

Informasjonssikkerhet og personvern

Malvik kommune

Prosjektplan

2026

FR1374

1 FAKTA OM OPPDRAGET

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?

TIDS- OG RESSURSBRUK

Timeforbruk: 300 timer

Rapport til sekretær: Innen 12. august

OPPDRAGSANSVARLIG REVISOR

Anna Ølnes

Epost: aol@rmnsa.no

Telefon: 906 33 713

2 MANDAT

I dette kapitlet redegjøres det for bestillingen.

2.1 Bestilling

Revisjon Midt-Norge mottok i brev, datert 09.12.2025, bestilling av forvaltningsrevisjon om informasjonssikkerhet. Bestillingen ble vedtatt i kontrollutvalgets møte den 03.12.2025, sak 54/25. Basert på sekretærens saksutredning til saken, gjengis følgende formulering i bestillingsbrevet:

Informasjonssikkerhet

Som en viktig lokal styresmakt og tjenesteyter er kommunen avhengig av IKT på de fleste områder. Hvis IKT-systemet settes ut av funksjon, kan dette få store konsekvenser.

Eksempler på problemstillinger:

- Hva er risikoen for et dataangrep og hvordan beskytter kommunen seg mot det?
- Hvordan jobber kommunen for å møte krav til digitalisering og effektivisering?

Revisor tolker at eksemplene på problemstillinger ikke er bindende, men at de gir signal på aktuelle områder som kan dekkes i en forvaltningsrevisjon. Revisor viser til kapittel 3.1 om problemstillinger.

2.2 Bakgrunnsinformasjon

I bestillingen fra kontrollutvalget brukes «informasjonssikkerhet» i overskriften, og «IKT» og «IKT-systemet» i innledningen til eksemplene på problemstillinger. Begrepene som brukes er delvis overlappende, og her redegjøres det nærmere for forståelsen av dem.

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 (Jøsang 2025). Ulike typer informasjon vil ha ulik verdi og dermed forskjellig beskyttelsesbehov. Videre skriver Jøsang 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.¹

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 01.10.2025.² 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.³

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 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 i punkt 1 og 7. Personopplysningsloven skal regulere og sikre at

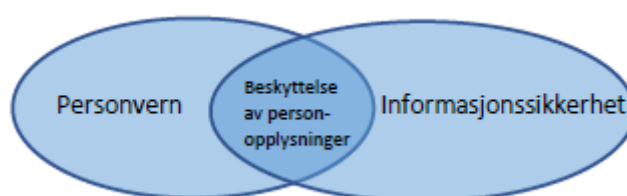
¹ KS, Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

² <https://lovdata.no/dokument/NL/lov/2023-12-20-108?q=Lov%20om%20digital%20sikkerhet>

³ <https://www.regjeringen.no/no/aktuelt/ny-lov-om-digital-sikkerhet-trer-i-kraft-i-dag/id3121009/>

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 § 5). Det er flere prinsipper enn disse. Datatilsynet har en oversikt⁴

Personvern og informasjonssikkerhet er to fagområder som har mye til felles, men som også er forskjellige.⁵ Det kan illustreres i figuren nedenfor:



Kilde: KS, Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

Figur 1. Sammenhengen mellom informasjonssikkerhet og personvern.

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.⁶

Det er lovpålagt med personvernombud for alle offentlige virksomheter.⁷ 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

⁴ <https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/>

⁵ KS, Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

⁶ KS, Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

⁷ <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/personvernombud/hvem-ma-ha-personvernombud/trinn-for-trinn-veileder/>

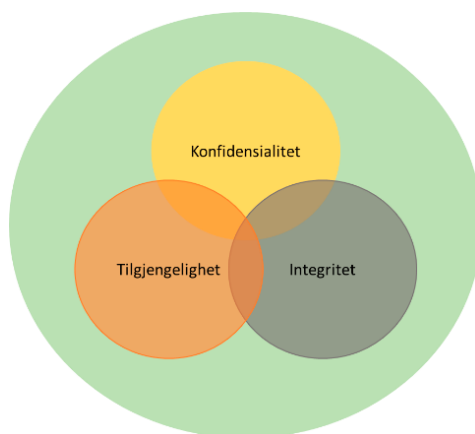
etterlevelsen av regelverket. I tillegg skal de være kontaktpunkt for de registrerte og Datatilsynet.

