en skriftlig sikkerhetsstrategi. Videre viser rapporten at det overordnede kvalitetssystemet Compilo og fagsystemet Visma Draftit inneholder regelverk, prosedyrer og rutiner for informasjonssikkerhet og personvern.

Sikkerhetsstrategi: Kommunedirektøren deler revisors vurdering av at en skriftlig sikkerhetsstrategi vil bidra til å synliggjøre hvordan kommunen skal nå de vedtatte sikkerhetsmålene. At dette foreløpig ikke har vært utarbeidet, skyldes at organisasjonen har prioritert å få på plass de mest kritiske styrende og kontrollerende dokumentene først.

Opplæring og kompetanse: Det er positivt at revisjonen trekker frem kommunens opplæringstiltak, herunder veilederen for kunstig intelligens (KI), phising-simuleringer og kursportalen GLUP. Kommunedirektøren erkjenner imidlertid svakheten ved at det i dag mangler systematisk oversikt over ansattes gjennomføring av kompetansetiltakene.

Postadresse: Postboks 140, 7551 HOMMELVIK
Besøksadresse: Torggata 7
E-postadresse: postmottak@malvik.kommune.no
Nettsted: malvik.kommune.no
Telefon: 73 97 20 00
Org.nummer: 971 035 560

2.2 Personvern (kapittel 2.4)

Revisjonen konkluderer med at regelverket for personopplysninger i varierende grad er fulgt opp når det gjelder behandlingsprotokoller, personvernkonsekvensutredninger (DPIA) og databehandleravtaler.

Behandlingsprotokoller og databehandleravtaler: Kommunedirektøren merker seg at kun 22 av 39 registrerte behandlinger i Visma Draftit står oppført som ferdigstilt, og at systemeierne i varierende grad har full oversikt over databehandleravtalene innenfor sine områder. Det er igangsatt et viktig arbeid på skoleområdet etter tilsyn fra Datatilsynet, der databehandleravtaler har blitt prioritert. Dette arbeidet videreføres og systematiseres for hele kommunen.

Vurdering av personvernkonsekvenser (DPIA): Ved revisjonsgjennomgangen var det kun registrert én fullført DPIA i Draftit. Etter avsluttet revisjon er det fire fullførte DPIA. Kommunedirektøren deler vurderingen om at dette arbeidet må prioriteres høyere, og vil støtte arbeidet med å importere standardiserte maler (såkalte 80 % DPIA-er fra KS/DFØ) for å redusere tidsbruken og heve kvaliteten i virksomhetene.

Personvernombud og personvernkontakter: Ordningen med personvernombud og personvernkontakter vurderes som en styrke for organisasjonen. Samtidig bekreftes det at rollene er relativt nye og ulikt praktisert. Det er behov for å tydeliggjøre grensesnittene og ansvarsforholdene mellom personvernombudet, vertskommunen og Malvik kommunes egen ledelse.

2.3 Vertskommunesamarbeid om IKT-tjenester (Kapittel 3)

Overgangen til IKT-samarbeidet gjennom VarIT fra 1. januar 2025 har vært en omfattende prosess, og migreringen av infrastruktur ble ferdigstilt våren 2026. Kommunedirektøren er tilfreds med at samarbeidet har gitt kommunen et betydelig sikkerhetsløft på det tekniske området, inkludert kontinuerlig overvåking og tilgang til ekstern SOC-tjeneste (Security Operations Center). Revisjonen peker imidlertid på vesentlige formelle avvik i styringen av samarbeidet:

Virksomhetsplan og rapportering: Det foreligger ikke en virksomhetsplan med mål og resultatkrav for VarIT, til tross for at dette er et krav i samarbeidsavtalens kapittel 5. Det har heller ikke blitt rapportert tertialvis til kommunestyret i samsvar med avtalens bestemmelser. Kommunedirektøren tar dette til etterretning og vil ta initiativ overfor vertskommunen Stjørdal for å rette opp disse styringsmessige manglene.

Operasjonell teknologi (OT): Revisjonen påpeker at overvåking og ansvarsforhold knyttet til operasjonell teknologi (for eksempel i vann- og avløpssystemer) foreløpig ikke har vært fullt ut avklart. Kommunedirektøren bekrefter at det er igangsatt en prosess med VarIT for å etablere en felles, dedikert ressurs for å sikre nødvendig OT-kompetanse og OT-sikkerhet.

Gjenoppretting og beredskap: Arbeidet med gjenoppretting og prioritering av kritiske systemer ved alvorlige hendelser er ikke tilstrekkelig samordnet med VarIT. Kommunedirektøren vil sørge for at dette avklares, og viser til at kommunen planlegger en større beredskapsøvelse knyttet til bortfall av e-kom høsten 2026, der også VarIT skal delta.