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.⁸

Figuren nedenfor illustrerer beskyttelsesbehovet, med de tre elementene: kan illustreres i figuren nedenfor.



Kilde: KS, Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

Figur 2. Beskyttelsesbehov for personvern og informasjonssikkerhet.

Internkontroll

Kommunedirektørens ansvar for internkontroll følger av kommuneloven kapittel 25. I tillegg er internkontroll regulert av eForvaltningsforskriften 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.

⁸ KS, Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet

Digitalisering

En definisjon på digitalisering er at det er å bruke 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.⁹

SINTEF Digital forklarer automatisering og robotisering.¹⁰ Det er en viktig del av digitaliseringen og effektiviseringen av samfunnet. Automasjon brukes innen mange områder for å øke produktivitet og løse oppgaver som ikke er egnet for manuelt arbeid. Autonomi trekker automasjon et hakk videre ved å gi systemer mulighet for å ta egne beslutninger i kompliserte omgivelser. Robotikk handler om alt fra roboter som utfører oppgaver på fabrikker til ubemannede fartøy eller droner – på land, i lufta, på vann og under vann. Droner og andre typer roboter brukes i dag mest til datainnsamling, logistikk eller til fysiske oppgaver.

Digitalisering innebærer også bruk av mulighetene som ligger i kunstig intelligens (KI). Algoritmer og maskinlæring brukes for å tolke signaler, støtte beslutninger og gjennomføre tiltak.

Digitaliserings- og forvaltningsdepartementet har hatt et utkast til ny lov om KI¹¹ ute på høring i perioden 30. juni – 30. september 2025. Per første del av januar 2026, er loven ikke ferdigbehandlet i Stortinget, og derfor ikke tredd i kraft.

Informasjonssikkerhet, personvern og digitalisering er fagområder som er forskjellige, men som også har en del fellesnevne. Der informasjonssikkerhet og personvern i hovedsak gjelder sikring av de digitale løsningene som er tatt i bruk, gjelder digitalisering i større grad utviklingsarbeid og å ta i bruk nye, digitale løsninger. I kapittel 3.2, om avgrensning, vil revisor beskrive hvordan dette er tenkt å løses i dette prosjektet.

2.3 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 for helse og velferd, barn og unge og samfunn. Organisasjonssjefen leder kommunedirektørens fagstab, HR, servicetorg og Værnesregionen

⁹ <https://www.sintef.no/fagomrader/digitalisering/>

¹⁰ <https://www.sintef.no/fagomrader/digitalisering/>

¹¹ <https://www.regjeringen.no/no/aktuelt/lov-om-kunstig-intelligens-i-norge-sendes-na-pa-horing/id3113732/>

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 (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.
- 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, men det er lokal tilstedeværelse i alle kommunene som er med i samarbeidet.¹²

Malvik kommune har også personvernombud gjennom Værnesregionen. På kommunens nettside framgår det personvernerklæring, med forskjellige opplysninger om personvern, deriblant navn og kontakinformasjon for personvernombudet.

¹² <https://www.stjordal.kommune.no/tjenester/varnesregionen-fellestjenester/it-avdeling/>

3 PROSJEKTDESIGN

Dette kapittelet redegjør for revisors forslag til løsning av oppdraget.

3.1 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?

3.2 Avgrensing

Revisor forslår at forvaltningsrevisjonen avgrenses til å gjelde informasjonssikkerhet og personvern. Det andre eksempelet på problemstilling i kontrollutvalgets bestilling holdes utenfor denne forvaltningsrevisjonen, med begrunnelse i at det er et eget, omfattende temaområde, som fortjener et eget prosjekt.