3. Oppfølging av revisjonens anbefalinger

Kommunedirektøren vil iverksette følgende tiltak for å følge opp anbefalingene i rapporten:

Revisors anbefaling	Kommunedirektørens planlagte oppfølging og tiltak
Beskrive sikkerhetsstrategi for å nå sikkerhetsmålene	Det skal utarbeides et utkast til overordnet sikkerhetsstrategi for Malvik kommune. Strategien skal beskrive de organisatoriske, tekniske og strategiske valgene kommunen gjør for å realisere sikkerhetsmålene i policyen. Utkastet vil bli lagt frem for strategisk ledergruppe for forankring og vedtak.
Sørge for at kommunestyret får avtalt rapportering om personvernombudet og VarITs virksomhet	Kommunedirektøren vil gå i dialog med administrativ ledelse i vertskommunen Stjørdal for å sikre at de avtalte årsrapportene for både personvernombudet og VarIT blir utarbeidet og lagt frem for kommunestyret i Malvik i samsvar med samarbeidsavtalene.
Utarbeide og ajourføre behandlingsprotokoller, databehandleravtaler og konsekvensvurderinger for personvern (DPIA)	Det vil bli gitt en tydelig bestilling til alle kommunalsjefer og virksomhetsledere om å ferdigstille og oppdatere behandlingsprotokoller og tilhørende databehandleravtaler i henholdsvis Visma Draftit og arkivsystemet Elements. For å effektivisere arbeidet med DPIA-er vil det legges til rette for bruk av standardiserte maler (80 % DPIA) i samarbeid med KS der dette er tilgjengelig.
Følge opp ansattes opplæring og informasjon om informasjonssikkerhet og personvern	Innføring av KS kunnskap (2026/2027) vil forhåpentligvis gi mulighet for etablering av lederdashbord som gjør det mulig for enhetsledere å følge opp og dokumentere ansattes gjennomføring av obligatoriske kurs i informasjonssikkerhet og personvern. Gjennomføring av planlagte workshops og e-kom-øvelsen høsten 2026 vil også bidra til å øke den praktiske beredskapskompetansen.
Avklare uklarheter i roller og ansvar i samarbeidet med VarIT	Kommunedirektøren vil ta opp behovet for en revisjon og presisering av vertskommuneavtalen om IKT i arbeidsutvalget (AU) for Værnesregionen. Det er særskilt behov for å avklare ansvarsgrenser mellom systemeier (Malvik kommune) og driftsleverandør (VarIT), samt formalisere opprettelsen av et digitaliseringsråd for bedre prioritering og styring på tvers av samarbeidet.

4. Konklusjon

Den gjennomførte forvaltningsrevisjonen bekrefter at overgangen til et interkommunalt samarbeid gjennom VarIT har gitt Malvik kommune et mer robust teknisk fundament for informasjonssikkerhet. Samtidig viser rapporten at det administrative og systematiske internkontrollarbeidet i kommunens egne virksomheter må styrkes for å etterleve regelverket fullt ut.

Kommunedirektøren vurderer rapporten som et nyttig verktøy i dette arbeidet, og de beskrevne tiltakene vil bli fulgt opp systematisk. Det er imidlertid avgjørende å formidle til kontrollutvalget og kommunestyret at arbeidet med informasjonssikkerhet og personvern ikke er et tidsavgrenset prosjekt med en endelig sluttdato, det er kontinuerlige prosesser og aktiviteter som krever vedvarende oppfølging.

Dette gjelder særskilt oppgavene med å etablere og ajourføre behandlingsprotokoller, samt den løpende oppfølgingen av databehandleravtaler. I en digitalisert kommunesektor er systemer, leverandører og underleverandører i konstant endring. Når leverandører videreutvikler sine løsninger og bytter underleverandører, utløser dette fortløpende behov for revidering og oppdatering av databehandleravtaler. Å sikre 100 % etterlevelse på alle områder til enhver tid er derfor en betydelig styrings- og driftsmessig utfordring.

I likhet med mange andre kommuner har ikke Malvik kommune dedikerte operative fulltidsressurser som utelukkende arbeider med informasjonssikkerhet

og personvern. Som revisjonsrapporten synliggjør, må disse oppfølgings- og kontrollaktivitetene i stor grad løses av ledere og saksbehandlere som skal ivareta dette i tillegg til sine ordinære driftsoppgaver. Dette gjør arbeidet sårbart og krevende å gjennomføre helhetlig.

Kommunedirektøren vil derfor understreke at arbeidet med informasjonssikkerhet og personvern krever en vedvarende bevissthet, løpende oppfølging og en realistisk tilnærming til ressursbruk for å sikre at kommunen opprettholder et forsvarlig sikkerhets- og etterlevelsesnivå over tid.

Med hilsen

Stig Roald AmundsenStig Roald Amundsen Jens Berget

kommunedirektørKommunedirektørorganisasjonssjef

Dokumentet er elektronisk godkjent og kan være uten underskrift.

Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no