Det kan være nyttig å få tilgang til noe informasjon om avtaler, som, og Malvik kommunes oppfølging av disse, både fra ansatte i Malvik kommune og fra ansatte i VarIT.

3.3 Kilder til kriterier

Aktuelle kilder til revisjonskriterier er:

- Lov om kommuner og fylkeskommuner (kommuneloven), kapittel 20 (vertskommunesamarbeid) og 25 (kommunedirektørens internkontroll).
- Lov om nasjonal sikkerhet (Sikkerhetsloven)
- Lov om behandling av personopplysninger med personvernforordningen (Personopplysningsloven)
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
- Veileder i sikkerhetsstyring, Nasjonal sikkerhetsmyndighet
- NSMs grunnprinsipper for IKT-sikkerhet, Nasjonal sikkerhetsmyndighet
- ISO 27001
- Virksomhetenes plikter knyttet til personvernregelverket, Datatilsynet
- KS' veileder i internkontroll (Orden i eget hus)
- KS' veileder for interkommunalt IKT-samarbeid

- Andre veiledere som f.eks. gjelder informasjonssikkerhet og personvern og internkontroll i kommuner

De nevnte kildene er aktuelle. Underveis vil revisor vurdere om noen kilder kan utelukkes, eller om flere kilder for kriterier bør tas inn.

3.4 Metoder for innsamling av data

Revisor vil innhente dokumentasjon fra kommunen for å besvare problemstillingene. Gjennomgang av kommunale dokumenter vil være en viktig datakilde for å undersøke hvordan kommunen jobber med informasjonssikkerhet og personvern. Eksempler på dokumenter er styringsdokumenter innenfor informasjonssikkerhet, risikovurderinger, beredskapsplaner, rutinebeskrivelser for ulike tiltak og ulike planer innenfor informasjonssikkerhet og personvern. Vertskommuneavtale (samarbeidsavtale) og eventuelle andre avtaler som Malvik kommune har inngått med Stjørdal kommune og VarIT, vil også være aktuell dokumentasjon.

Dokumentgjennomgang er en god metode for å finne frem til opplysninger som er nødvendige og relevante for kommunal oppgaveløsning og forvaltning. Det offentlige har i mange tilfeller plikt til å dokumentere sitt arbeid og sin regeletterlevelse. Informasjonssikkerhet og personvern er underlagt internkontroll og er relevant å se på meldte avvik på dette området.

Det vil være aktuelt å gjennomføre intervjuer med kommunens ledelse og nøkkelpersoner for informasjonssikkerhet og personvern. Det vil også være behov for intervju med enkelte ansatte i VarIT.

Intervju gir utfyllende informasjon for å få dybdekunnskap om hvordan arbeidet med informasjonssikkerhet foregår i kommunen og for å forstå sammenhengene. Intervjuene kan gi informasjon om at det som er beskrevet i dokumentasjonen fungerer i praksis. Det kan også være aktuelt å intervju personvernombudet i kommunen og andre ansatte i kommunen.

Det kan også være aktuelt med andre metoder innsamling og analyse av data.

3.5 Prosjektteam

Oppdragsansvarlig revisor	Anna Ølnes
Prosjektmedarbeider	Anne Grete Wold
Kvalitetssikrer	Grethe Gilstad
Kvalitetssikrer	Margrete Haugum

3.6 Milepælsplan

Bestillingsdato	09.12.2025
Prosjektplan til sekretær	21.01.2026
Oppstartsmøte	Februar/mars 2026
Datainnsamling ferdig	Mai/juni 2026
Rapport til uttalelse	Ca 1. juni 2026
Rapport til sekretær	Innen 1. august 2026

Trondheim/16.01.2026

Anna Ølnes

Oppdragsansvarlig revisor



Hovedkontor: Brugata 2, Steinkjer

Tlf. 907 30 300 - www.revisjonmidtnorge.no